Міністерство транспорту та зв'язку України
Державна адміністрація зв'язку

Одеська національна академія зв'язку ім. О.С. Попова

Інститут економіки та менеджменту
Кафедра менеджменту та маркетингу

Тардаскіна Т.М., Кононович В.Г.

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Навчальний посібник

*Рекомендовано Міністерством освіти і науки України
як навчальний посібник для
студентів вищих навчальних закладів*

Одеса-2009

УДК 338.47: 65.012.8

Менеджмент інформаційної безпеки: Навчальний посібник / Тардаскіна Т.М., Кононович В.Г. - Одеса: ОНАЗ ім. О.С. Попова, 2009. - 265с.

Рецензенти:

О.С. Редькін д.е.н., професор, заступник директора з наукової роботи Одеського інституту фінансів УДУФМТ Міністерства фінансів України.

д.е.н., професор зав. каф. Економічної та фінансової політики Одеського регіонального інституту національної академії державного управління при Президентові України.

Рекомендовано Міністерством освіти і науки України як навчальний посібник для студентів вищих навчальних закладів. Лист № 14/18- Г-315 від 09.02.07.

ISBN 5-8 404-0175-7

У навчальному посібнику розглянуті теоретичні засади й практичні аспекти менеджменту інформаційної безпеки в галузі зв'язку. Навчальний посібник містить теоретичну частину, контрольні питання, завдання для самостійної роботи та тести. У посібнику висвітлюються основні поняття та задачі менеджменту інформаційної безпеки в умовах формування інформаційного суспільства. Розглядаються основні цілі, задачі та функції забезпечення інформаційної безпеки, джерела загроз та засоби їх впливу на об'єкти інформаційної безпеки, особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки. Детально вивчається технологічне управління інформаційною безпекою. Розглядаються методичні основи оцінки економічної доцільності захисту інформації та ризики інформаційної безпеки, особливості організації служби інформаційної безпеки підприємства та менеджменту персоналу у сфері інформаційної безпеки.

Навчальний посібник призначений для студентів, які отримують базову вищу освіту за напрямом „Інформаційна безпека". Посібник буде також корисним для аспірантів, викладачів, слухачів післядипломної освіти та працівників підприємств галузі зв'язку.

© Тардаскіна Т.М., Кононович В.Г. 2009.

© Одеська національна академія зв'язку ім. О.С. Попова, 2009.

ISBN

ВСТУП

Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів. Формування та рівень розвитку інформації, інформаційних ресурсів та всього інформаційного простору є основою та головною характеристикою розвитку будь-якої соціально-економічної системи на макро- та мікрорівнях.

Особливості необмеженого та неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому.

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності телекомунікаційних мереж. Отже, проблема менеджменту інформаційної безпеки та живучості мереж в умовах розвитку та впровадження нових інформаційних технологій є актуальною та своєчасною.

Вагомий внесок у становлення і розвиток інформаційної безпеки внесли українські та російські вчені В. Герасименко, В. Домарєв, Д. Зегжда, Г. Конахович, А. Малюк, С. Петренко, С. Расторгуєв, О. Редькін, Ю. Уфімцев, П. Хорєв, В. Хорошко, В. Шорошев. Значний внесок у розвиток цих проблем належить зарубіжним вченим Н. Вінеру, Д. Сяо, Б. Ролкеру, Л. Дж. Хоффману, К. Шеннону. Творчістю цих та багатьох інших вчених напрацьовано величезний науково-теоретичний та методичний матеріал, запропоновано безліч різноманітних практичних рекомендацій щодо розв'язання тих чи інших питань, вирішення прикладних завдань.

Разом з тим, аналіз опублікованих праць з даної проблематики дає підстави говорити, що в цілому дослідження зосереджені на формуванні стандартних процедур захисту інформації. Недостатньо науково розкритими залишаються організаційно-економічні аспекти інформаційної безпеки, в Україні ще й досі чітко не установленні регламенти, які визначили б вимоги, характеристики, параметри і поняття, що пов'язані з розробкою концептуальної моделі системи інформаційної безпеки.

Актуальним на сьогодні є підготовка фахівців, які вміють ефективно організувати захист інформації і володіють сучасними технологіями захисту інформації та мають достатню кваліфікацію для проектування та розробки нових засобів і методів захисту. Саме на підготовку таких спеціалістів розрахована дисципліна «Менеджмент інформаційної безпеки».

Забезпечення інформаційної безпеки підприємств та організацій зв'язку є допоміжною діяльністю в організації і включає у себе реалізацію та підтримку двох процесів: процесу створення, функціонування та вдосконалення системи інформаційної безпеки та процесу менеджменту інформаційної безпеки.

Система менеджменту інформаційної безпеки є частиною загальної системи менеджменту організації та призначена для створення, реалізації, експлуатації, моніторингу, аналізу, підтримки й підвищенню інформаційної безпеки з врахуванням всіх ризиків організації. Система менеджменту інформаційної безпеки включає організаційну структуру, політику, діяльність з планування, процедури, процеси та ресурси. Ефективність системи менеджменту інформаційної безпеки багато у чому залежить від дотримання та виконання правил політик інформаційної безпеки всіма без винятку співробітниками організації.

Цей навчальний посібник повинен допомогти студентам, які навчаються за напрямом підготовки 1601 «Інформаційна безпека» оволодіти теоретичними знаннями та практичними навичками забезпечення інформаційної безпеки підприємства та звернути увагу на проблеми, які виникають в процесі створення комплексної системи захисту інформаційної безпеки на підприємствах зв'язку.

Наприкінці кожної частини наведено контрольні завдання та завдання до самостійної роботи, за допомогою яких можна перевірити рівень засвоєння теоретичного матеріалу.

В додатку наведено тести для перевірки одержаних знань студентів та запропоновано дороблену навчальну програму з дисципліни „Менеджмент інформаційної безпеки", яку складено у відповідності до навчального плану підготовки бакалаврів за напрямом 1601 «Інформаційна безпека» в ОНАЗ ім. О.С. Попова.

Навчальний посібник підготували: к.е.н., доцент кафедри менеджменту та маркетингу Т.М. Тардаскіна (вступ, розд. 1...5, 10...12, тести, додаток), к.т.н., доцент кафедри інформаційної безпеки та передачі даних В.Г. Кононович (вступ, розд. 5...9, 13, тести, додаток).

РОЗДІЛ 1

ОСНОВНІ ПОНЯТТЯ ТА ЗАДАЧІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

1.1 Роль та місце інформаційної безпеки в інформаційному суспільстві

Інформаційна безпека є однією з важливих складових глобальної безпеки, невід'ємною умовою глобалізації та одним з чинників впливу глобальних процесів на всі сфери діяльності. Дедалі більше посилюється роль інформаційної безпеки у процесі глобалізації і, навпаки, вплив глобальних процесів на інформаційну безпеку та взаємозв'язану з нею економічну, національну та глобальну безпеку в умовах побудови інформаційного суспільства – нового ступеня розвитку людства.

Глобальний процес інформатизації суспільства, який є відображенням загальних закономірностей генезису цивілізації, сьогодні охопив усі сфери соціокультурної діяльності людини. Стрімкий розвиток і розповсюдження нових інформаційно-комунікаційних технологій обумовлює кардинальні зміни в управлінні господарськими системами різних рівнів. Формування та рівень розвитку інформації, інформаційних ресурсів та всього інформаційного простору є основою та головною характеристикою розвитку будь-якої соціально-економічної системи на макро- та мікрорівнях.

Особливості необмеженого та неконтрольованого впливу, несанкціонованого доступу, а також виникнення комп'ютерних вірусів та інших загроз, викликають необхідність у забезпеченні інформаційної безпеки, яка є головною частиною економічної безпеки держави та національної безпеки в цілому.

Життєдіяльність суспільства, його інформаційна безпека залежить від стабільного функціонування, живучості, надійності та готовності інформаційно-телекомунікаційних мереж.

Завдяки стрімкому технологічному прогресу постає ряд життєво важливих питань щодо організації процесів оброблення, зберігання, поширення та захисту інформації в глобальних інформаційно-комунікаційних системах. Бо саме інформаційні технології та розвинена інфраструктура телекомунікацій відіграють сьогодні вирішальну роль у забезпеченні зростання продуктивності виробництва, адміністративного і господарського управління, у розширенні інформаційної взаємодії між людьми, у поширенні масової інформації, у процесі інтелектуалізації суспільства.

Інформаційна безпека має важливе значення для того, щоб інформаційні технології могли відповідати очікуванням ділового світу, споживачів і урядів та щоб дійсно надавали всі ті потенційні вигоди, що їх забезпечують інформаційно-комунікаційні технології.

Інформаційна безпека в глобальних процесах набуває особливого значення і, внаслідок її тісних взаємовпливів з економічною та національною безпекою, вносить свій значний вклад у глобальну безпеку. Глобальною безпекою назвемо такий стан глобальних процесів та форм їхньої реалізації за якого забезпечуються [157]:

– гармонічне поєднання інтересів народів, націй, держав та інтересів усього людства;

– ефективне вирішення завдань, які стоять перед людством та окремими державними, регіональними та місцевими адміністраціями;

– усебічний розвиток і забезпечення потреб кожної людини.

Вплив глобальних процесів на інформаційну безпеку, її роль та взаємозв'язок з економічною, національною та глобальною безпекою в умовах побудови інформаційного суспільства показано на рис. 1.1 [157].

Глобальна безпека має фундаментальний характер і може бути досягнута за необхідного забезпечення її складових частин.

Рисунок 1.1 – Роль та місце інформаційної безпеки у процесі глобалізації

Складовими частинами глобальної безпеки є: національна, економічна, інформаційна, технічна, юридична, фізична, соціальна, військова, екологічна, ресурсна, продовольча, енергетична, фінансово-грошова, цінова, демографічна, пожежна, медична, психологічна, психічна, кримінальна безпеки (рис. 1.2).

Особливості розвитку інформації, можливості необмеженого та неконтрольованого впливу, несанкціонований доступ, комп'ютерні віруси та інше гостро поставили перед суспільством проблеми інформаційної безпеки. Інформаційна безпека повинна здійснюватися комплексно та систематично з використанням повного набору засобів (організаційних, технічних, апаратно-програмних та ін.) щоб запобігти інформаційному тиску та в цілому будь-якій іншій небезпеці.

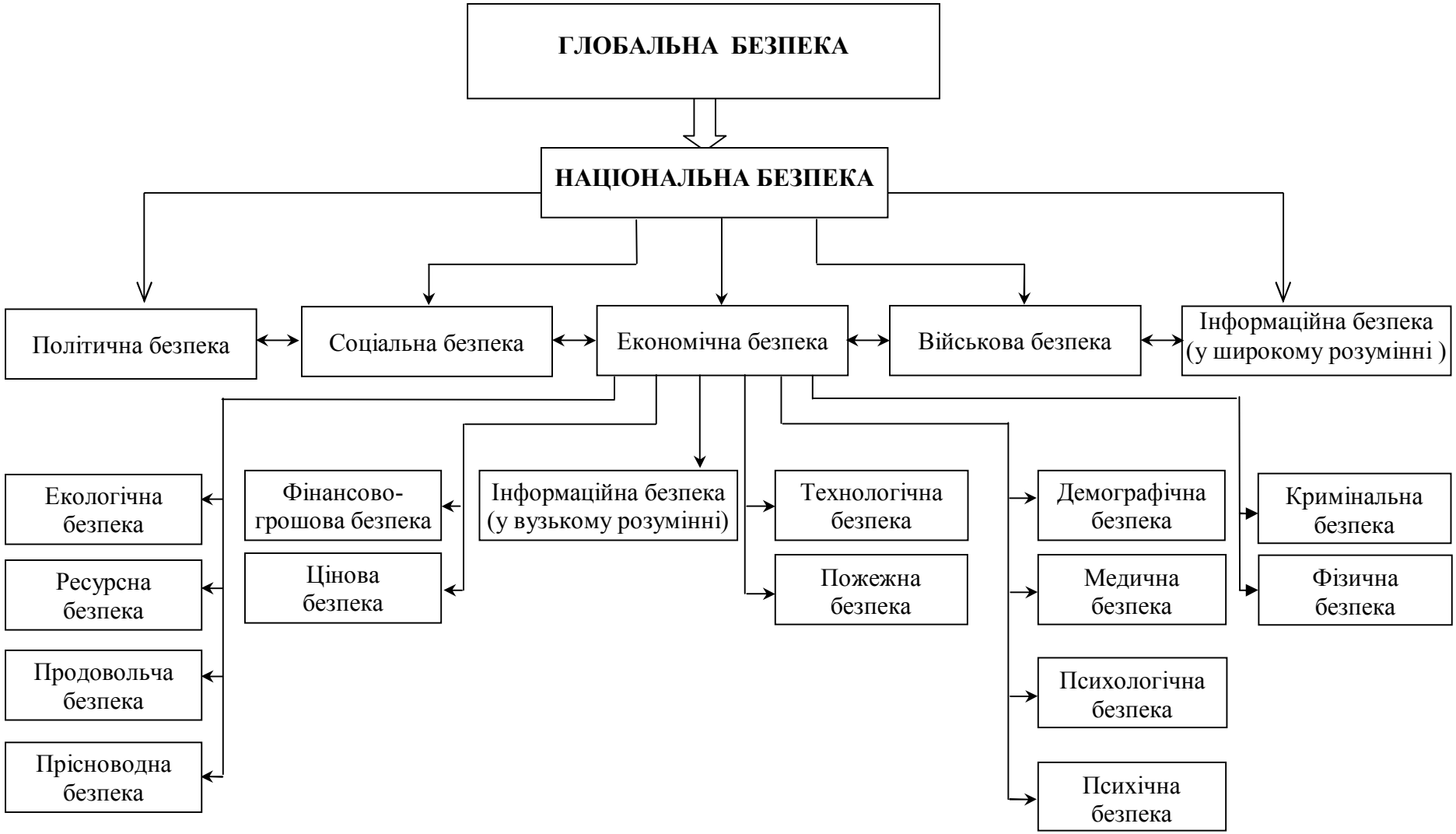


Рисунок 1.2 – Складові глобальної безпеки

Зрозуміло, що становлення суспільства нового типу дуже гостро ставить питання інформаційної безпеки простору держави, людини, суспільства, а також створення ефективної системи забезпечення прав громадян і соціальних інститутів на вільне одержання, поширення і використання інформації. Це питання неможливо обійти, тим більше, що воно стає дуже актуальним зараз і для нашої країни.

Інформаційна безпека є більш вузьким поняттям і розглядається як складова національної безпеки. Інформаційна безпека містить у собі захист інформаційних мереж, ресурсів, програмних засобів, об'єктів інтелектуальної власності й інших нематеріальних активів, включаючи майнові інтереси учасників підприємницької діяльності [91].

В умовах глобалізації посилюється значимість проблем, які пов'язані з інформаційно безпекою, таких як [186]:

– виникнення та зростання кіберзлочинності та кібертероризму;

– виникнення окремих видів інформаційної зброї та ведення глобальних інформаційних війн;

– втрата національної культури або злиття її з іншими, вплив культур країн світу та менталітету інших націй;

– стимулювання інформаційно-розвиненими державами „відпливу інтелекту" та капіталів;

– виникнення явищ „інформаційного вибуху", „інформаційного голоду" та „інформаційних війн".

– ускладнення вирішення питань збереження державної, комерційної, службової та персональної таємниці, тому що низький рівень вітчизняних інформаційних технологій обумовив побудову інформаційної інфраструктури України на базі імпортної техніки й технології;

– розвиток телебіометрики й сенсорних мереж у взаємодії людей між собою та навколишнім середовищем.

Інформаційна безпека не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації. Концептуальними є пропозиції щодо широкого залучення саме вітчизняних учених та виробників до вирішення цієї проблеми як складової національної безпеки. Тенденції розвитку сучасного світу характеризуються створенням єдиного глобального інформаційного простору на планеті, отож, проблема інформаційної безпеки стає проблемою колективною, а не окремо взятої країни.

1.2 Сутність та зміст понять у сфері інформаційної безпеки

Поняття „інформаційна безпека". Існує значна кількість робіт [24, 34, 65, 91, 99, 128, 203, 204, 160, 211], в яких з різних позицій досліджуються різноманітні аспекти поняття „інформаційна безпека". Поняття інформаційної безпеки може розглядатись у широкому та у вузькому розумінні.

Інформаційна безпека (у вузькому розумінні) є необхідною, але невід'ємною складовою інших видів безпеки. Інформаційна безпека – це невід'ємна частина політичної, економічної, військової, соціальної та інших

складових національної безпеки. Інформаційна безпека (у вузькому розумінні) розглядається як одна зі складових економічної безпеки, тому що інформація, яка циркулює на підприємстві має комерційний характер і впливає на економічні показники діяльності підприємства. Інформаційна безпека (у вузькому розумінні) розглядається як інформаційна безпека підприємства – це стан захищеності інформації підприємства від дестабілізуючого впливу зовнішніх та внутрішніх загроз.

Інформаційна безпека (у широкому розумінні) є самостійним видом безпеки поряд з національною, економічною, військовою, соціальною і політичною. Інформаційна безпека (у широкому розумінні) розглядається як інформаційна безпека держави – це складова національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз.

Інформаційна безпека інформатизації знайшла юридичний вираз на законодавчому рівні у Законі України „Про Національну програму інформатизації" [55]. Відповідно до цього Закону інформаційну безпеку забезпечують:

- комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу;
- комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації;
- банк засобів діагностики, локалізації і профілактики комп'ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високо надійні криптографічні методи захисту інформації тощо [55].

В умовах поширення інформаційних впливів справедливе визначення В. Рубана: „Інформаційна безпека людини, суспільства, держави – це стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб'єктів" [161].

Інформаційна безпека розглядається також як єдність концептуальних, теоретичних і технічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, військової, духовної та ін.), а також сфер формування, циркулювання, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління в усіх різновидах діяльності тощо [161].

В організаційно-управлінському аспекті поняття „інформаційна безпека" розглядається як: „…стан захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму завдання збитків через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації [161].

Автори книги [126] пропонують наступне визначення поняття „інформаційна безпека". „Інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій і держави".

За конкретних умов середовища функціонування інформації можна формулювати уточненні визначення, що відповідають цим умовам.

Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства) – це суспільні відносини щодо створення і підтримання в належному стані режиму нормального функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи, систем телекомунікацій; комплекс організаційних, правових та інженерно-технологічних (технічних та програмно-математичних) заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних загроз, реалізація яких може порушити або припинити життєдіяльність конкретної соціотехнічної інформаційної системи [205].

В іншому випадку: „Інформаційна безпека – це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати збитку власникам або користувачам інформації і підтримуючій інфраструктурі" [214].

На думку Н. Мойсеєва під інформаційною безпекою системи розуміється: „…властивість захищеності її інформаційної сфери (сукупності інформаційних ресурсів і інформаційної інфраструктури) від випадкових або навмисних впливів природного або штучного характеру, здатних призвести до погіршення заданих якісних характеристик функціонування і тим самим до нанесення збитку її користувачам або власникам" [106].

Поняття „інформаційна безпека" характеризує стан (властивість) інформаційної захищеності людини, суспільства, природи в умовах можливої дії загроз і досягається системою заходів, спрямованих:

– на попередження загроз. Попередження загроз – це превентивні заходи для забезпечення інформаційної безпеки в інтересах попередження можливості їхнього виникнення;

– на виявлення загроз. Виявлення загроз виражається в систематичному аналізі і контролі можливості появи реальних або потенційних загроз і своєчасних заходів для їхнього попередження;

– на локалізацію злочинних дій і вживання заходів по ліквідації загрози або конкретних злочинних дій;

– на ліквідацію наслідків загроз і злочинних дій та відновлення статус-кво.

У Законі України „Про телекомунікації" під інформаційною безпекою розуміють: „…здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення установленого порядку її маршрутизації" [61].

Як видно з наведених визначень, інформаційна безпека пов'язана із процесом захисту інформації. Тобто, якщо інформація захищена, виходить, що

вона в безпеці. Розмежуємо поняття „інформаційна безпека” та „захист інформації”.

Поняття „захист інформації”. Під захистом інформації розуміють сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією [53].

Під захистом інформації, у більш широкому сенсі, розуміють комплекс організаційних, правових і технічних заходів для запобігання загрозам інформаційної безпеки й усуненню їхніх наслідків. Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела є загрозою безпеці інформації. Мета та методи захисту інформації відображають її сутність. У цьому розумінні захист інформації ототожнюється з процесом забезпечення інформаційної безпеки, як глобальної проблеми безпечного розвитку світової цивілізації, держав, співдружностей людей, окремої людини, існування природи.

Попередження можливих загроз і протиправних дій може бути забезпечене всілякими засобами, починаючи від створення клімату глибоко-усвідомленого відношення співробітників до проблеми безпеки і захисту інформації до створення глибокої, ешелонованої системи захисту фізичними, апаратними, програмними і криптографічними засобами. Попередження загроз можливе і шляхом одержання інформації про протиправні акти, які готуються, плановані розкрадання, підготовчі дії й інші елементи злочинних вчинків. У попередженні загроз важливу роль відіграє інформаційно-аналітична діяльність служби безпеки на основі глибокого аналізу криміногенного стану й діяльності конкурентів і зловмисників.

Виявлення має на меті проведення заходів щодо збирання, нагромадження й аналітичного оброблення відомостей щодо можливої підготовки злочинних вчинків з боку кримінальних структур або конкурентів на ринку виробництва та збуту товарів і продукції.

Виявлення загроз – це дії з визначення конкретних загроз та їхніх джерел, які приносять той або інший вид збитку. До таких дій можна віднести виявлення фактів розкрадання або шахрайства, а також фактів розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів.

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози і конкретних злочинних вчинків.

Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози.

Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань і забезпечити:

– запобігання розголошення і витоку конфіденційної інформації;

– заборону несанкціонованого доступу до джерел конфіденційної інформації;

– збереження цілісності, повноти і доступності інформації;

– дотримання конфіденційності інформації;

– забезпечення авторських прав.

Інформація, що захищається, містить відомості, що складають державну, комерційну, службову та інші таємниці, які охороняються законом. Кожен вид інформації, має свої особливості в галузі регламентації, організації і здійснення цього захисту.

Найбільш загальними принципами захисту будь-якого виду інформації, що охороняється, є:

– захист інформації організує і проводить власник інформації або уповноважені ним особи (юридичні або фізичні);

– захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне захистити її від незаконного заволодіння і використання на шкоду його інтересам;

– захист інформації здійснюється шляхом проведення комплексу заходів для обмеження доступу до захищеної інформації, що захищається, і створення умов, що виключають або суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та її носіїв.

Захищена інформація, яка є державною або комерційною таємницею, як і будь-який інший вид інформації, необхідна для управлінської, науково-виробничої та іншої діяльності. Сьогодні перед захистом інформації ставляться більш широкі задачі: забезпечити безпеку інформації. Це обумовлено низкою обставин, і в першу чергу тим, що все більш широке застосування в накопичуванні й обробленні захищеної інформації, одержують електронно обчислювальні машини (ЕОМ), в яких може відбуватися не тільки витік інформації, але і її руйнування, перекручування, підроблення, блокування й інші втручання в інформацію й інформаційні системи.

Отже, під захистом інформації слід також розуміти забезпечення безпеки інформації і засобів інформації, в яких накопичується, обробляється і зберігається захищена інформація.

Таким чином, захист інформації – це діяльність власника інформації або уповноваженої ним особи з:

– забезпечення своїх прав на володіння, розпорядження і управління захищеною інформацією;

– запобігання витоку і втрати інформації;

– збереження повноти, вірогідності, цілісності захищеної інформації, її масивів і програм обробки;

– збереження конфіденційності або таємності захищеної інформації, відповідно до правил, установлених законодавчими й іншими нормативними актами.

Таким чином, захист інформації – це діяльність, яка спрямована на забезпечення конфіденційності, цілісності та доступності інформації в процесі одержання, зберігання, оброблення і поширення за допомогою організаційних, правових, технічних та економічних засобів.

Засоби забезпечення збереження та захисту інформації в державній організації, на підприємстві або фірмі відрізняються за своїми масштабами і формами. Вони залежать від виробничих, фінансових та інших можливостей

фірми, від кількості секретів, які вона охороняє та їхньої значимості. При цьому вибір таких заходів необхідно здійснювати за принципом економічної доцільності, дотримуючись у фінансових розрахунках „золотої середини", оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, можуть викликати втрату певної частки прибутку або призвести до непоправних збитків. Відсутність у керівників підприємств чіткого уявлення про умови, що сприяють витоку конфіденційної інформації, приводять до її несанкціонованого поширення.

Наявність значної кількості уразливих місць на будь-якому сучасному підприємстві або фірмі, широкий спектр загроз і досить висока технічна оснащеність зловмисників вимагає обґрунтованого вибору спеціальних рішень з захисту інформації. Основою таких рішень можна вважати:

1. Застосування наукових принципів з забезпечення інформаційної безпеки, що включають у себе: законність, економічну доцільність і прибутковість, самостійність і відповідальність, наукову організацію праці, тісний зв'язок теорії з практикою, спеціалізацію і професіоналізм, програмно-цільове планування, взаємодію і координацію, доступність у поєднанні з необхідною конфіденційністю.

2. Прийняття правових зобов'язань з боку співробітників підприємства по відношенню до збереження довірених їм відомостей (інформації).

3. Створення таких адміністративних умов, за яких виключається можливість крадіжки, розкрадання або перекручування інформації.

4. Правомірне залучення до карної, адміністративної й інших видів відповідальності, які гарантують повне відшкодування збитку від втрати інформації.

5. Проведення діючого контролю і перевірки ефективності планування і реалізації правових форм, методів захисту інформації відповідно до обраної концепції безпеки.

6. Організація договірних зв'язків з державними органами регулювання в галузі захисту інформації.

Здійснюючи комплекс захисних заходів головне – обмежити доступ у ті місця і до тієї техніки, де зосереджена конфіденційна інформація (не забуваючи, звичайно, про можливості і методи дистанційного її одержання). Зокрема, використання якісних замків, засобів сигналізації, хорошої звукоізоляції стін, дверей, стелі та підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму й ін.) серйозно ускладнять або зроблять безглуздими спроби впровадження спецтехніки.

Для надійного захисту конфіденційної інформації доцільно застосовувати наступні організаційні заходи:

1. Визначення рівнів (категорій) конфіденційності інформації, що захищається.

2. Вибір принципів (локальний, об'єктовий або змішаний), методів і засобів захисту.

3. Установлення порядку оброблення захищеної інформації.

4. Облік просторових факторів:

- уведення контрольованих зон;

- правильний вибір приміщень і розташування об'єктів між собою і щодо межі контрольованої зони.

5. Облік тимчасових факторів:

– обмеження часу оброблення захищеної інформації – доведення часу оброблення інформації з високим рівнем конфіденційності до вузького кола осіб.

6. Облік фізичних і технічних факторів:

– визначення можливості візуального (або за допомогою технічних засобів) спостереження відображуваної інформації сторонніми особами;

– відключення контрольно-вимірювальної апаратури від інформаційного об'єкта і її знеструмлення;

– максимальне рознесення інформаційних кабелів між собою і щодо провідних конструкцій;

– їхнє перетинання під прямим кутом.

Для блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів і створення системи захисту об'єкта по них необхідно здійснити низку заходів:

- проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і підведенні комунікації;

- виділити ті приміщення, всередині яких циркулює конфіденційна інформація і врахувати технічні засоби використані в них.

Основні поняття та їх зміст у сфері інформаційної безпеки наведені у табл. 1.1.

Таблиця 1.1 - Основні поняття та їх зміст у сфері інформаційної безпеки

№	Визначення	Джерело
1	**Блокування інформації** - дії, наслідком яких є припинення доступу до інформації.	*Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 р. № 81/94-ВР*
2	**Витік інформації** - результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї.	*Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 р. № 81/94-ВР*
3	**Втрата інформації -** дія, внаслідок якої інформація в автоматизованій системі (АС) перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.	*Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 р. № 81/94-ВР*
4	**Інформація** - відомості, подані у вигляді сигналів, знаків,	*Закон України «Про*

	звуків, рухомих або нерухомих зображень чи в інший спосіб.	*телекомунікації» від 18.11.03 р. № 1280-IV*
5	**Інформатизація** - сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки.	*Закон України «Про Національну програму інформатизації» від 04.02.98 р. № 74/98-ВР*
6	**Інформаційна система** - система оброблення даних засобами накопичення, зберігання, обновлення та їх пошуку і відображення.	*Постанова Кабінету Міністрів України «Про затвердження Концепції створення Єдиної державної автоматизованої паспортної системи» від 20.01.97 р. № 40*
7	**Інформаційний продукт** (продукція) - документована інформація, підготовлена і призначена для задоволення потреб користувачів.	*Закон України «Про Національну програму Інформатизації» від 04.02.98 р. № 74/98-ВР*
8	**Інформаційний ресурс** - сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).	*Закон України «Про Національну програму Інформатизації» від 04.02.98 р. № 74/98-ВР*
9	**Інформаційна послуга -** дії суб'єктів щодо забезпечення споживачів інформаційними продуктами.	*Закон України «Про Національну програму Інформатизації» від 04.02.98р.№ 74/98-ВР*
10	**Інформаційне суспільство** – суспільство з наступними головними прикметами: - створюється мережа взаємопов'язаних загальнодоступних для кожного громадянина банків знань і даних; - більшість трудящих зайняті у сфері послуг та виробництва інформації; - інформація стає товаром і поряд з інформаційною технологією займає ключове місце в економіці.	*Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.07 р. № 537-V*
11	**Електронний цифровий підпис** - вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.	*Закон України «Про електронний цифровий підпис» від 22.05.03 р. № 8'52-IV*
12	**Несанкціонований доступ** - доступ до інформації, що здійснюється з порушенням встановлених в автоматизованій системі правил розмежування доступу.	*Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 р. № 81/94-ВР*

13	**Обробка інформації** - вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін каналами передачі даних.	*Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 р. М 81/94-ВР*
14	**Оператор телекомунікацій** – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічне обслуговування та експлуатацію телекомунікаційних мереж;	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
15	**Особистий ключ** - параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.	*Закон України «Про електронний цифровий підпис» від 22.05.03 р. № 852-IV*
16	**Підробка інформації** - навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в автоматизованих системах (АС).	*Закон України «Про захист інформації в автоматизованих системах» від 05.07.94 р. № 81/94-ВР*
17	**Провайдер телекомунікацій** – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
18	**Ресурси телекомунікаційних мереж** - наявні в телекомунікаційних мережах кількість номерів (номерний ресурс), кількість і пропускна спроможність ліній з металевими жилами, оптичними волокнами, радіоліній, каналів, трактів для передавання інформації, комутаційних станцій та вузлів, радіочастотний ресурс.	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
19	**Споживач телекомунікаційних** послуг (споживач) - юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб.	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
20	**Суб'єкти ринку телекомунікацій** - оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій.	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
21	**Телекомунікації (електрозв'язок)** - передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводних, оптичних або інших електромагнітних системах.	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
22	**Телекомунікаційна мережа** - комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.	*Закон України «Про телекомунікації» від 18.11.03 р. № 1280-IV*
23	**Телекомунікаційна послуга** - продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері	*Закон України, «Про телекомунікації» від 18.11.03 р. № 1280-IV*

	телекомунікацій.	
24	**Шифрування** - перетворення електронного документа із застосуванням криптографічних методів з метою захисту його змісту.	*Закон «Про платіжні системи» від 05.04.01 р. № 2346-111*

1.3 Задачі менеджменту та функції управління інформаційною безпекою

Функції управління інформаційною безпекою. Управління інформаційною безпекою є частиною функцій інформаційної безпеки, які забезпечуються ієрархією послуг безпеки і механізмів безпеки.

Функції управління інформаційною безпекою включають послуги безпеки для комунікацій та інформаційних систем, виявлення подій безпеки і звітність.

Для безпеки комунікацій надаються послуги автентифікації, контролю доступу, конфіденційності даних, цілісності даних, невідмовності від (причетності до) отримання чи авторства у процесах комунікації між системами, між користувачами і системами, між внутрішніми споживачами та системами. Крім того, визначені скрізь проникаючі механізми безпеки для виявлення подій, контролю безпеки журналу аудиту, відновлення безпеки тощо.

Виявлення подій безпеки та повідомлення звітів вищим рівням безпеки – це діяльність щодо виявлення, аналізу і усунення інцидентів з порушення безпеки. Прикладом інциденту безпеки може бути виявлення неавторизованого користувача, фізичне пошкодження обладнання тощо.

Управління безпекою включає у себе такі групи функцій:

- попередження;
- виявлення;
- стримування та відновлення;
- адміністрування безпеки.

Набір функцій попередження необхідний для перешкоджання проникненню. У склад цього набору входять функції безпеки:

- забезпечення законного доступу до інформаційних ресурсів;
- забезпечення безпечного доступу фізичними засобами (біометричні, електронні системи доступу тощо);
- охорони об’єктів доступу;
- аналізу персонального ризику для перевірки надійності працівників;
- екранування безпеки користувачів для підтримки запитів на підтвердження надійності замовника послуги, наприклад платоспроможності.

Набір функцій виявлення вторгнень включає у себе функції безпеки:

- дослідження суттєвих змін у доходах, що можуть вказати на аферу або крадіжку;
- захист елементів підтримки типу моніторингу та аналізу аварійної сигналізації: пожежної, повені, відкривання дверей, вікон тощо;

- доступу замовників до інформації порушення безпеки у їхніх частинах мережі;

- аналізу та ідентифікації аномалій і нерегулярності у даних користувача, які можуть вказувати на вилом у захисті або крадіжку послуг;

- аналіз даних користувача, які характеризують його характерну поведінку;

- дослідження крадіжки службових послуг за даними його характерної поведінки;

- дослідження внутрішнього трафіку, даних характерної поведінки та інформації контрольного журналу для виявлення вилому у захисті або крадіжки послуг через дії персоналу;

- сигналізація безпеки мережі;

- аудит вторгнень програм, наприклад вірусів;

- підтримки звітів порушень елементів безпеки.

Набір функцій стримування та відновлення необхідні для відмови у доступі зловмиснику, ліквідування порушень, зроблених зловмисником, відновлення роботи системи захисту. У цей набір входять функції захисту:

- захищене зберігання ділових даних, даних замовника послуг, даних конфігурації мережі та кінцевих елементів мережі;

- підтримка запитів на звіти порушень безпеки і запитів на дії з обмеження чи ізоляції обладнання або даних, виключення прав доступу, а також запитів на відновлення спотворених даних чи обладнання;

- підтримка судових справ проти порушників та їх затримки;

- підтримки запитів до резервних файлів для відновлення послуг, конфігурації мережі, кінцевого елемента після виявлення порушення безпеки;

- адмініструванні списків відміни для доступу до списків всіх ключів та сертифікатів замовника послуг, конфігурації мережі, контролю доступу, які підозрюються у непрацездатності унаслідок порушення безпеки;

- підтримка запитів на роз’єднання зовнішніх чи внутрішніх зв’язків для спроби збереження даних чи системи за виявлення порушення безпеки;

Набір функцій адміністрування безпеки необхідні для планування та адміністрування політики безпеки та безпеки відносно ділової інформації. У цей набір входять функції захисту:

- політики безпеки, який забезпечують доступ до директив компанії для встановлення і підтримки безпечного середовища для персоналу, технічних засобів та програмного забезпечення;

- підтримки доступу до засобів і процедур, які використовуються для відновлення мережі та спотворених даних при події порушення безпеки;

- аналізу інформації контрольного журналу для ідентифікації можливих або потенційних порушень безпеки індивідуумами або групами користувачів;

- аналізу та оцінки порушень безпеки за допомогою директив моніторингу;

- оцінки цілісності корпоративних наборів даних для захисту від несанкціонованого доступу;

- адміністрування внутрішніх та зовнішніх запитів і відповідей ідентифікації, контролю доступу, видачі сертифікатів, кодування і ключів;

- управління порушенням безпеки замовника послуги для виявлення атаки на безпеку в його частині мережі;

- тестування механізмів контрольного журналу;

- управління журналом аудиту мережі, порушення безпеки мережі та кінцевих пунктів;

- адміністрування ключів та підтримки запитів на генерацію ключів, які використовуються у комунікаціях між кінцевими пунктами та іншими елементами мережі. Такі ключі можуть бути використані для ідентифікації, цілісності та конфіденційності.

На конкретному об'єкті інформаційної діяльності встановлюються сценарії послідовного використання функцій безпеки для виявлення, стримування та ліквідації порушень інформаційної безпеки

Контрольні запитання та завдання

1. Поясніть роль та значення інформаційної безпеки інформаційно-телекомунікаційних систем в інформаційному суспільстві.
2. Що розуміють під глобальною безпекою та який її зв'язок з економічною та національною безпекою?
3. Назвіть та поясніть складові частини глобальної безпеки.
4. Дайте визначення поняття «інформаційна безпека».
5. Які проблеми ускладнюють забезпечення інформаційної безпеки в умовах глобалізації?
6. Дайте визначення поняття «інформаційної безпеки» у вузькому й широкому розумінні.
7. Що називають захистом інформації?
8. Обґрунтуйте необхідність захисту інформації.
9. Що є основою рішень щодо вибору спеціальних рішень із захисту інформації.
10. Які організаційні заходи необхідні для захисту конфіденційної інформації?
11. Сформулюйте задачі менеджменту інформаційної безпеки.
12. Сформулюйте функції управління інформаційною безпекою.

Завдання до самостійної роботи

1. Проаналізуйте основні поняття інформаційної безпеки та їх зміст, користуючись як джерелом чинними нормативно-правовими документами сфери інформаційної безпеки.

РОЗДІЛ 2

ХАРАКТЕРИСТИКА СУЧАСНОЇ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ НОРМАТИВНОЇ БАЗИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Етапи розвитку нормативної бази у сфері інформаційної безпеки

Розвиток телекомунікаційних мереж проходить на фоні підвищення вимог з боку користувачів та держави до інформаційної безпеки поряд з вимогами до надійності функціонування зв'язку, сталості телекомунікаційних мереж та якості телекомунікаційних послуг. Зростає потреба у безпечних інформаційно-телекомунікаційних системах для забезпечення інформаційно-аналітичної діяльності державних установ та установ усіх форм власності, ефективного функціонування електронної інформаційної системи «Електронний уряд», систем електронно-цифрового підпису, електронного документообігу. Інформаційної безпека та сталість телекомунікаційних мереж є частиною задач захисту інформаційного простору України та державної політики у сфері зв'язку щодо забезпечення оборони, національної безпеки, охорони правопорядку.

Основи державної політики щодо безпеки України в інформаційній сфері визначені основоположним Законом "Про основи національної безпеки України" (від 19.06.2003 № 964-IV). Закон визначає основні засади гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз національним інтересам і національній безпеці України в усіх сферах життєдіяльності [58]. В інформаційній сфері виокремлено загрози:

- прояви обмеження свободи слова та доступу громадян до інформації;
- комп'ютерної злочинності та комп'ютерного тероризму;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Закон передбачає такі основні напрями державної політики з питань національної безпеки в інформаційній сфері:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидій монополізації інформаційної сфери України.

Розробляється низка нормативно-правових актів у сфері інформаційної безпеки та захисту інформаційно-телекомунікаційних систем. Інформаційна безпека телекомунікаційних мереж, як складової інформаційно-телекомунікаційних мереж, стала важливою техніко-економічною й політичною проблемою.

Розвиток нормативно-правової бази стосовно інформаційної безпеки інформаційно-телекомунікаційних систем можна поділити на ряд етапів.

Перший етап започатковано в 1992 – 1996 рр. Законами України "Про інформацію" (від 02.10.92 р), "Про державну таємницю" (від 21.01.94 р.), "Про науково-технічну інформацію" (від 25.06.93 р.). Разом з угодами з країнами СНГ щодо взаємного захисту інформації, яка становить державні таємниці, дані закони дозволили організувати чітку систему захисту інформації, використовуючи низку нормативних документів колишнього СРСР.

Захист інформаційної системи, згідно із Законом України "Про інформацію", є обов'язком її власника. Власники інформаційних систем можуть делегувати свої повноваження із захисту окремим користувачам-адміністраторам чи постачальникам послуг. Проте власники все одно несуть відповідальність щодо забезпечення безпеки системи [52].

Першим документом стосовно інформаційно-телекомунікаційних систем на першому етапі є прийнятий 05.07.94 р. Закон України "Про захист інформації в автоматизованих системах". Мережі з автоматичними програмно-керованими телефонними станціями та автоматичною комутацією можуть класифікуватись як автоматизовані системи. Законом означені загальні вимоги щодо захисту інформації, політика в галузі захисту інформації, служба захисту інформації, тощо. За цим задачі захисту інформації в галузі зв'язку конкретизувались Законом України "Про зв'язок", (від 16.05.95 р.), що діяв до 2003 р. Перший етап завершується стандартизацією положень технічного захисту інформації в ДСТУ 3396.0-96, ДСТУ 3396.1-96, ДСТУ 3396.2-97.

Другий етап розвитку нормативно-правової бази розпочатий затвердженням Кабінетом Міністрів України 8 жовтня 1997 р. постанови № 1126 про "Концепцію технічного захисту України". Відповідно, в галузі телекомунікацій приймається "Концепція технічного захисту інформації в галузі зв'язку України» (від 24.09.1999 р.).

Згідно цих концепцій в Україні започатковується система технічного захисту інформації (ТЗІ) і на підприємствах будь-якої форми власності утворюються підрозділи ТЗІ. В Укртелекомі були утворені регіональні центри ТЗІ, а в кожній дирекції ВАТ "Укртелеком" – групи ТЗІ.

На протязі другого етапу спостерігався бурхливий розвиток нормативно-правової бази системи технічного захисту інформації. Створені пакет нормативних документів щодо захисту інформації в комп'ютерних та автоматизованих системах від несанкціонованого доступу, пакет нормативних документів щодо технічного захисту інформації в програмно-керованих АТС загального користування. В цей же період стали активно діяти ряд підприємств із виготовлення засобів захисту інформації, захищених комп'ютерів ("Плутон",

“Плазма-3В”, ЕОМ-П тощо), програмно-апаратних комплексів захисту інформації від несанкціонованого доступу (“Гриф”, “Інспектор”, “АІС”, тощо).

Третій етап розвитку нормативно-правової бази ініційований низкою Указів Президента України “Про заходи щодо розвитку національної складової глобальної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні” від 31.07.2000 р. № 928 і вінчається постановою Кабінету Міністрів України № 208 від 24 лютого 2003 р. “Про заходи щодо створення електронної інформаційної системи “Електронний Уряд”. Характерним для цього періоду є розширення об’єкту захисту – захистові підлягає не тільки державна таємниця і конфіденційна інформація, що належить державі, а й відкрита інформація. Об’єктом технічного захисту на програмно-керованих АТС, а також на відомчих (корпоративних) АТС є конфіденційна, а також відкрита важлива для особи, суспільства і держави інформація, яка зберігається та циркулює на цих АТС. Указом Президента України передбачено:

- вирішення задач щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства;

- посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів всіх форм власності, за навмисне поширення комп’ютерних вірусів.

Одночасно видані Укази Президента України “Про заходи щодо захисту інформаційних ресурсів держави” від 10 квітня 2000 р. № 582 та “Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних” від 24 вересня 2001 р. № 891. Державному комітету зв’язку та інформатизації України доручено визначити, в установленому законодавством порядку, підприємства (операторів), що здатні забезпечити передачу органами виконавчої влади, іншими органами даних глобальними мережами з додержанням установлених законодавством вимог щодо захисту інформації.

На виконання Указів Президента наказом ДСТЗІ СБ України № 76 від 24 грудня 2001 р. затверджено “Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах”, де викладено основи організації та порядок захисту державних інформаційних ресурсів в мережі передавання даних (МПД).

Відповідно до п.п 12-20 цього Порядку оператори повинні забезпечувати створення, упровадження та супроводження на кожному з вузлів комутації МПД *комплексної системи захисту інформації (КСЗІ)*, яка є сукупністю технічних, криптографічних, організаційних та інших заходів і засобів захисту, спрямованих на недопущення блокування та/або модифікування інформації під час її передавання МПД. Захисту підлягають державні інформаційні ресурси, інформація користувачів, яка передається мережею незалежно від способу її фізичного та логічного представлення, технологічна інформація та інформація бази даних захисту (*security management information base − SMIB*) самої КСЗІ.

При цьому, здійснення заходів щодо забезпечення *конфіденційності державних інформаційних ресурсів* та захист від несанкціонованого доступу до них в автоматизованих системах покладається не на оператора, а на

користувачів МПД. Згідно з чинним законодавством, створення переліку вимог, сертифікацію й атестацію систем шифрування покладено на відповідний уповноважений орган виконавчої влади. Ця діяльність регламентується нормативним документом "Положення про порядок здійснення криптографічного захисту інформації в Україні".

Вимоги щодо захисту інформації в МПД полягають у наступному:

- КСЗІ має регламентувати порядок опрацювання інформації користувачів МПД, технологічної інформації, що формується в МПД, та інформації бази даних захисту КСЗІ;
- в мережах загального користування має виключатися можливість несанкціонованого копіювання та зберігання інформації користувачів;
- має забезпечуватись *конфіденційність* інформаційної бази захисту КСЗІ та технологічної інформації МПД;
- КСЗІ МПД має забезпечувати *цілісність* інформації, яка передається мережею, шляхом забезпечення доступу до неї лише персоналу МПД у відповідності із встановленими функціональними повноваженнями, а також впровадженням механізмів та процедур виявлення фактів порушення цілісності зазначеної інформації, її вилучання чи копіювання;
- КСЗІ МПД має вести облік і здійснювати реєстрування подій, які пов'язані із спробами доступу до інформації, здійснювати періодичний контроль за такими подіями та забезпечувати захист реєстраційної інформації від несанкціонованого модифікування, руйнування чи знищення. Обсяг реєстраційної інформації має бути достатнім для встановлення причин та джерела виникнення зареєстрованої події;
- послуги МПД мають надаватись лише зареєстрованим користувачам за умови їхнього достовірного розпізнавання;
- взаємодія вузлів комутації МПД з метою передавання інформації поміж ними може здійснюватися після достовірного взаємного розпізнавання;
- КСЗІ повинна мати можливість контролювати цілісність власного складу та окремих програмно-технічних компонентів;
- має забезпечуватись можливість однозначного встановлення належності інформації, яка передається МПД, певному користувачеві;
- має забезпечуватись можливість встановлення факту передавання чи одержання оператором чи користувачем певної інформації;
- повинне унеможливлюватися несанкціоноване чи неконтрольоване використання користувачами ресурсів МПД;
- критичні, з точки зору безпеки, компоненти КСЗІ мають резервуватися, з тим, аби їхня відмова не призводила до переривання процесу надавання послуг;
- у разі виникнення відмов, які порушують функціонування КСЗІ, надавання вузлом послуг користувачам має бути призупинене.

Важливим є положення про те, що: *передавання державних інформаційних ресурсів дозволяється лише через вузли комутації, що мають атестат відповідності КСЗІ вимогам із захисту інформації, який надається за результатами державної експертизи в сфері технічного захисту інформації.*

На протязі третього етапу введені в дію нормативні документи щодо

вимог до захисту інформації в локальних обчислювальних мережах і в Інтернет [122, 123].

Характерним є все більший наголос на захисті відкритої інформації.

Приміром, комплексна система захисту інформації має забезпечувати реалізацію *вимог із захисту цілісності та доступності розміщеної на WEB-сторінці загальнодоступної інформації, а також конфіденційності та цілісності технологічної інформації WEB-сторінки* [123].

Для розв'язання завдань захисту інформації в інфокомунікаціях України стали актуальними також рекомендації ITU X.800 "Архітектура безпеки ВВС", ISO/SEC 10181 "Основні положення безпеки відкритих систем" [218, 217].

Теоретичні положення і теореми щодо інформаційної безпеки є досить складними, а деякі з них залишаються засекреченими. Тому результати теоретичних досліджень і аналізу практики побудови систем інформаційної безпеки прийнято викладати у вигляді стандартів. Стандарти містять основні практичні правила, вичерпний набір засобів управління інформаційною безпекою та процедури забезпечення інформаційної безпеки. Стосовно управління інформаційною безпекою найбільш відомим є британський стандарт BS 7799 "Практичні правила управління інформаційною безпекою". Стандарт розроблений як керівництво і рекомендації. Набір засобів управління безпекою заснований на реальних заходах захисту інформації.

Розширення сфери дії інформаційних технологій потребує перегляду підходів до інформаційної безпеки. Загальні принципи побудови й експлуатації безпечних інформаційних технологій окреслюються за допомогою базової технічної моделі забезпечення безпеки інформаційних технологій (позначається як модель IT-безпеки). Така модель впроваджується міжнародним стандартом ISO/IEC 15408 "Єдині критерії оцінювання безпеки інформаційних технологій" і визначає принципово нову технологію створення систем IT-безпеки на підставі розробляння профілю захисту та проекту безпеки.

Четвертий етап розвитку нормативно-правової бази ознаменувався прийняттям Закону "Про телекомунікації". Інформаційна безпека телекомунікаційних мереж визначається законом як здатність телекомунікаційних мереж забезпечувати захист від знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку її маршрутизації.

Закон "Про телекомунікації" визначає основні ключові завдання інформаційної безпеки телекомунікаційних мереж, основні засоби їх виконання та відповідальність суб'єктів інформаційних відносин щодо забезпечення інформаційної безпеки [61].

Ключові завдання інформаційної безпеки телекомунікаційних мереж поділяються на такі групи: захист інформації з обмеженим доступом, що є власністю держави; захист державних інформаційних ресурсів; охорона таємниці телефонних розмов, телеграфної, іншої кореспонденції та захист інформації про споживача; захист інформації, що передається телекомунікаційними мережами; забезпечення безпеки мереж телекомунікацій та безпеки телекомунікаційних послуг.

Інформаційна безпека мереж зв'язку Єдиної національної системи зв'язку і захищеність інформації споживачів неможлива без комплексного науково обґрунтованого підходу до їх забезпечення та врахування низки технологічних та експлуатаційних характеристик засобів телекомунікацій:

- сталості та надійності телекомунікаційної мережі, де сталість розуміється як властивість телекомунікаційної мережі зберігати повністю або частково свої функції за умови впливу дестабілізуючих чинників;
- технологічної цілісності всіх мереж та засобів телекомунікацій;
- безпеки, якості та своєчасності отримання телекомунікаційних послуг, тобто показників, які в узагальненому вигляді входять у поняття цілісності та доступності;
- показники доставки інформації споживачеві, які в узагальненому вигляді входять у показники доступності та частково в показники конфіденційності та цілісності;
- критеріїв безпеки мереж телекомунікацій, що мають враховуватись при виборі засобів телекомунікацій, які можуть застосовуватись в телекомунікаційних мережах;
- контролю за додержанням стандартів та нормативних актів у сфері телекомунікацій.

Закон вимагає застосовувати в телекомунікаційних мережах лише такі засоби телекомунікацій, які мають підтвердження відповідності чинним нормативним документам у сфері телекомунікацій та технічним регламентам, критеріям забезпечення надійності, безпеки мереж телекомунікацій.

В Україні прийнята та діє Концепція технічного захисту інформації в Україні (постанова Кабінету Міністрів України від 08.10.97 № 1126). Але ця концепція відноситься та охоплює тільки питання технічного захисту інформації, не враховуючи усі аспекти інформаційної безпеки. Крім того, Концепція була створена 9 років назад. З огляду на високі темпи розвитку інформаційних технологій, вона потребує переогляду.

П'ятий етап – є етапом розвитку нормативно-правової бази захисту інформаційних ресурсів в усіх видах державної, комерційної та персональної інформації в інформаційно-телекомунікаційних системах та інформаційному просторі України. Серед інфраструктури комунікацій телекомунікаційні мережі є найбільш критично важливими для безпеки суспільства та держави. Інформаційній безпеці інформаційно-телекомунікаційних мереж в Україні приділяється все більша увага. Термін «автоматизована система» замінюється на термін «інформаційно-телекомунікаційна система».

Інформаційна (автоматизована) система – це організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Телекомунікаційна система – це сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформаційно-телекомунікаційна система – це сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Під термінами «інформаційно-комунікаційна система» (так у назві спеціальності) й «інформаційно-телекомунікаційна система» (так у більшості нормативно-правових документів) ми будемо розуміти одне й те ж саме.

На даному етапі вступають в дію Закон та Правила забезпечення захисту інформації в інформаційно-телекомунікаційних системах [62], а також Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [145].

У Документі: «ПРАВИЛА забезпечення захисту інформації *в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», встановлюється, що захисту в системі підлягає* [62]:

а) відкрита інформація, яка є власністю держави і у визначенні Закону України "Про інформацію" належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами;

б) конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, у тому числі конфіденційна інформація про фізичну особу;

в) інформація, що становить державну або іншу передбачену законом таємницю.

Відкрита інформація під час обробки в системі *повинна зберігати цілісність*, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або навмисної модифікації чи знищення.

Усім користувачам *повинен бути забезпечений доступ до ознайомлення з відкритою інформацією*. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження. Спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора блокуються.

Під час обробки *конфіденційної і таємної інформації повинен забезпечуватися її захист від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення*.

Доступ до конфіденційної інформації надається тільки ідентифікованим та автентифікованим користувачам. Спроби доступу до такої інформації неідентифікованих осіб чи користувачів з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора блокуються.

У системі забезпечується можливість надання користувачеві права на виконання однієї або кількох операцій з обробки конфіденційної інформації або позбавлення його такого права.

Вимоги до захисту в системі інформації від несанкціонованого блокування визначаються її власником (розпорядником), якщо інше для цієї інформації або системи, в якій вона обробляється, не встановлено законодавством.

У системі здійснюється обов'язкова реєстрація:

- результатів ідентифікації та автентифікації користувачів;
- результатів виконання користувачем операцій з обробки інформації;
- спроб несанкціонованих дій з інформацією;
- фактів надання та позбавлення користувачів права доступу до інформації та її обробки;
- результатів перевірки цілісності засобів захисту інформації.

Забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратором безпеки). Реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки.

Ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом.

Передача конфіденційної і таємної інформації з однієї системи до іншої здійснюється у зашифрованому вигляді або захищеними каналами зв'язку згідно з вимогами законодавства з питань технічного та криптографічного захисту інформації.

У системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється.

Значна увага продовжує приділятись захисту комерційної інформації та персональної інформації, яка зберігається в базах даних інформаційних систем. Низка важливих міжнародних стандартів прийняті як державні стандарти України методом обкладинки [39…47]. Тобто ці міжнародні стандарти переведені на українську мову і введені як обов'язкові для виконання на території України. Їх впровадження дає змогу бізнесу отримувати міжнародні сертифікати на побудовані системи інформаційної безпеки.

2.2 Звід та характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки

Характеристика основної сучасної національної та міжнародної нормативної бази в галузі інформаційної безпеки наведена у табл. 2.1.

Нині процес інформаційного розвитку в Україні значною мірою обумовлений недосконалістю законодавчої бази, що його регулює, та

пов’язаний із вирішенням таких проблем, як різноплановість нормативно-законодавчого регулювання суспільних відносин в інформаційній сфері; відсутність, неузгодженість, суперечливість, неповнота законодавчих і нормативних (підзаконних) актів у сфері телекомунікацій, використання Інтернет-технологій, створення та використання електронних інформаційних ресурсів і продуктів, впровадження електронного документообігу й електронного цифрового підпису, інформаційної безпеки і захисту інформації тощо.

Ефективне функціонування сучасної економіки, побудованої на знаннях, можливе лише в умовах існування належної нормативно-правової бази, а це потребує прийняття пакету законів України, зокрема про діяльність у сфері інформатизації, захисту персональних даних, внесення змін до деяких законодавчих актів України (щодо боротьби з комп’ютерною злочинністю).

Чинні Закони України, зокрема Закони "Про інформацію", "Про захист інформації в автоматизованих системах", "Про захист інформації в інформаційно-комунікаційних системах", "Про Національну програму інформатизації”, "Про електронні документи та електронний документообіг", "Про електронний цифровий підпис" тощо не можуть забезпечити всебічне та повне врегулювання усіх правовідносин, що виникають у сфері інформатизації, оскільки їхня дія не поширюється на аспекти та умови, які виникають унаслідок постійних технологічних змін, що значно впливають і на суспільні відносини.

Таблиця 2.1 – Звід основної сучасної національної та міжнародної нормативної бази в галузі інформаційної безпеки

№	Дата прийняття і номер	Назва нормативно-правового акту
ЗАКОНИ УКРАЇНИ		
1	02.10.1992 р. № 2657-XII	**Закон України** “Про інформацію”
2	21.09.1999 р. № 1079-XIV.	**Закон України** “Про державну таємницю”
3	5.06.1994 № 81/94-ВР	**Закон України** “Про захист інформації у автоматизованих системах”
4	10.01.2002 р. № 2919-III	**Закон України** “Про Національну систему конфіденційного зв’язку”
5	18.11.03 р. № 1280-IV.	**Закон України** „Про телекомунікації”
6	04.02.1998 р. № 74/98-ВР	**Закон України** “Про Національну програму інформатизації”
7	25.03.1992р. № 2229-XII	**Закон України** “Про Службу безпеки України”
8	10.02.1995 № 51/95-ВР.	**Закон України** “Про наукову та науково-технічну діяльність”
9	01.06.2000 р.	**Закон України** “Про ліцензування певних видів господарської діяльності”
10	4.02. 1998 р.	**Закон України** „Про Концепцію Національної програми

	№ 75/98-ВР	інформатизації”
11	21.01.1994 р. № 3855-XII	**Закон України** „Про державну таємницю”
12	22.05.2003 р. № 851-IV.	**Закон України** „Про електронні документи та електронний документообіг”
13	22.05.2003 р. № 852- IV.	**Закон України** „Про електронний цифровий підпис”
14	31.05.2005 р. № 2594-IV	**Закон України** “Про захист інформації в інформаційно-телекомунікаційних системах”
15	19.06.03 р. № 964-IV.	**Закон України** „Про основи національної безпеки України”
16	09.01.07 р. № 537-V	**Закон України** «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки»
УКАЗИ ПРЕЗИДЕНТА УКРАЇНИ		
1	22.04. 1998 р. № 346	Про деякі заходи щодо захисту інтересів держави в інформаційній сфері
2	22.05. 1998 р. № 505	Положення про порядок здійснення криптографічного захисту інформації в Україні
3	27.09.1999 р. № 1229	Положення про технічний захист інформації в Україні
4	11.02.1998 р. № 110/98.	Про заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних та інформаційних системах
5	10.04 2000 р. № 582	Про заходи щодо захисту інформаційних ресурсів держави
6	06.10 2000 р. № 1120	Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби Безпеки України
7	24.09.2001 р. № 891	Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних
ПОСТАНОВИ КАБІНЕТУ МІНІСТРІВ УКРАЇНИ		
1	26.06.1996 № 677	Порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації
2	02.02.1997 №180	Положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах
3	08.10.199 № 1126.	Концепція технічного захисту інформації в Україні
4	04.02. 1998 № 121	Перелік обов’язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних
5	27.11.1998 р. № 1893	Інструкція про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави
6	04.01. 2002 р. № 3	Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади
7	–	Концепція розвитку телекомунікацій в Україні до 2010 року.
8	24.09.1999	Концепція технічного захисту інформації в галузі зв’язку України.

НАКАЗИ ДЕПАРТАМЕНТУ СПЕЦІАЛЬНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА ЗАХИСТУ ІНФОРМАЦІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ ТА ІНШИХ ВІДОМСТВ		
1	22.12.1999 № 61	Положення про контроль за функціонуванням системи технічного захисту інформації
2	01.03.2001 р. № 52	Звід відомостей, що становлять державну таємницю
3	24.12.2001 р. № 76	Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах
4	23.02.2002 р. № 9	Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб
ДЕРЖАВНІ СТАНДАРТИ УКРАЇНИ		
1	ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення	
2	ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт.	
3	ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення	
4	ДСТУ ISO/IEC TR 13335-1-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Ч. 1. Концепції і моделі безпеки (IT/ISO/IEC TR 13335-1:1996)	
5	ДСТУ ISO/IEC TR 13335-2-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Ч. 2. Керування та планування безпеки (IT/ISO/IEC TR 13335-2:1997)	
6	ДСТУ ISO/IEC TR 13335-3-2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Ч. 3. Методи керування захистом (IT/ISO/IEC TR 13335-3:1998)	
7	ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту (ISO/IEC TR 13335-4:2000)	
8	ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою (ISO/IEC TR 13335-5:2001)	
НОРМАТИВНІ ДОКУМЕНТИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ		
1	НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп’ютерних системах від несанкціонованого доступу	
2	НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу	
3	НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі	
4	НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення	
5	НД ТЗІ 2.5-004-99. Критерії захищеності інформації комп’ютерних системах від несанкціонованого доступу	
6	НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу	
7	НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання та створення комплексної системи захисту інформації в автоматизованій системі	

8	НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження і модернізації засобів технічного захисту інформації від несанкціонованого доступу.
9	НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення.
10	НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту.
11	НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту.
12	НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту.
13	НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт.
14	НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова).
МІЖНАРОДНІ ДОКУМЕНТИ, ЯКІ ФОРМІРУЮТЬ СУЧАСНУ МЕТОДОЛОГІЧНУ ТА ТЕХНОЛОГІЧНУ ОСНОВУ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ІТС	
1	ISO/IEC 74982 – Архитектура безопасности ВОС.
2	ISO/IEC 10181 – Архитектура безопасности открытых систем.
3	ISO/IEC 13335:2000 – Управление безопасностью.
4	ISO/IEC 17799:2000 – Практические правила обеспечения безопасности информации (кодекс лучшей практики).
5	ISO/IEC 21847 – Инжиниринг систем безопасности. Модель зрелости системы обеспечения безопасности.
6	ISO/IEC 15408 – Общие Критерии оценки защищенности систем информационных технологий.
7	ISO/IEC 7498-2 – Архитектура безопасности ВОС.
8	ISO/IEC 10181 – Архитектура безопасности открытых систем.
9	ISO/IEC 13335 – Управление безопасностью.
10	ISO/IEC 17799 – Практические правила обеспечения безопасности информации (кодекс лучшей практики).
11	ITU-T Recommendation X.200. Reference model of open systems interconnection for CCITT applications. – Geneva, 1991. – 75 с.
12	ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. – Geneva, 1991. – 48 с.
13	ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. – Geneva, 1991. – 28 с.

Таким чином, серед основних проблем у сфері інформаційної безпеки слід назвати недостатня захищеність інформації на законодавчому рівні.

Контрольні запитання та завдання

1. Які загрози в інформаційній сфері виокремлені у Законі України «Про основи національної безпеки України»?
2. Поясніть основні напрями державної політики з питань національної безпеки в інформаційній сфері.
3. Чим характерні кожен з етапів розвитку нормативно-правової бази у сфері інформаційної безпеки?
4. Якими нормативно-правовими документами передбачається захист відкритої інформації, важливої для особи, суспільства та держави?
5. Які складові інформаційної безпеки телекомунікаційних мереж передбачаються Законом України «Про телекомунікації»?
6. Прокоментуйте вимоги до інформаційної безпеки у мережах передавання даних.
7. Яка інформація підлягає захисту у інформаційно-телекомунікаційних системах?
8. Сформулюйте вимоги до захисту відкритої інформації у інформаційно-телекомунікаційних системах.
9. Для чого у системі здійснюється обов’язкова реєстрація подій з інформаційною безпекою і що реєструється?

10 Як здійснюється контроль за цілісністю програмного забезпечення?

Завдання до самостійної роботи

1. Проаналізуйте сучасну національну та міжнародну нормативну базу в галузі інформаційної безпеки інформаційно-телекомунікаційних систем на повноту і достатність для вирішення сучасних задач забезпечення інформаційної безпеки.
2. Проаналізуйте вимоги до інформаційної безпеки та комплексної системи захисту інформації у мережах передавання даних.

РОЗДІЛ 3

ОСНОВНІ ЦІЛІ ТА ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Основні цілі і завдання забезпечення інформаційної безпеки

Основні цілі забезпечення інформаційної безпеки визначаються на базі стійких пріоритетів національної безпеки, що відповідають довготривалим інтересам суспільного розвитку, до яких відносяться [103]:

- збереження і зміцнення української державності і політичної стабільності в суспільстві;
- збереження і розвиток демократичних інститутів суспільства, забезпечення прав і свобод громадян, зміцнення законності і правопорядку;
- забезпечення гідної ролі України в світовій спільноті;
- забезпечення територіальної цілісності країни;
- забезпечення прогресивного соціально-економічного розвитку України;
- збереження національних культурних цінностей і традицій.

Відповідно до вказаних пріоритетів основними цілями інформаційної безпеки є:

- захист національних інтересів України в умовах глобалізації інформаційних процесів, формування світових інформаційних мереж і прагнення США та інших розвинених країн до інформаційного домінування;
- забезпечення органів державної влади і управління, підприємств і громадян достовірною, повною і своєчасною інформацією, необхідною для ухвалення рішень, а також запобігання порушенням цілісності і незаконного використання інформаційних ресурсів;
- реалізація прав громадян організацій і держави на здобуття, поширення і використання інформації.

До основних завдань забезпечення інформаційної безпеки відносяться [103]:

- виявлення, оцінка і прогнозування джерел загроз інформаційній безпеці;
- розробка державної політики забезпечення інформаційної безпеки, комплексу заходів і механізмів її реалізації;
- розробка нормативно-правової бази забезпечення інформаційної безпеки, координація діяльності органів державної влади й управління та підприємств по забезпеченню інформаційної безпеки;
- розвиток системи забезпечення інформаційної безпеки, вдосконалення її організації, форм, методів і засобів запобігання, парирування і нейтралізації загроз інформаційній безпеці і ліквідації наслідків її порушення;
- забезпечення активної участі України в процесах створення і використання глобальних інформаційних мереж і систем.

Цілями інформаційної безпеки є забезпечення безперебійної роботи організації і зведення до мінімуму збитку від подій, що таять загрозу безпеці,

за допомогою їх запобігання і зведення наслідків до мінімуму. Управління інформаційною безпекою дозволяє колективно використовувати інформацію, забезпечуючи при цьому її захист і захист обчислювальних ресурсів. Інформаційна безпека включає три основних компонента: конфіденційність (захист конфіденційної інформації від несанкціонованого розкриття або перехоплення), цілісність (забезпечення точності і повноти інформації і комп'ютерних програм), доступність (забезпечення доступності інформації і життєво важливих послуг для користувачів, коли це потрібно).

Інформація існує в різних формах. Її можна зберігати на комп'ютерах, передавати обчислювальними мережами, роздруковувати або записувати на папері, а також озвучувати в розмовах. З точки зору безпеки всі види носіїв інформації (паперова документація, плівки, мікрофільми, моделі, магнітні стрічки, дискети, розмови тощо), які використані для передачі знань і ідей, вимагають належного захисту.

Інформація та що підтримують її інформаційні системи і мережі є коштовними виробничими ресурсами. Міра їх доступності, цілісність і конфіденційність можуть мати особливе значення для забезпечення конкурентоспроможності, руху грошової готівки, рентабельності, відповідності правовим нормам та іміджу організації. Власники інформації можуть зіткнутися із зростаючою загрозою порушення режиму безпеки, витікаючої від цілого ряду джерел. Інформаційним системам і мережам можуть загрожувати такі небезпеки, як комп'ютерні віруси і хакери, а також інші джерела відмов і аварій. Передбачається, що такі загрози інформаційній безпеці з часом стануть поширенішими, небезпечнішими і витонченішими. В той же час зростаюча залежність власників інформації від інформаційних систем і послуг робить її безпеку більш уразливого по відношенню до загроз порушення захисту. З поширенням обчислювальних мереж надаються нові можливості для несанкціонованого доступу до комп'ютерних систем, а тенденція до переходу на розподілені обчислювальні системи зменшує можливість централізованого контролю інформаційних систем фахівцями. Захисні заходи виявляються значно дешевшими і ефективнішими, якщо вони вбудовані в інформаційні системи і послуги на стадіях завдання вимог по їх проектуванню. Чим швидше будуть прийняті заходи щодо захисту своїх інформаційних систем, тим дешевше і ефективніше вони будуть для неї згодом.

Аналіз стану справ в області інформаційної безпеки показує, що у ряді розвинених держав склалася і успішно функціонує сповна стала інфраструктура системи інформаційної безпеки (СІБ), тобто системи заходів, що забезпечує такий стан конфіденційної інформації, за якого виключаються її розголошування, витік, несанкціонований доступ (зовнішні загрози), а також спотворення, модифікація, втрата (внутрішні загрози).

Проте зловмисні дії над інформацією не лише не скорочуються, а мають досить стійку тенденцію до зростання. Досвід показує, що для успішної протидії цій тенденції необхідно постійно вдосконалювати системи захисту.

Оскільки інформація є продуктом інформаційної системи (ІС), тобто організаційно-впорядкованої сукупності інформаційних ресурсів,

технологічних засобів, що реалізують інформаційні процеси в традиційному або автоматизованому режимах для задоволення інформаційних потреб користувачів, то матеріальними об'єктами інформаційної безпеки є елементи таких ІС, як споживачі та персонал; матеріально-технічні засоби (МТС) інформатизації; інформаційні ресурси (ІР) з обмеженим доступом.

До об'єктів інформаційної безпеки України відносять:

- інформаційні ресурси, незалежно від форм зберігання, що містять інформацію, що складає державну таємницю і обмеженого доступу, комерційну таємницю і обмеженого доступу, комерційну таємницю і іншу конфіденційну інформацію, а також відкриту (загальнодоступну) інформацію і знання;
- систему формування, поширення і використання інформаційних ресурсів, що включає інформаційні системи різного класу і призначення, бібліотеки архіви, бази і банки даних, інформаційні технології, регламенти і процедури збору, обробки, зберігання і передачі інформації, науково-технічний і обслуговуючий персонал;
- інформаційну інфраструктуру, що включає центри обробки і аналізу інформації, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж, зокрема системи і засоби захисту інформації;
- систему формування суспільної свідомості (світогляд, політичні погляди, моральні цінності тощо), що базується на засобах масової інформації і пропаганди;
- права громадян, юридичних осіб і держави на здобуття поширення і використання інформації, захист конфіденційної інформації і інтелектуальної власності.

Інформаційна безпека всіх вищезгаданих об'єктів створює умови надійного функціонування державних і суспільних інститутів, а також формування суспільної свідомості, що відповідає прогресивному розвитку країни.

У сфері інформаційної безпеки головне відзначити наступне:

- об'єктом захисту стає не просто інформація як якісь відомості, а інформаційний ресурс, тобто інформація на матеріальних носіях (документи, бази даних, патенти, технічна документація і так далі), право на доступ до якої юридично закріплене за її власником і їм же регулюється;
- інформаційна безпека користувачів на відміну від фізичної забезпечує захищеність їх прав на доступ до ІР для задоволення своїх інформаційних потреб;
- з точки зору економічної доцільності захищати слід лише ту інформацію, розголошування (витік, втрата і.т.д.) якої неминуче приведе до матеріального і морального збитку.

3.2 Джерела загроз та засоби їх впливу на об'єкти інформаційної безпеки

Джерела загроз інформаційній безпеці можна поділити на зовнішні і внутрішні [103].

До зовнішніх джерел відносяться:

- недружня політика іноземної держави в області глобального інформаційного моніторингу, поширення інформації і нових інформаційних технологій;
- діяльність іноземних розвідувальних і спеціальних служб;
- діяльність іноземних політичних і економічних структур, направлена проти інтересів держави; злочинні дії міжнародних груп, формувань і окремих осіб;
- стихійні лиха і катастрофи.

До внутрішніх джерел відносяться:

- протизаконна діяльність політичних і економічних структур в області формування, поширення і використання інформації;
- неправомірні дії державних структур, що приводять до порушення законних прав громадян і організацій в інформаційній сфері;
- порушення встановлених регламентів збору, обробки і передачі інформації; навмисні дії і неумисні помилки персоналу інформаційних систем; відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах.

Засоби дії загроз на об'єкти інформаційної безпеки поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові [103].

До інформаційних засобів відносяться:

- порушення адресності і своєчасності інформаційного обміну, протизаконний збір і використання інформації;
- несанкціонований доступ до інформаційних ресурсів;
- маніпулювання інформацією (дезинформація, приховання або спотворення інформації);
- незаконне копіювання даних в інформаційних системах;
- використання засобів масової інформації з позицій, що суперечать інтересам громадян, організацій і держав, розкрадання інформації з бібліотек, архівів, банків і баз даних; порушення технології обробки інформації.

Програмно-математичні засоби включають:

- впровадження програм-вірусів;
- установку програмних і апаратних закладних пристроїв;
- знищення або модифікацію даних в інформаційних системах.

Фізичні засоби включають:

- знищення або руйнування засобів обробки інформації і зв'язку; знищення, руйнування або розкрадання машинних або інших оригіналів носіїв інформації;

- розкрадання програмних або апаратних ключів і засобів криптографічного захисту інформації;

- дія на персонал; постачання «заражених» компонентів інформаційних систем.

Радіоелектронними засобами є:

- перехоплення інформації в технічних каналах її витоку;

- впровадження електронних пристроїв перехоплення інформації в технічних засобах і приміщеннях;

- перехоплення, дешифровка і нав'язування помилкової інформації в мережах передачі даних і лініях зв'язку;

- дія на парольно-ключові системи; радіоелектронне придушення ліній зв'язку і систем управління.

Організаційно-правові засоби включають:

- закупівлю недосконалих або застарілих інформаційних технологій і засобів інформатизації;

- невиконання вимог законодавства і затримки в прийнятті необхідних нормативно-правових положень в інформаційній сфері;

- неправомірне обмеження доступу до документів, що містять важливу для громадян і організацій інформацію.

Можливі наслідки дії загроз інформаційній безпеці України.

В результаті дії загроз інформаційній безпеці може бути завдано серйозного збитку життєво важливим інтересам України в політичній, економічній, оборонній та інших сферах діяльності держави, заподіяний соціально-економічний збиток суспільству і окремим громадянам.

Наслідком такої дії можуть бути: створення перешкод на шляху рівноправної співпраці України з розвиненими країнами і дружніми державами; скрута прийняття найважливіших політичних, економічних і інших рішень; підривання державного авторитету України на міжнародній арені; створення атмосфери напруженості і політичної нестабільності в суспільстві; порушення балансу інтересів особи, суспільства і держави; дискредитація органів державної влади і управління; провокація соціальних, національних і релігійних конфліктів; ініціація страйків і масових безладів; порушення функціонування систем державного управління, а також систем управління військами, озброєнням і військовою технікою, об'єктами підвищеної небезпеки.

Наслідком такої дії загроз можуть бути зниження темпів науково-технічного розвитку країни, втрата культурної спадщини, прояви бездуховності і аморальності. Вельми істотний економічний збиток в різних сферах суспільного життя і в сфері бізнесу може бути причинний в результаті порушень законодавства в інформаційній сфері і комп'ютерних злочинів.

Загрози інформаційній безпеці можуть завдати фізичного, матеріального і морального збитку громадянам, викликати неадекватну соціальну або кримінальну поведінку груп людей або окремих осіб, здійснити вплив на процеси освіти і формування особи.

В цілях запобігання, парирування і нейтралізації загроз інформаційній безпеці застосовуються базові методи. До них відносяться правові, програмно-технічні й організаційно-економічні методи.

Правові методи передбачають розробку комплексу нормативно-правових актів і положень, що регламентують інформаційні стосунки в суспільстві, керівних і нормативно-методичних документів по забезпеченню інформаційної безпеки.

Програмно-технічні методи включають запобігання просочуванню оброблюваної інформації шляхом виключення несанкціонованого доступу до неї; запобігання спеціальним діям, що викликають руйнування, знищення, спотворення інформації або збої в роботі засобів інформатизації; виявлення упроваджених програмних або апаратних закладних пристроїв; виключення перехоплення інформації технічними засобами; вживання криптографічних засобів захисту інформації при передачі каналами зв'язку.

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної та конфіденційної інформації; сертифікацію цих систем за вимогами інформаційної безпеки; ліцензування діяльності у сфері інформаційної безпеки, стандартизації способів і засобів захисту інформації; контроль за дією персоналу в захищених інформаційних системах. Важливе місце серед цих методів займають мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу, зайнятого забезпеченням інформаційної безпеки.

3.3 Основні фактори, що впливають на стан інформаційної безпеки

Процеси перетворення, що відбуваються в даний час, в політичному житті і економіці України безпосередньо впливають на стан її інформаційної безпеки. При цьому виникають нові чинники, які необхідно враховувати при оцінці реального стану інформаційної безпеки і визначенні ключових проблем в цій області. Їх можна розділити на політичні, економічні і організаційно-технічні [103].

До політичних факторів відносяться:

- зміна геополітичної обстановки унаслідок фундаментальних змін в різних регіонах світу, зведення до мінімуму ймовірності світової ядерної і звичайної воєн;
- інформаційна експансія США і інших розвинених країн, що здійснюють глобальний моніторинг світових політичних, економічних, військових, екологічних та інших процесів, що поширюють інформацію з метою здобуття однобічних переваг;
- становлення нової української державності на основі принципів демократії, законності, інформаційної відвертості;
- руйнування раніше існуючої командно-адміністративної системи державного управління, а також системи забезпечення безпеки країни, що склалася;

- порушення інформаційних зв'язків унаслідок утворення незалежних держав на території колишнього СРСР;

- прагнення України до тіснішої співпраці із зарубіжними країнами в процесі проведення реформ на основі максимальної відвертості сторін;

- низька загальна правова і інформаційна культура в українському суспільстві.

До економічних факторів відносяться:

- перехід України на ринкові стосунки в економіці, поява численних вітчизняних і зарубіжних комерційних структур – виробників і споживачів інформації, засобів інформатизації і захисту інформації, включення інформаційної продукції в систему товарних стосунків;

- критичний стан вітчизняних галузей промисловості, що виробляють засоби інформатизації і захисту інформації;

- кооперація, що розширюється, із зарубіжними країнами в розвитку інформаційної інфраструктури України.

До організаційно-технічних факторів відносяться:

- недостатня нормативно-правова база у сфері інформаційних стосунків, у тому числі в області забезпечення інформаційної безпеки;

- слабке регулювання державою процесів функціонування розвитку ринку засобів інформатизації, інформаційних продуктів і послуг в Україні;

- широке використання у сфері державного управління і кредитно-фінансовій сфері не захищених від просочування інформації імпортних технічних і програмних засобів для зберігання, обробки і передачі інформації;

- зростання обсягів інформації, переданої відкритими каналами зв'язку, у тому числі мережами передачі даних і між машинного обміну;

- загострення криміногенної обстановки, зростання числа комп'ютерних злочинів, особливо в кредитно-фінансовій сфері.

3.4 Основні функції системи інформаційної безпеки

Основними функціями інформаційної безпеки є:

- розробка і реалізація стратегії забезпечення інформаційної безпеки;

- реалізація прав громадян і організацій на здобуття, поширення і використання інформації;

- оцінка стану інформаційної безпеки в країні, виявлення джерел внутрішніх і зовнішніх загроз інформаційній безпеці, визначення пріоритетних напрямів запобігання, парирування і нейтралізації цих загроз;

- координація і контроль діяльності суб'єктів системи інформаційної безпеки;

- організація розробки федеральних і відомчих програм забезпечення інформаційної безпеки і координація робіт з їх реалізації;

- проведення єдиної технічної політики в області забезпечення інформаційної безпеки;

- організація фундаментальних, пошукових і прикладних наукових досліджень в області інформаційної безпеки;

- забезпечення контролю за створенням і використанням засобів захисту інформації за допомогою обов'язкового ліцензування діяльності в області захисту інформації і сертифікації засобів захисту інформації;

- здійснення міжнародної співпраці у сфері інформаційної безпеки, представлення інтересів України у відповідних міжнародних організаціях.

Система повинна забезпечувати гнучке управління процесами інформаційної безпеки на державному, регіональному, галузевому, виробничому і призначеному для користувача рівнях.

Масштабність, складність і різноманітність перерахованих функцій вимагають створення ієрархічної організаційної структури, що забезпечує координацію діяльності всіх складових системи інформаційної безпеки.

Контрольні запитання та завдання

1. Поясніть цілі забезпечення інформаційної безпеки.
2. Які основні завдання забезпечення інформаційної безпеки?
3. Що відноситься до об'єктів інформаційної безпеки?
4. Покажіть класифікацію загроз інформаційній безпеці.
5. Які є засоби дії загроз на об'єкти інформаційної безпеки?
6. Опишіть можливі наслідки реалізації загроз інформаційній безпеці.
7. Що відноситься до базових методів запобігання, парирування і нейтралізації загроз інформаційній безпеці?
8. Розкрийте основні фактори, які впливають на стан інформаційної безпеки.
9. Які є основні функції системи забезпечення інформаційної безпеки?

Завдання до самостійної роботи

1. Проаналізуйте як залежить конкурентоспроможність, рентабельність, рух грошової готівки підприємства від доступності, цілісності й конфіденційності інформації, яка циркулює на підприємстві та від інформаційної безпеки його інформаційних систем.

РОЗДІЛ 4

СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

4.1 Складові інформаційної безпеки підприємства

Діяльність суб'єктів господарювання в умовах становлення ринкових відносин потребує швидкого виявлення факторів, які обумовлюють інформаційну безпеку підприємства та адаптації останнього до динаміки зовнішнього середовища шляхом усунення виниклих загроз. Ринкова економіка, як відомо, ґрунтується на засадах конкуренції між учасниками ринку, що є постійним джерелом ризику.

Таким чином, управління інформаційною безпекою можна розглядати як невід'ємну частину системи управління підприємством, спрямованого на протидію зовнішнім і внутрішнім загрозам його функціонуванню. Здійснення заходів щодо забезпечення інформаційної безпеки підприємства необхідне для захищеності його діяльності від негативних впливів зовнішнього середовища і підтримки стану найефективнішого використання всіх видів ресурсів з метою запобігання загрозам і забезпечення стійкості та стабільного функціонування підприємства у поточний час і на перспективу.

Наведемо загальну схему головних складових інформаційної безпеки підприємства (рис. 4.1).

Складові інформаційної безпеки підприємства - це сукупність основних напрямів його інформаційної безпеки, істотно відмінних один від одного за своїм змістом. Розглянемо детально кожну зі складових інформаційної безпеки.

1. Технічна складова. Найбільш дослідженою та головною в усій сукупності складових інформаційної безпеки є технічна, яка в свою чергу складається з засобів захисту та каналів витоку.

Вся сукупність технічних засобів захисту поділяється на фізичні, програмно-технічні та апаратні і включає в себе електричні, механічні, електромеханічні та електронні пристрої. Фізичні засоби реалізуються у вигляді автономних пристроїв та систем, що виконують функції загального захисту об'єктів, на яких обробляється інформація. Програмно-технічні засоби є програмним забезпеченням, що виконує функції захисту інформації.

Апаратні засоби розміщують безпосередньо в обчислювальній техніці, в телекомунікаційній апаратурі чи в пристроях, що зв'язані з подібною апаратурою за допомогою стандартного інтерфейсу.

Канали витоку інформації у свою чергу підрозділяються на акустичні, вібро-акустичні, електро-акустичні, радіо-електронні, канали за рахунок ПЕМВН, канали за рахунок ВЧ-нав'язування та оптичні канали.

Акустичні. Під прямим акустичним каналом звичайно розуміють можливість прослуховування приміщень через природні і штучно створені отвори і щілини в стінах, стелях, через різні повітряноводні і вентиляційні шахти тощо. При цьому може бути використана звукопідсилювальна та записуюча апаратура, але в середині можна обійтися і без неї.

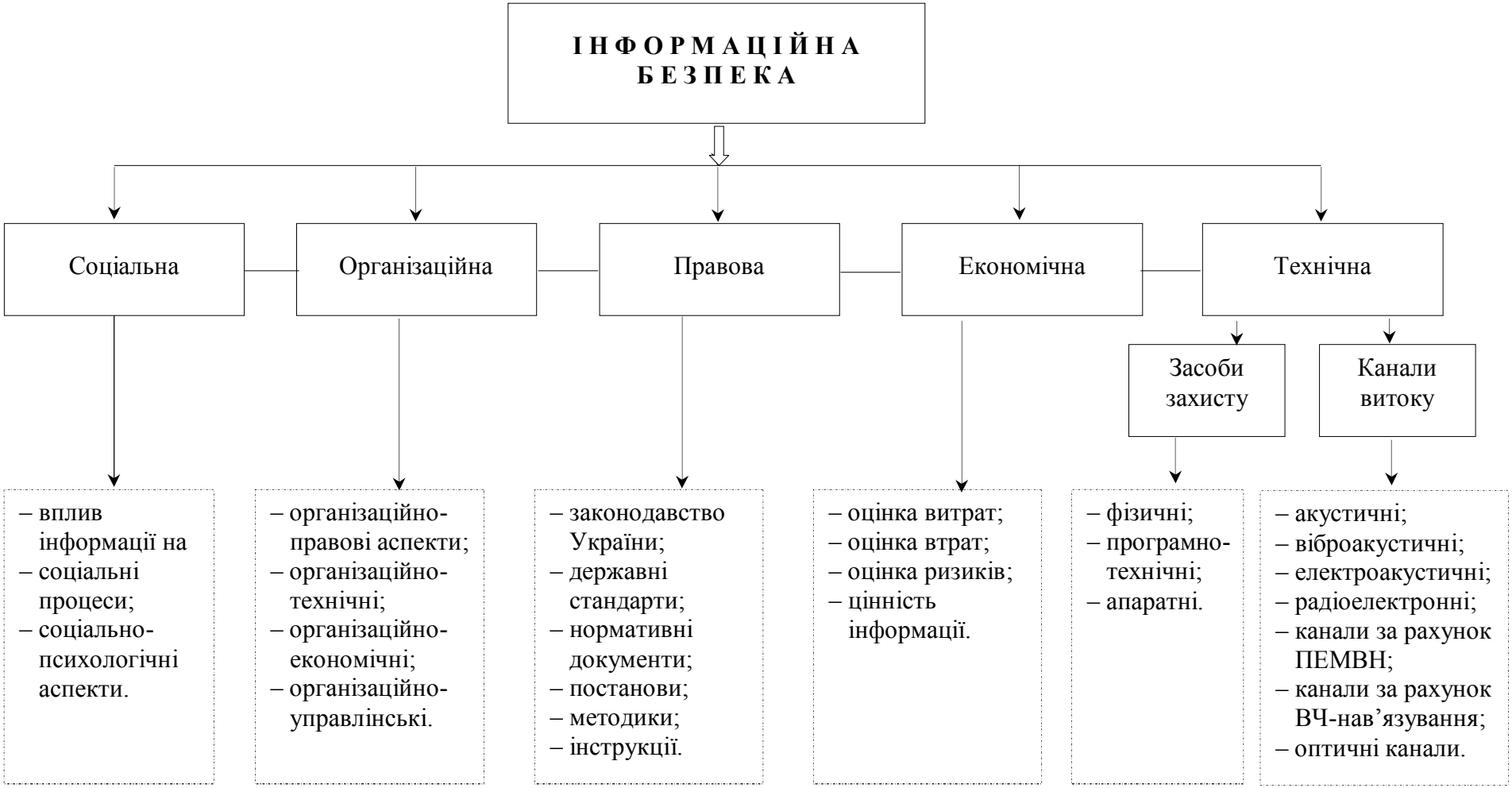


Рисунок 4.1 – Складові інформаційної безпеки підприємства

Оскільки наявність таких каналів витоку інформації на пряму пов'язана з якістю будівництва і ремонту, а також особливостями будівельних конструкцій, мало хто уявляє, що саме прямі акустичні канали звичайно приносять найбільші сюрпризи.

Віброакустичні. Віброакустичний канал витоку інформації – це можливість прослуховування приміщень за допомогою електронних стетоскопів, що перетворять вібраційні коливання будівельних конструкцій в електричний сигнал. Після посилення і найпростішої обробки цей сигнал може бути прослуханий, записаний на магнітофон або переданий радіоканалом.

У такий спосіб інформація може зніматися зі стін, перекрить, дверей, віконних рам і стекол, труб опалення і водопостачання, різних коробів тощо.

Це один з самих зручних для зловмисника видів знімання інформації.

По-перше, він не вимагає проникнення у зацікавлене приміщення, по-друге, стетоскопи відносно недорогі, легко встановлюються і знімаються, можуть використовуватися багаторазово.

Використання зловмисником таких каналів не залишає слідів і практично залишається на рівні припущень. Відстань, з якої може бути прослухане приміщення у випадку підключення стетоскопа до труб або інших металевих конструкцій складає десятки метрів.

Електроакустичні. Електроакустичні технічні канали витоку інформації виникають за рахунок електроакустичних перетворень акустичних сигналів на електричні і включають перехоплення акустичних коливань через допоміжні технічні засобі й системи, яким є притаманний „мікрофонний ефект", а також шляхом високочастотного нав'язування.

Перехоплення акустичних коливань в певному каналі витоку інформації здійснюються шляхом безпосереднього приєднування до з'єднувальних ліній допоміжних технічних засобів та систем, яким притаманний „мікрофонний ефект", спеціальних високочутливих низькочастотних підсилювачів. Наприклад, приєднуючи такі засоби до з'єднувальних ліній телефонних апаратів з електромеханічними викличними дзвінками, можна прослуховувати розмови, які точаться в приміщеннях, де встановлено ці апарати.

Радіоелектронні. Під час пересилання конфіденційної інформації в елементах схем, конструкцій, підвідних і з'єднувальних проводах протікають струми інформативних (небезпечних) сигналів. Електромагнітні поля, що виникають при цьому, можуть впливати на випадкові антени. Сигнали, прийняті випадковими антенами, можуть призвести до утворення каналів витоку інформації.

Канали за рахунок ПЕМВН (побічного електромагнітного випромінювання і наводів). Електромагнітне випромінювання і наведення є побічним результатом функціонування технічних засобів і можуть бути носіями інформації. Під час пересилання інформативного (небезпечного) сигналу одним колом у сусідніх колах – за їх паралельного пробігу – з'являються струми, наведені внаслідок електромагнітного впливу. Перехід електромагнітної енергії з одного кола в інше є можливим каналом витоку інформації.

Канали за рахунок ВЧ-нав'язування. Під час надходження високочастотних сигналів у нелінійні (або параметричні) кола, що несуть конфіденційну інформацію, відбувається модуляція високочастотного сигналу. Таким чином, високочастотні коливання стають носіями інформативних (небезпечних)сигналів і створюють канал витоку інформації.

Оптичні канали. Для прихованості проведення перехоплення мовних повідомлень із приміщень можуть бути використані пристрої, у яких передача інформації здійснюється в оптичному діапазоні. Найчастіше використовується невидимий для простого ока інфрачервоний діапазон випромінювання.

Найбільш складними і дорогими засобами дистанційного перехоплення мови з приміщень є лазерні пристрої. Принцип їхньої дії полягає в посилці зондувального променя в напрямку джерела звуку і прийманні цього променя після відбивання від яких-небудь предметів, наприклад, шибок, дзеркал тощо. Ці предмети вібрують під дією навколишніх звуків і модулюють своїми коливаннями лазерний промінь. Прийнявши відбитий від них промінь, можна відновити коливання, що модулюють.

2. Правова складова. До правової складової відноситься законодавство України, державні стандарти, нормативні документи, постанови, методики та інструкції, які регулюють та контролюють забезпечення інформаційної безпеки країни. До основних задач правової складової належить створення нормативно-правових засад забезпечення інформаційної безпеки, координація діяльності органів державної влади та управління, установ і підприємств із реалізації політики інформаційної безпеки.

Аналіз правової складової інформаційної безпеки розуміє аналіз законодавства сфери інформаційної безпеки. На основі аналізу законів України, державних стандартів, нормативно-правових документів системи технічного захисту інформації визначаються основні проблеми інформаційної безпеки телекомунікаційних систем.

Механізм формування вимог до інформаційної безпеки та основні напрямки нормативно-правового забезпечення захисту інформації в Україні наведені на рис. 4.2 та рис. 4.3 відповідно.

3. Організаційна складова. *Організаційна складова складається з* організаційно-правових, організаційно-технічних, організаційно-економічних та організаційно-управлінських аспектів.

Для захисту інтересів суб'єктів інформаційних відносин необхідно поєднувати заходи наступних рівнів: правових (закони, нормативні акти, стандарти і т.п.); управлінських дій загального характеру, організації, що здійснюються керівництвом; та конкретні заходи безпеки, що мають справу з людьми; технічних (конкретні технічні заходи) та економічних заходів.

Організаційно-правовий аспект. Правовий чи законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Більшість людей не здійснюють протиправних дій не тому, що це технічно неможливо, а тому, що це засуджується і карається суспільством, тому, що так поводитись не прийнято.

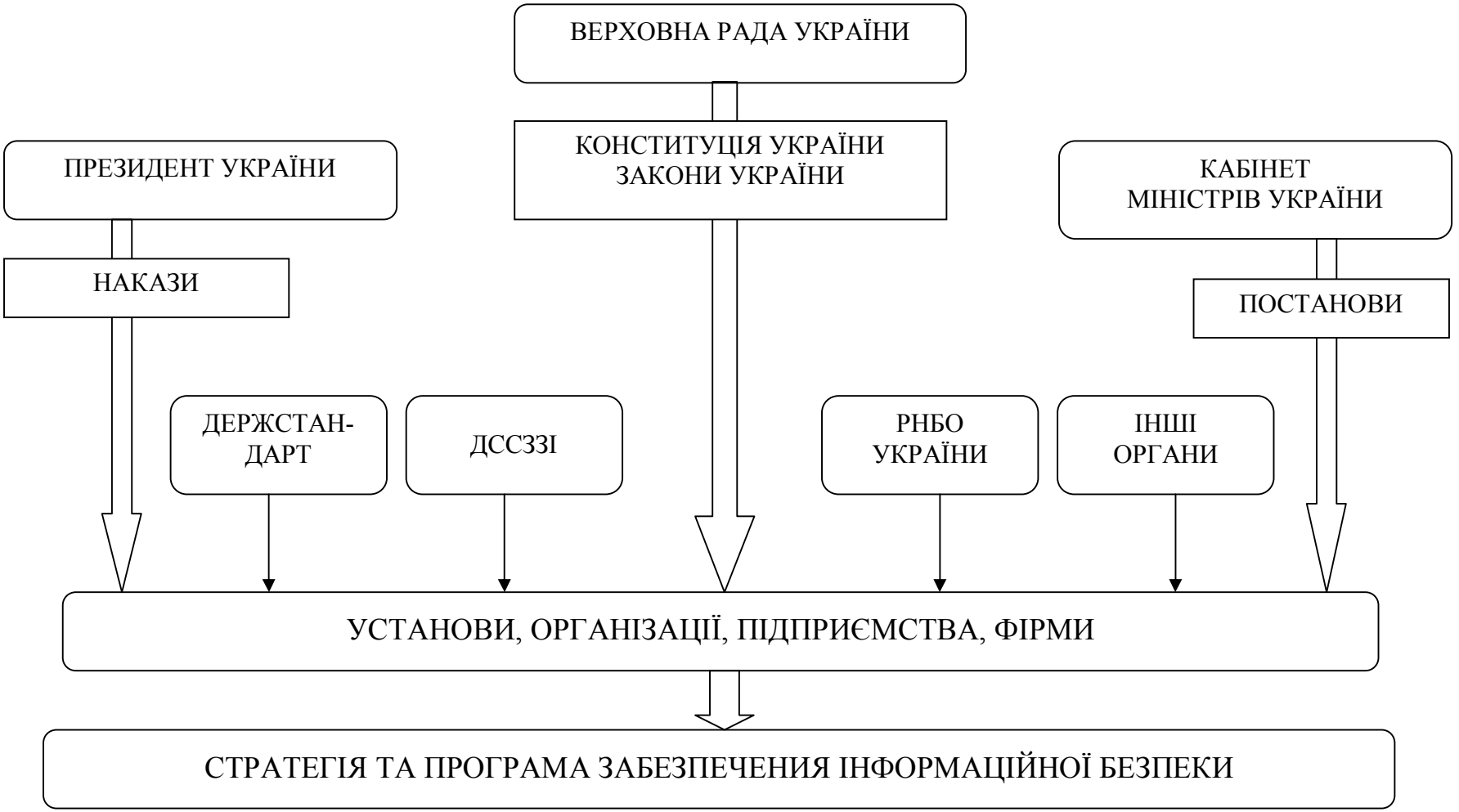


Рисунок 4.2 – Механізм формування вимог до інформаційної безпеки

Рисунок 4.3 – Основні напрямки нормативно-правового забезпечення захисту інформації в Україні

Ми розрізнятимемо на законодавчому рівні дві групи заходів: заходи, спрямовані на створення і підтримку в суспільстві негативного (зокрема карального) відношення до порушень і порушників інформаційної безпеки; і координуючі заходи, які направляють, сприяють підвищенню утвореної суспільством сфери інформаційної безпеки, що допомагають в розробці і розповсюдженні засобів забезпечення інформаційної безпеки.

До першої групи слід віднести, в першу чергу, Закони України "Про інформацію", "Про державну таємницю", "Про телекомунікації" та "Про захист інформації в інформаційно-телекомунікаційних системах" [52, 56, 61, 62]. Правда, положення цих законів носять вельми загальний характер, а основний зміст статей, присвячених інформаційній безпеці, зводиться до необхідності використовувати виключно сертифіковані засоби, що, загалом, правильно, але далеко не достатньо. Це, безумовно, кроки в правильному напрямі, оскільки робиться спроба охопити всі категорії суб'єктів інформаційних відносин.

До другої групи відноситься ряд документів, що регламентують процеси ліцензування і сертифікації у області інформаційної безпеки.

В світі глобальних мереж нормативно-правова база повинна бути узгоджена з міжнародною практикою. Ми хотіли б звернути особливу увагу на бажаність приведення українських стандартів і сертифікаційних нормативів у відповідність із міжнародним рівнем інформаційних технологій взагалі і, зокрема, інформаційної безпеки. Є багато причин, за яких це повинно бути зроблено. Одна з них – необхідність захищеної взаємодії із зарубіжними організаціями і зарубіжними філіалами українських організацій. Друга (істотніша) – домінування апаратно-програмних продуктів зарубіжного виробництва. На законодавчому рівні повинне одержати рішення питання про відношення до таких виробів. Тут необхідно розділити два аспекти: незалежність у області інформаційних технологій і інформаційну безпеку. Використання зарубіжних продуктів в деяких критично важливих системах (передусім військових) може представляти загрозу національній безпеці (зокрема інформаційній), оскільки не можна виключити ймовірність вбудовування закладних елементів. В той же час, в переважній більшості випадків потенційні загрози інформаційної безпеки носять виняткова внутрішній характер. У таких умовах незаконність використання зарубіжних розробок (зважаючи на складнощі з їх сертифікацією) за відсутності вітчизняних аналогів утрудняє захист інформації без серйозних на те підстав. Проблема сертифікації апаратно-програмних продуктів зарубіжного виробництва дійсно є складною, проте, як показує досвід європейських країн, вона може бути успішно вирішена. Система сертифікації, що склалася в Європі на вимоги інформаційної безпеки, дозволила оцінити операційні системи, системи управління базами дані і інші розробки американських компаній. Входження України в цю систему і участь українських фахівців у сертифікованих випробуваннях спроможні зняти наявну суперечність між незалежністю у області інформаційних, технологій і інформаційною безпекою без будь-якого зниження національної безпеки.

Головне ж, чого, на наш погляд, не вистачає сучасному українському законодавству (і що можна почерпнути із зарубіжного досвіду), це позитивної (не

каральної) спрямованості. Інформаційна безпека – це нова область діяльності, тут важливо навчити, роз'яснити, допомогти, а не заборонити і покарати. Суспільство повинне усвідомити важливість даної проблематики, зрозуміти основні шляхи рішення відповідних задач, повинні бути скоординовані наукові, учбові і виробничі плани. Держава може зробити це оптимальним чином. Тут не потрібно великих матеріальних витрат, потрібні інтелектуальні вкладення. Приклад позитивного законодавства – Британський стандарт BS 7799:1995, що описує основні положення політики безпеки. Більше 60% крупних організацій використовують цей стандарт в своїй практиці, хоча закон, строго кажучи, цього не вимагає.

Підводячи підсумок, можна намітити наступні основні напрями діяльності у організаційно-правовому аспекті: розробка нових законів з урахуванням інтересів всіх категорій суб'єктів інформаційних відносин; орієнтація на творчі, а не каральні закони; інтеграція – в світовий правовий простір, урахування сучасного стану інформаційних технологій, а також взаємодія між усіма складовими інформаційної безпеки.

Організаційно-управлінський аспект. Основою заходів організаційно-управлінського аспекту, тобто заходів, що робляться керівництвом організації, є політика безпеки та особливості управління персоналом. Належний рівень інформаційної безпеки у великій мірі залежить від складу кадрів, їхнього інтелекту та професіоналізму. Питання управління персоналом присвячено 12 розділ навчального посібника, тому зупинятися детально на цьому питанні не будемо.

Під політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації і асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації у області інформаційної безпеки, а також ту міру уваги й кількість ресурсів, яку керівництво вважає за доцільне виділити. Стандарт BS 7799:1995 рекомендує включати в документ, що характеризує політику безпеки організації, наступні розділи: ввідний, підтверджуючий заклопотаність вищого керівництва проблемами інформаційної, безпеки; організаційний, такий, що містить опис підрозділів, комісій, груп тощо, що відповідають за роботи у області інформаційної безпеки; класифікаційні наявні в організації матеріальні та інформаційні ресурси і необхідний рівень їх захисту, що описують штатні, характерні заходи безпеки, вживані до персоналу (опис посад з погляду інформаційної безпеки, організація навчання і перепідготовки персоналу порядок реагування на порушення режиму безпеки тощо); розділ, який освітлює питання фізичного захисту; розділ, що описує підхід до управління комп'ютерами і комп'ютерними мережами; розділ, що описує правила розмежування доступу до виробничої інформації; розділ, що характеризує порядок розробки супроводу систем; розділ, що описує заходи, направлені на забезпечення безперервної роботи організації; юридичний розділ, підтверджуючий відповідність політики безпеки чинному законодавству.

Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані і стратегія захисту визначена, складається програма, реалізація якої повинна

забезпечити інформаційну безпеку. Під цю програму виділяються ресурси, призначаються відповідальні, визначається порядок контролю виконання програми тощо. Організаційно-управлінський аспект – біла пляма у вітчизняній практиці інформаційної безпеки. Немає законів, що зобов'язують організації мати політику безпеки. Жодне з відомств, що займаються інформаційною безпекою, не пропонує типових розробок в даній області. Жоден учбовий заклад не готує фахівців із складання політики безпеки. Мало хто з керівників знає, що таке політика безпеки, ще менше число організацій таку політику мають. В той же час, без подібної основи інші заходи інформаційної безпеки повисають у повітрі, вони не можуть бути всеосяжними, систематичними і ефективними. Наприклад, заходи захисту від зовнішніх хакерів і від власних скривджених співробітників повинні бути абсолютно різними, тому в першу чергу необхідно визначитися, які загрози чреваті нанесенням найбільшого збитку. Відзначимо в зв'язку з цим, що, за статистикою, найбільший збиток походить від випадкових помилок персоналу, обумовлених неакуратністю або некомпетентністю, тому в першу чергу важливі не хитрі технічні засоби, а заходи навчання, тренування персоналу і регламентація його діяльності.

Розробка політики безпеки вимагає урахування специфіки конкретних організацій. Безглуздо переносити практику режимних державних організацій на комерційні – структури, учбові заклади або персональні комп'ютерні системи. У цій області доцільно запропонувати, по-перше, основні принципи розробки політики безпеки, а по-друге, - готові шаблони для найбільш важливих різновидів організацій. Аналіз ситуації на адміністративному рівні інформаційної безпеки ще раз показує важливість творчого, а не карального законодавства. Можна зажадати від керівників наявності політики безпеки (і в перспективі це правильно), але спочатку потрібно роз'яснити, навчити, показати для чого вона потрібна і як її розробляти.

У вітчизняних організаціях накопичений багатий досвід складання і реалізації організаційних заходів, проте проблема полягає в тому що вони прийшли з до комп'ютерного минулого і тому потребують істотного перегляду.

Можна виділити наступні групи організаційних заходів, спрямованих на забезпечення інформаційної безпеки: управління персоналом, фізичний захист, підтримка працездатності, реагування на порушення режиму безпеки та планування відновних робіт.

Управління персоналом в контексті інформаційної безпеки, як вже говорилося вище, залишається не проробленим та не розвинутим питанням. По-перше, для кожної посади повинні існувати кваліфікаційні вимоги щодо інформаційної безпеки. По-друге, в посадові інструкції повинні входити розділи, що стосуються інформаційної безпеки. По-третє, кожного працівника потрібно навчити заходам безпеки теоретично і відтренувати виконання цих заходів практично (проводити подібні тренування двічі на рік. Потрібна інформаційна цивільна оборона. Спокійно, без нагнітання пристрастей, потрібно роз'яснювати суспільству не тільки переваги, але і небезпеки, які витікають із використання інформаційних технологій. Акцент, на наш погляд, слід робити не на військовій або кримінальній стороні справи, а на чисто цивільних аспектах,

пов’язаних з підтримкою нормального функціонування апаратного і програмного забезпечення, тобто концентруватися на питаннях доступності і цілісності даних.

Охорона організаційно-управлінського аспекту інформаційної безпеки охоплює взаємозв’язані і водночас самостійні напрями діяльності того чи іншого суб’єкта господарювання.

На першій стадії процесу охорони цієї складової інформаційної безпеки здійснюється оцінка загроз негативних дій і можливої шкоди від таких дій. З-поміж основних негативних впливів на інформаційну безпеку підприємства виокремлюють недостатню кваліфікацію працівників тих чи тих структурних підрозділів, Їхнє небажання або нездатність приносити максимальну користь своїй фірмі. Це може бути зумовлене низьким рівнем управління персоналом, браком коштів на оплату праці окремих категорій персоналу підприємства чи нераціональним їх витрачанням.

Процес планування та управління персоналом, спрямований на охорону належного рівня інформаційної безпеки, має охоплювати організацію системи підбору, найму, навчання й мотивації праці необхідних працівників, включаючи матеріальні та моральні стимули, престижність професії, волю до творчості, забезпечення соціальними благами.

Зрозуміло, розділи, що стосуються інформаційної безпеки, повинні стати частиною шкільних і тим більше вузівських курсів інформатики. Заходи фізичного захисту, відомі з давніх часів, потребують доопрацювання у зв’язку з розповсюдженням мережних технологій і мініатюризацією обчислювальної техніки. Перш за все, слід захиститися від просочування інформації технічними каналами. Підтримка працездатності – ще одна біла пляма, що утворилася порівняно недавно. У епоху панування великих ЕОМ вдалося створити інфраструктуру,, здатну забезпечити, по суті, будь-який наперед заданий рівень працездатності (доступності) на всьому протязі життєвого циклу інформаційної системи. Ця інфраструктура включала як технічні так і процедурні регулятори (навчання персоналу і користувачів, проведення робіт відповідно до апробованих регламентів тощо). При переході до персональних комп’ютерів і технології клієнт/сервер інфраструктура забезпечення доступності багато в чому виявилася втраченою, проте важливість даної проблеми не тільки не зменшилася, але, навпаки, істотно зросла. Перед державними і комерційними організаціями стоїть завдання поєднання впорядкованості і регламентованості, властивих світу великих ЕОМ, з дружелюбністю і гнучкістю сучасних систем. Реагування на порушення інформаційної безпеки – знову біла пляма. Припустимо, користувач або системний адміністратор зрозумів, що має місце порушення. Що він повинен робити? Спробувати прослідкувати зловмисника? Негайно вимкнути устаткування? Подзвонити в міліцію? Проконсультуватися з фахівцями? Жодне відомство, причетне до інформаційної безпеки, не запропонувало регламенту дій в подібній екстремальній ситуації або свою консультаційну допомогу. Необхідно організувати національний центр інформаційної безпеки, в коло обов’язків якого входило б, зокрема, відстежування сучасного стану цієї області знань,

інформування користувачів всіх рівнів про появу нових загроз і заходи протидії, оперативна допомога організаціям у разі порушення їх інформаційної безпеки.

Планування відновних робіт і вся проблематика, пов'язана з відновленням працездатності після аварій, також потребує уваги. Адже жодна організація від таких порушень не застрахована. Тут необхідно відпрацювати дії персоналу в час і після аварій, заздалегідь потурбуватися про організацію резервних виробничих майданчиків, відпрацювати процедуру перенесення на ці майданчики основних інформаційних ресурсів, а також процедуру повернення до нормального режиму роботи. Підкреслимо, що подібний план потрібен не тільки найважливим військовим організаціям, але і звичайним комерційним компаніям, якщо вони не хочуть зазнати великих фінансових втрат.

Організаційно-економічний аспект. Система інформаційної безпеки телекомунікаційних мереж може бути ефективною, якщо витрати на її створення та управління будуть при наймі менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку маршрутизації інформації.

Оцінка витрат на захист інформації повинна завжди бути співвідносною з оцінкою втрат, якщо цю інформацію не захищати, та цінністю інформації, а також завжди враховувати можливі ризики. Тоді забезпечення інформаційної безпеки буде насправді якісним.

Завжди оцінюються загрози інформаційної безпеці, що мають політико-правовий характер і включають:

- внутрішні негативні дії;
- зовнішні негативні дії;
- форс мажорні обставини.

Забезпечення інформаційної безпеки компанії має цілком конкретний економічний зміст. А досягнення цієї мети повинне здійснюватися економічно виправданими мірами. Приймати рішення про фінансування проекту з інформаційної безпеки доцільно лише в тому випадку, коли упевнені, що не просто збільшили видаткову частину свого бюджету, а зробили інвестиції в розвиток компанії.

Саме тому організаційно-економічний аспект грає не маловажну роль у системі інформаційної безпеки і лежить в основі більшості методів оцінки ефективності вкладень в інформаційну безпеку - зіставлення витрат, необхідних на забезпечення інформаційної безпеки, і збитку, що може бути заподіяний компанії через відсутність цієї системи.

Організаційно-технічний аспект. Згідно сучасним переконанням, в рамках інформаційних систем повинні бути доступні принаймні наступні механізми безпеки: ідентифікація і перевірка справжності (автентифікація) користувачів; управління доступом; протоколювання і аудит; криптографія; міжмережне екранування; забезпечення високої доступності. Крім того, інформаційною системою в цілому і механізмами безпеки особливо необхідно управляти. І управління, і механізми безпеки повинні функціонувати в різнорідному, розподіленому середовищі, побудованому, як правило, в архітектурі клієнт/сервер.

Це означає, що згадані засоби повинні спиратися на загальноприйняті стандарти бути стійкими до мережних загроз, зважати на специфіку окремих сервісів.

На сьогодні переважна більшість розробок орієнтована на платформи Intel/DOS/Windows. В той же час найбільш значуща інформація концентрується на інших, серверних платформах. Захисту потребують не окремі персональні комп'ютери і локальні мережі на базі таких комп'ютерів, а в першу чергу істотно більш просунуті сучасні корпоративні системи.

Розглянемо типову державну організацію, що має декілька виробничих майданчиків, на кожній з яких можуть знаходитися критично важливі сервери, в доступі до яких мають потребу працівники, що базуються на інших майданчиках, і мобільні користувачі. До числа підтримуваних інформаційних сервісів входять файловий і поштовий сервіс, системи управління базами даних (СУБД), Web-сервіс і т.д. У локальних мережах і за між мережному доступі основним є протокол TCP/IP.

Для побудови ешелонованої оборони подібної інформаційної системи необхідні принаймні наступні захисні засоби програмно-технічного рівня: між мережні екрани (розмежування між мережного доступу); засоби підтримки приватних віртуальних мереж (реалізація захищених комунікацій між виробничими майданчиками відкритими каналами зв'язку); засоби ідентифікації /автентифікації, що підтримують концепцію єдиного входу в мережу (користувач один раз доводить свою справжність при вході в мережу організації, після чого дістає доступ до всіх наявних сервісів відповідно до своїх повноважень); засоби протоколювання і аудиту, що відстежують активність на всіх рівнях - від окремих застосувань до мережі організації в цілому, що оперативно виявляють підозрілу активність: комплекс засобів централізованого адміністрування інформаційної системи організації; засоби захисту, які входять до складу застосувань, сервісу і апаратно-програмних платформ.

Комерційні структури, на відміну від держструктур, певною мірою вільніші в своєму виборі захисних засобів. Проте, через цілий ряд обставин (необхідність взаємодії з держструктурами, розширювальне трактування поняття "державна таємниця" – необхідність отримання ліцензії на експлуатацію криптографічних засобів, обмеження на імпорт криптографічних засобів ця свобода не дуже велика. Практично на усі категорії суб'єктів інформаційних відносин перенесений підхід, розрахований на держструктури.

4. Економічна складова. Економічна складова інформаційної безпеки є невід'ємною, так як на захист інформації будь-якого підприємства чи компанії потрібні гроші, тобто капітальні вкладання. Уся сукупність технічних та організаційних засобів базується саме на економічній складовій, тому цю складову неможливо залишити без уваги чи обійти зовсім.

На наш погляд економічна складова складається з наступних частин: оцінки витрат на інформаційну безпеку, оцінка втрат від можливих перешкод та зловживань, оцінки можливих ризиків та їх страхування та оцінка цінності інформації.

Система інформаційної безпеки може бути ефективною, якщо витрати на її створення та управління будуть принаймні менші за втрати внаслідок

знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення встановленого порядку маршрутизації інформації.

Неможливо створити абсолютно надійну систему безпеки. В основному через те, що постійно розробляються нові види загроз, яким система не зможе протистояти, а також через те, що ефективність системи захисту залежить від обслуговуючого персоналу, а людині властиво помилятися. Вартість подолання захисту повинна бути більше вартості, що досягається при її зломі. У будь-якому випадку вартість засобів забезпечення безпеки повинні відповідати ризику і прибутку у середовищі, який оточує даний суб'єкт.

Керівництво будь-якої компанії розуміє, що неможливо виділити необмежений обсяг фінансів і людських ресурсів на забезпечення інформаційної безпеки. З економічної точки зору вкладення в безпеку повинні показати прибуток або скорочення можливих витрат, що мали місце. Політика забезпечення інформаційної безпеки повинна визначати пріоритети інвестицій у напрямку найбільшої уразливості.

Існує ряд методів та методик за допомогою яких оцінюється доцільність витрат на забезпечення інформаційної безпеки підприємства. Але кожне підприємство повинно обирати свій метод чи методику оцінки витрат на інформаційну безпеку, в залежності від специфіки та діяльності підприємства. Але усі існуючі методи об'єднують єдині принципи та правила:

- метод повинен забезпечувати кількісну оцінку витрат на безпеку, використовувати показники оцінки можливостей дій та їх наслідків;
- метод повинен бути прозорим з точки зору користувача та давати можливість вводити особисті емпіричні данні;
- метод повинен бути універсальним, тобто однаково використовуватися до оцінки витрат на закупівлю апаратних засобів, спеціалізованого та універсального програмного забезпечення, витрат на послуги, витрат на переміщення персоналу та навчання користувачів;
- обраний метод повинен дозволяти моделювати ситуацію, за якої існує декілька контрзаходів, направлених на попередження виявленої загрози.

На практиці використовуються наступні методи:

- Прикладний інформаційний аналіз (Applied Information Economics);
- Споживчий індекс (Customer Index);
- Доданої економічної вартості (Economic Value Added);
- Економічної вартості (Economic Value Sourced);
- Управління портфелем активів (Portfolio Management);
- Оцінка дійсних можливостей (Real Option Valuation);
- Метод життєвого циклу штучних систем (System Life Cycle Analysis);
- Система збалансованих показників (Balanced Scorecard);
- Сукупної вартості володіння (Total Cost of Ownership);
- Функціонально-вартісний аналіз (Activity Based Costing).

У розділі 10 даного навчального посібника розроблено методичні основи оцінки економічної доцільності захисту інформації для телекомунікаційних мереж та для підприємств зв'язку.

5. Соціальна складова. Включає в себе вплив інформації на соціальні процеси та соціально-психологічні аспекти. Відбувається величезне зростання обсягів інформації, знання диференціюються та спеціалізуються, неминуче зростає сфера послуг, тому процес становлення інформаційної цивілізації є об'єктивним і закономірним. Інша річ, що різні держави, в залежності від свого інтелектуального, наукового, технологічного рівня розвитку мають різні перспективи щодо цього. Високо розвинуті держави світу вже пройшли початковий етап становлення суспільства інформаційної демократії, інші знаходяться на заключній фазі індустріалізму, треті – ще не мають навіть більш-менш розвинутого індустріального сектора. Але так чи інакше світ все більше залежить від влади інформації.

Інформація в сучасному світі вже є засобом і ціллю повноцінної життєдіяльності та набуває чітких рис реальної влади, яка тісно вплетена в усі сфери функціонування суспільства та всі інші види влади. Людство, таким чином, безустанно просувається до нової ери свого розвитку – ери, де найвищими цінностями виступають інформація та знання.

Як соціальне явище інформатизація охоплює поточні та перспективні проблеми – економічні, організаційні, соціальні, пов'язані з розвитком культури та освіти, діяльністю всіх ланок соціального управління та народного господарства. Як показує досвід інших країн, інформатизація сприяє забезпеченню національних інтересів, розвитку наукомістких виробництв та високих технологій, підвищенню продуктивності праці, вдосконаленню управління економікою, соціально-економічних відносин, збагаченню духовного життя та подальшої демократизації суспільства. Тому соціальна складова є також невід'ємною для забезпечення інформаційної безпеки.

В сучасних умовах інформація проникає в усі сфери життєдіяльності, тобто процеси конвергенції інформації і телекомунікацій та їх вплив на формування нових управлінських технологій незбіжні.

З визначення складових ІБ підприємства випливає, що для того, щоб перейти до методів та засобів захисту конфіденційної інформації на підприємстві необхідно розглянути джерела загроз інформації.

4.2 Джерела загроз інформаційної безпеки підприємства

Засоби впливу загроз на інформаційну безпеку конкретного підприємства є такі самі, як і загальні засоби впливу, які були розглянуті у розділі 3.2. Конкретне підприємство буде мати і специфічні загрози, характерні для його середовища і характеру діяльності.

Реалізація інформаційних загроз на рівні особи призводить до порушення або обмеження доступу громадян до інформації загального користування. Це створює загрозу інформаційній безпеці особистості як з боку органів влади, так і з боку сторонніх осіб або угрупувань, порушує баланс стосунків між особистістю, суспільством і державою.

Наслідком впливу інформаційних загроз на соціальну спільноту є ускладнення соціальних процесів, що виявляється у загостренні суперечностей

між різними соціальними прошарками, загостренні політичної боротьби, розпалюванні релігійних та етнічних суперечностей, зниженні загальної культури населення, розвитку бездуховності, зростанні злочинності, розповсюдженні антигуманних ідей. Наслідки інформаційних злочинів в економічній сфері можуть призвести до економічних втрат за рахунок знецінення і втрати товарної частини інформаційного ресурсу – промислових і інформаційних технологій.

Основні види загроз інформаційним активам підприємства [8]:

Під час побудови системи захисту інформаційних активів підприємства важливим є визначення та систематизація загроз, що діють на них. Створення ефективної системи захисту інформації на підприємстві є важливий та трудомісткий процес, що складається з наступних етапів:

- визначення меж огляду;
- ідентифікація активів та встановлення залежності між ними;
- оцінювання активів та встановлення залежності між ними;
- оцінювання загроз;
- оцінювання вразливостей;
- ідентифікація наявних і (або) запланованих засобів захисту;
- оцінювання ризиків;
- вибір засобів захисту;

Після визначення меж огляду, інвентаризації та проведення оцінки активів важливим є визначення загроз, які можуть діяти на інформаційну систему підприємства. Потенційно можливий несприятливий вплив, що приводить до зниження цінності ресурсів підприємства, називається загрозою [110].

У випадку реалізації загрози цінність інформаційного ресурсу підприємства може знизитись внаслідок порушення цілісності, конфіденційності та доступності інформації.

Всі загрози повинні бути визначені, а ймовірність їх прояву оцінена. Оцінку вартості повинні проводити власники інформаційних активів. Але в більшості випадків вони не здатні визначити перелік всіх загроз, які можуть впливати на їхні ресурси. Тому перелік загроз інформаційним активам в організації, потрібно скласти із залученням спеціалістів у сфері інформаційної безпеки, а також керівників та їх власників. У зв’язку з постійною модифікацією та вдосконаленням загроз такий перелік потрібно періодично переглядати та вносити до нього зміни [67].

За природою походження джерела їх можна поділити на [94]:

Об’єктивні загрози виникають незалежно від прямої діяльності людини і пов’язані з різними стихійними природними явищами такими, як пожежі, блискавки, землетруси, радіоактивне випромінювання, напади гризунів тощо.

Суб’єктивні загрози, виникнення яких залежить від діяльності людини.

Суб’єктивну загрозу в свою чергу за мотивами можна розділити на навмисну чи випадкову. *Навмисна* – пов’язана з діями людини, направленими на отримання певної вигоди, а *випадкова* включає зазначену складову і

пов’язана з помилками людини, її недбалістю, проектно-технологічними недоліками в програмному та апаратному забезпеченні тощо.

Приклади загроз [147] наведені в таблиці 4.1.

Таблиця 4.1 – Приклади загроз

Суб’єктивна		**Об’єктивна**
Навмисні	**Випадкові**	
Підслуховування	Помилки та недогляд	Землетрус
Зміна інформації	Вилучення файлу	Блискавка
Злом системи	Неправильна маршрутизація	Потоп
Навмисний програмний код	Фізичні ушкодження	Пожежі

Загрози можуть бути викликані однією чи кількома навмисними, чи випадковими подіями.

Перелік можливих загроз наведений [147] у табл. 4.2. Наведені в таблиці загрози інформаційним активам є прикладом. Не можливо скласти єдиний вичерпний їх перелік універсальний для всіх підприємств. В кожному випадку для визначення загроз інформаційним активам потрібно застосувати індивідуальний підхід.

Таблиця 4.2 – Перелік можливих загроз

№ п. п	**Загроза**	**Суб’єктивна**		**Об’єктивна**
		Навмисна	**Випадкова**	
1	Землетрус			+
2	Потоп	+	+	+
3	Ураган			+
4	Блискавка			+
5	Промисловий вплив	+		+
6	Бомбова атака	+		+
7	Використання зброї	+		+
8	Вогонь	+		+
9	Навмисне пошкодження	+		
10	Несправність електроживлення		+	
11	Несправність водопостачання		+	
12	Несправність кондиціювання повітря	+	+	
13	Відмова апаратури		+	
14	Нестабільність живлення		+	+
15	Екстремальні значення температури і вологості	+	+	+
16	Пил			+
17	Електромагнітне випромінювання	+	+	+
18	Електростатичний заряд			+
19	Злодійство	+		
20	Неуповноважене використання носіїв даних	+		

21	Погіршення носіїв даних			+
22	Помилка оперативного персоналу	+	+	
23	Помилка обслуговуючого персоналу	+	+	
24	Програмний збій	+	+	
25	Використання програмного забезпечення користувачами що не уповноважені	+	+	
26	Використання програмного забезпечення не уповноваженим способом	+	+	
27	Невідповідність ідентифікатора користувача	+		
28	Незаконне використання програмного забезпечення	+	+	
29	Зловмисна програмна закладка	+	+	
30	Незаконний імпорт або експорт програмного забезпечення	+		
31	Помилка оператора	+	+	
32	Помилка супроводу	+	+	
33	Доступ до мережі користувачами що не уповноважені	+		
34	Використання мережених засобів не уповноваженим способом	+		
35	Технічна несправність мережених компонентів		+	
36	Помилка під час пересилання інформації		+	
37	Пошкодження ліній зв’язку	+	+	
38	Перевантаження трафіку	+	+	
39	Підслуховування	+		
40	Просочування даних під час зв’язку	+		
41	Неуповноважений аналіз потоків інформації	+		
42	Неправильна маршрутизація повідомлень		+	
43	Зміна маршруту повідомлень	+		
44	Збій послуг зв’язку	+	+	
45	Недоліки що допускає персонал в роботі		+	
46	Помилки користувача	+	+	
47	Неправильне застосування ресурсів	+	+	

Загрозу можна виміряти кількісно (кількість загиблих, сума економічних збитків тощо) та відповідно класифікувати:

1. *За ступенем вірогідності:* невірогідна, маловірогідна, вірогідна, цілком вірогідна.

2. *За ступенем розвитку:* виникнення, експансія, стабілізація, ліквідація.

3. *За розвитком у часі:* безпосередня, близька (до 1 року), далека (більше року).

4. *За розвитком у просторі:* територія підприємства, прилегла територія, територія регіону, територія країни, зарубіжна територія.

5. *За напруженістю:*

- нормальна; підвищена; близька до межі; надлишкова;
- така, що зростає; стабільна; така, що має тенденцію до зниження.

6. *За природою виникнення:* природна (об'єктивна), що викликана стихійним природним явищем, незалежним від людини; близька до штучної (суб'єктивна) спричинена діяльністю людини, ненавмисна або навмисна.

7. *За сферою виникнення розрізняють загрози:* економічна; соціальна; правова; організаційна; інформаційна; екологічна; технічна, кримінальна.

Причини небезпеки, на нашу думку, можна класифікувати за такими ознаками:

- за природою виникнення: на макро- і мікрорівнях, культурно-етичні, випадкові і злочинні;
- з чиєї вини виникла небезпека: керівництво, боржники, ділові партнери, треті особи;
- за характером виникнення і джерелом заподіяння збитків: власними діями, діями третіх осіб, стихійними лихами, аваріями, катаклізмами;
- за можливістю впливу підприємства на усунення загроз: усуваються самим підприємством, важко усуваються, не усуваються;
- за можливістю прогнозування і діагностування: прогнозовані і діагностовані, причини не прогнозовані.

На нашу думку, найдоцільнішим є визначення факторів економічної безпеки підприємства насамперед залежно від ступеня виміру, які можна розділити на дві групи.

Зовнішні фактори: зміна форми власності, зміна пріоритетів держави щодо промислової політики; зміна оточення (споживачі - постачальники); зниження виробничого і споживчого попиту і зменшення внутрішнього ринку; кредитна система, недоступність ресурсів розвитку; нестабільність законодавчої бази та податкової системи; зростання безробіття, міжнародна конкуренція.

Внутрішні фактори: неефективні менеджмент і маркетинг; низький рівень використання усіх видів ресурсів, зокрема основних засобів; неефективна структура активів; зростання дебіторської заборгованості; недостатньо диференційований асортимент продукції та її не конкурентоспроможність.

Зрозуміло, що рівень стабільності підприємства залежить від ефективної діяльності служб підприємства, а саме: наскільки вдається запобігати загрозам й усувати збитки від їхніх негативних впливів на різні аспекти функціонування підприємства. Джерелами таких негативних впливів можуть бути: усвідомлені або неусвідомлені дії людей, організацій, у тому числі органів державної влади, міжнародних організацій або підприємств-конкурентів, а також збіг об'єктивних обставин – стан фінансової кон'юнктури на ринках підприємства, наукові відкриття і технологічні розробки, форс-мажорні обставини тощо. Залежно від суб'єктивної обумовленості негативних впливів на економічну безпеку підприємства можна застосувати таку градацію.

Об'єктивні негативні впливи виникають без участі і незалежно від волі підприємства або його службовців.

Суб'єктивні негативні впливи виникають як наслідок неефективної роботи підприємства в цілому або його працівників.

Нами було проаналізовано складові ІБ підприємства та джерела загроз інформаційної безпеки підприємства. Для того, щоб визначити стратегію ІБ підприємства та перейти до оцінки економічної доцільності захисту інформації на підприємстві розкриємо методи та засоби захисту конфіденційної інформації на підприємстві.

4.3 Методи та засоби захисту конфіденційної інформації на підприємстві

Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні і організаційно-економічні методи. Правові методи – передбачають розробку комплексу нормативно-правових актів і положень, регламентуючих інформаційні відносини в суспільстві, керівних і нормативно-методичних документів щодо забезпечення інформаційної безпеки.

Програмно-технічні методи - це сукупність засобів:

- запобігання витоку інформації;
- виключення можливості несанкціонованого доступу до інформації;
- запобігання впливам, які призводять до знищення, руйнування, спотворення інформації, або збоям чи відмовам у функціонуванні засобів інформатизації;
- виявлення закладних пристроїв;
- виключення перехоплення інформації технічними засобами;
- використання криптографічних засобів захисту інформації при передачі каналами зв'язку.

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно вимогам інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах. Важливе значення для запобігання інформаційним загрозам має мотивація, економічне стимулювання і психологічна підтримка діяльності персоналу, який забезпечує інформаційну безпеку.

Поняття захисту інформації. Під захистом інформації розуміють сукупність заходів і дій, спрямованих на забезпечення її безпеки конфіденційності і цілісності – у процесі збору, передачі, обробки і збереження.

Сутність захисту інформації полягає у виявленні, усуненні або нейтралізації негативних джерел, причин і умов впливу на інформацію. Ці джерела є загрозою безпеці інформації. Мета та методи захисту інформації відображають її сутність.

Попередження можливих загроз і протиправних дій може бути забезпечене всілякими засобами, починаючи від створення клімату глибоко-усвідомленого відношення співробітників до проблеми безпеки і захисту інформації до створення глибокої, ешелонованої системи захисту фізичними, апаратними, програмними і криптографічними засобами. Попередження загроз

можливе і шляхом одержання інформації про протиправні акти, які готуються, плановані розкрадання, підготовчі дії і інші елементи злочинних діянь. У попередженні загроз важливу роль відіграє інформаційно-аналітична діяльність служби безпеки на основі глибокого аналізу криміногенної обстановки і діяльності конкурентів і зловмисників.

Виявлення має на меті проведення заходів щодо збору, нагромадження й аналітичної обробки відомостей про можливу підготовку злочинних дій з боку кримінальних структур або конкурентів на ринку виробництва та збуту товарів і продукції.

Виявлення загроз – це дії по визначенню конкретних загроз і їхніх джерел, що приносять той або інший вид збитку. До таких дій можна віднести виявлення фактів розкрадання або шахрайства, а також фактів розголошення конфіденційної інформації або випадків несанкціонованого доступу до джерел комерційних секретів.

Припинення або локалізація загроз – це дії, спрямовані на усунення діючої загрози і конкретних злочинних дій.

Ліквідація наслідків має на меті відновлення стану, що передував настанню загрози.

Усі ці способи мають на меті захистити інформаційні ресурси від протиправних зазіхань і забезпечити:

- запобігання розголошення і витоку конфіденційної інформації;
- заборону несанкціонованого доступу до джерел конфіденційної інформації;
- збереження цілісності, повноти і доступності інформації;
- дотримання конфіденційності інформації;
- забезпечення авторських прав.

Інформація, що захищається, містить відомості, що складають державну, комерційну, службову та інші таємниці, які охороняються законом. Кожен вид інформації, що захищається, має свої особливості в галузі регламентації, організації і здійснення цього захисту.

Найбільш загальними ознаками захисту будь-якого виду інформації, що охороняється є:

- захист інформації організує і проводить власник або господар інформації або вповноважені ним особи (юридичні або фізичні);
- захистом інформації власник охороняє свої права на володіння і розпорядження інформацією, прагне відгородити її від незаконного заволодіння і використання на шкоду його інтересам;
- захист інформації здійснюється шляхом проведення комплексу заходів для обмеження доступу до інформації, що захищається, і створення умов, що виключають або істотно ускладнюють несанкціонований, незаконний доступ до засекреченої інформації і її носіїв.

Таким чином, *захист інформації* – це комплекс заходів, проведених власником інформації, для захисту своїх прав на володіння і розпорядження інформацією, створення умов, що обмежують її поширення і виключають або

істотно ускладнюють несанкціонований, незаконний доступ до засекреченої інформації і її носіїв.

Інформація, що захищається, яка є державною або комерційною таємницею, як і будь-який інший вид інформації, необхідна для управлінської, науково-виробничої й іншої діяльності. В даний час перед захистом інформації ставляться більш широкі задачі: забезпечити безпеку інформації. Це обумовлено низкою обставин, і в першу чергу тим, що все більш широке застосування в накопичуванні й обробці інформації, що захищається, одержують ЕОМ, у яких може відбуватися не тільки витік інформації, але і її руйнування, перекручування, підробка, блокування й інші втручання в інформацію й інформаційні системи.

Таким чином, захист інформації – це діяльність власника інформації або уповноваженої ним особи по:

- забезпеченню своїх прав на володіння, розпорядження і керування інформацією, що захищається;
- запобіганню витоку і втраті інформації;
- збереження повноти, вірогідності, цілісності інформації, що захищається, її масивів і програм обробки;
- збереженню конфіденційності або таємності інформації, що захищається, відповідно до правил, установлених законодавчими й іншими нормативними актами.

Задачі захисту інформації. Засоби забезпечення збереження та захисту інформації в державній організації, на підприємстві або фірмі відрізняються за своїми масштабами і формами. Вони залежать від виробничих, фінансових та інших можливостей підприємства, від кількості секретів, які вона охороняє та їхньої значимості. При цьому вибір таких мір необхідно здійснювати за принципом економічної доцільності, дотримуючись у фінансових розрахунках „золотої середини”, оскільки надмірне закриття інформації, так само як і халатне відношення до її збереження, можуть викликати втрату певної частки прибутку або призвести до непоправних збитків. Відсутність у керівників підприємств чіткого уявлення про умови, що сприяють витоку конфіденційної інформації, приводять до її несанкціонованого поширення.

Наявність великої кількості вразливих місць на будь-якому сучасному підприємстві або фірмі, широкий спектр загроз і досить висока технічна оснащеність зловмисників вимагає обґрунтованого вибору спеціальних рішень до захисту інформації. Основою таких рішень можна вважати:

1. Застосування наукових принципів по забезпеченню інформаційної безпеки, що включають у себе: законність, економічну доцільність і прибутковість, самостійність і відповідальність, наукову організацію праці, тісний зв’язок теорії з практикою, спеціалізацію і професіоналізм, програмно-цільове планування, взаємодію і координацію, доступність у поєднанні з необхідною конфіденційністю;

2. Прийняття правових зобов’язань з боку співробітників підприємства по відношенню збереження довірених їм відомостей (інформації);

3. Створення таких адміністративних умов, за яких виключається можливість крадіжки, розкрадання або перекручування інформації;

4. Правомірне залучення до карного, адміністративного й іншого видів відповідальності, які гарантують повне відшкодування збитку від втрати інформації;

5. Проведення дієвого контролю і перевірки ефективності планування і реалізації правових форм, методів захисту інформації відповідно до обраної концепції безпеки;

6. Організація договірних зв'язків з державними органами регулювання в галузі захисту інформації.

7. Здійснюючи комплекс захисних заходів головне – обмежити доступ у ті місця і до тієї техніки, де зосереджена конфіденційна інформація (не забуваючи, звичайно, про можливості і методи дистанційного її одержання). Зокрема, використання якісних замків, засобів сигналізації, хорошої звукоізоляції стін, дверей, стелі та підлоги, звуковий захист вентиляційних каналів, отворів і труб, що проходять через ці приміщення, демонтаж зайвої проводки, а також застосування спеціальних пристроїв (генераторів шуму тощо) серйозно ускладнять або зроблять безглуздими спроби впровадження спецтехніки.

Для надійного захисту конфіденційної інформації доцільно застосовувати наступні організаційні заходи:

1. Визначення рівнів (категорій) конфіденційності інформації, що захищається;

2. Вибір принципів (локальний, об'єктовий або змішаний) методів і засобів захисту;

3. Установлення порядку обробки інформації, що захищається;

4. Облік просторових факторів:

- введення контрольованих (охоронюваних) зон;

- правильний вибір приміщень і розташування об'єктів між собою і щодо межі контрольованої зони;

5. Облік тимчасових факторів:

- обмеження часу обробки інформації, що захищається – доведення часу обробки інформації з високим рівнем – конфіденційності до вузького кола осіб;

6. Облік фізичних і технічних факторів:

- визначення можливості візуального (або за допомогою технічних засобів) спостереження відображуваної інформації сторонніми особами, відключення контрольно-вимірювальної апаратури від інформаційного об'єкта і її знеструмлення, максимальне рознесення інформаційних кабелів між собою і щодо провідних конструкцій, їхній перетин під прямим кутом.

Для блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів і створення системи захисту об'єкта по них необхідно здійснити ряд заходів: проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і

підведені комунікації; виділити ті приміщення, усередині яких циркулює конфіденційна інформація і врахувати технічні засоби, використані в них.

Алгоритм створення системи забезпечення інформаційної безпеки підприємства наведено на рис. 4.4.

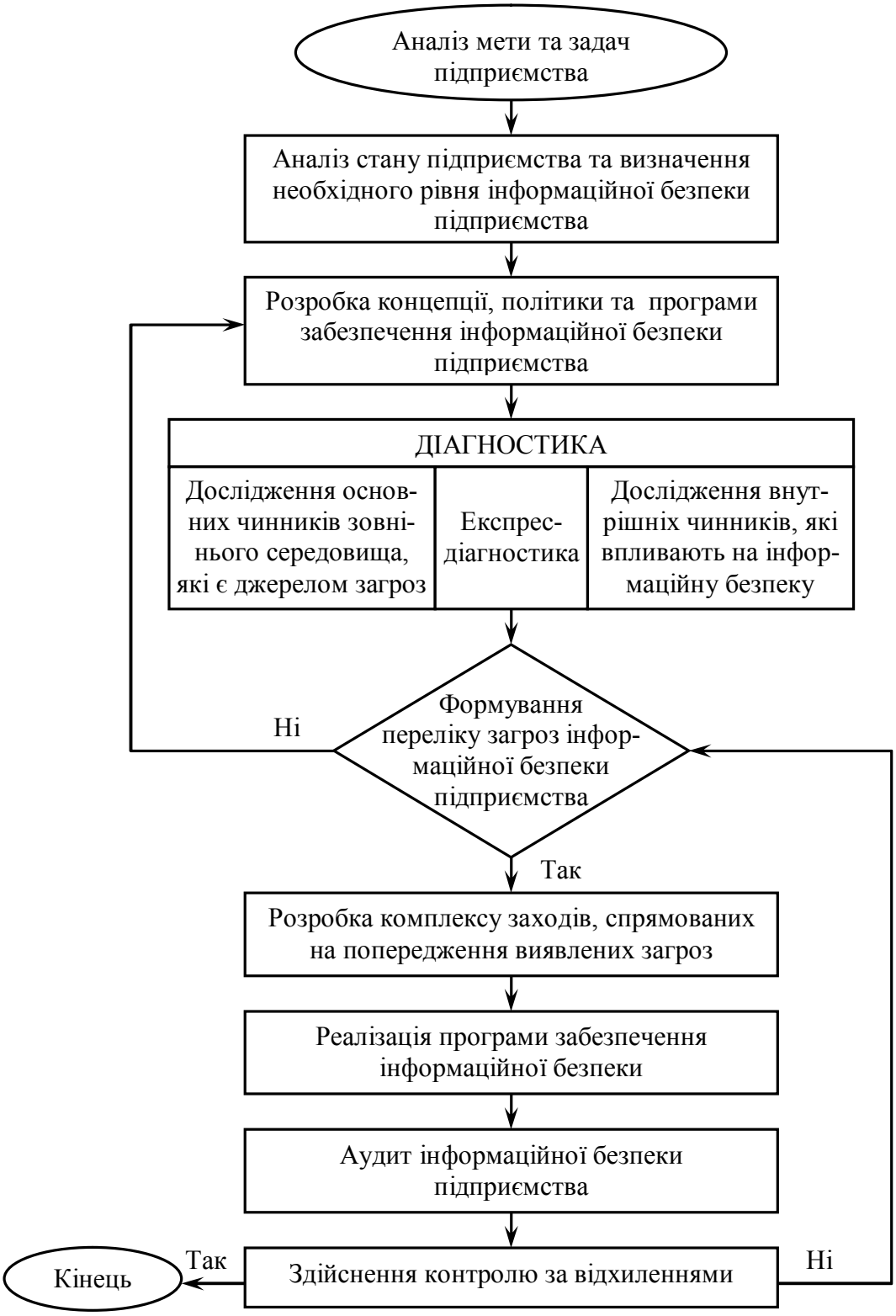


Рисунок 4.4 - Алгоритм створення системи забезпечення інформаційної безпеки підприємства

Після визначення складових інформаційної безпеки, а також визначення джерел загроз інформаційної безпеки та методів і засобів захисту конфіденційної інформації на підприємстві слід розробити алгоритм створення системи забезпечення інформаційної безпеки підприєиства, який може бути представлений наступною послідовністю дій.

1. Аналізується мета та задачі підприємства.
2. Аналізується стан підприємства та визначається необхідний рівень інформаційної безпеки підприємства. На основі цієї інформації оцінюються критерії інформаційної безпеки, їхні відхилення від порогових значень, аналізуються причини виникнення відхилень.
3. Розробляється концепція, політика та програми забезпечення інформаційної безпеки підприємства.
4. Проводиться діагностика підприємства. Аналізуються основні чинники зовнішнього середовища, які є джерелом загроз та внутрішні чинники, які впливають на інформаційну безпеку.
5. Формулюється перелік загроз інформаційної безпеки підприємства. Якщо цей перелік сформульований, то переходимо до розробки комплексу заходів, спрямованих на попередження виявлених загроз. Якщо цей перелік важко сформулювати, повертаємось до аналіз стану підприємства та визначення необхідного рівня інформаційної безпеки підприємства.
6. Розробляється комплекс заходів, спрямованих на попередження виявлених загроз або зниження витрат у випадку їхньої реалізації, у тому числі й заходів щодо локалізації загроз та ліквідації їхніх наслідків.
7. Реалізується програма забезпечення інформаційної безпеки.
8. Проводиться аудит інформаційної безпеки підприємства.
9. Здійснюється контроль по відхиленнях після проведення аудиту.

Запропонований алгоритм не прив’язаний до конкретних завдань та проблем, що стоять перед підприємством, тому він має універсальний характер і може використовуватися на усіх підприємствах галузі зв’язку.

Контрольні запитання та завдання

1. Назвіть складові інформаційної безпеки? Охарактеризуйте кожну складову.
2. Які існують технічні засоби захисту інформації?
3. Які існують канали витоку інформації? Охарактеризуйте існуючі канали витоку.
4. Назвіть основні напрямки нормативно-правового забезпечення захисту інформації в Україні?
5. Що включає економічна складова інформаційної безпеки?
6. Які методи використовуються для оцінки доцільності витрат на забезпечення інформаційної безпеки підприємства?
7. Що мається на увазі під „об’єктивними джерелами загроз” та „суб’єктивними джерелами загроз”?

8. Як класифікують загрози інформаційної безпеки?

9. Які існують методи захисту конфіденційної інформації на підприємстві?

10. Які існують засоби захисту конфіденційної інформації на підприємстві?

11. Які організаційні заходи використовують для захисту конфіденційної інформації?

12. З яких етапів складається алгоритм створення системи забезпечення інформаційної безпеки підприємства?

Завдання до самостійної роботи

1. Проаналізуйте аспекти організаційної складової забезпечення інформаційної безпеки:

- організаційно-правові аспекти;
- організаційно-технічні аспекти;
- організаційно-економічні аспекти;
- організаційно-управлінські аспекти.

РОЗДІЛ 5

ОСОБЛИВОСТІ ПОБУДОВИ АРХІТЕКТУРИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІДПОВІДНО ДО ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1 Особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки

Архітектура інформаційної безпеки визначає план та набір *принципів*, які описують структуру системи захисту інформаційної безпеки (СЗІБ) передавання інформації телекомунікаційною системою. Архітектура безпеки базується на концепціях, які розроблені в Рекомендаціях ITU-T X.200 та X.800 [217, 218] для ієрархічної семирівневої еталонної моделі архітектури Взаємодії Відкритих Систем (ВВС). Інформаційна безпека будується на принципах ієрархічної безпеки. Безпека забезпечується на кожному з рівнів моделі ВВС і функціональні послуги безпеки розподілено за цими рівнями. У моделі ВВС виокремлюються сім рівнів опрацювання інформації: 1 – фізичний; 2 – канальний; 3 – мережний; 4 – транспортний; 5 – сеансовий; 6 – представний; 7 – прикладний. Кожен рівень виконує певні завдання і функції та забезпечує умови функціонування суміжних рівнів. У моделі ВВС на кожному рівні існують окремі об'єкти, сервіс та послуги. Взаємодія об'єктів здійснюється через інтерфейси та протоколи. У моделі ВВС організовуються служби, які надають послуги. ITU-T стандартизує телеслужби, служби передавання, служби безпеки.

Служби безпеки забезпечують безпеку системи. Під терміном „безпека системи" розуміють такий стан системи, за якого мінімізовані уразливості ресурсів, що наявні у системі. Уразливість – це будь-яка слабкість, що її може бути використано для порушування структури системи чи інформації. Загроза ж – це потенційне порушування безпеки.

Інформаційна безпека телекомунікаційних мереж повинна забезпечуватись в умовах інтеграції інформаційних та телекомунікаційних технологій, конвергенції мереж і застосовуватись до радіо, оптичних і металевих голосових ліній зв'язку та передачі даних, а також в умовах дії на мережах операторів різних форм власності.

Архітектура інформаційної безпеки забезпечує всебічну, зверху-вниз та з кінця в кінець комплексну безпеку мереж та може застосовуватись до елементів, служб і застосувань для виявлення, прогнозування і коригування уразливості безпеки. Захисту підлягають усі складові елементи телекомунікаційних мереж: лінії, канали, системи передавання, обладнання, програмне забезпечення, інформація та персонал. Слід зазначити, що необхідно узгоджувати методи забезпечення інформаційної безпеки різних компонентів телекомунікаційних мереж, включаючи інформаційні ресурси, застосування, телекомунікаційні протоколи.

Комплексний підхід означає необхідність створення мережної інфраструктури забезпечення інформаційної безпеки, оскільки уразливість

будь-якої ланки мережі може створити проблеми для усіх її учасників – провайдерів, операторів і споживачів послуг. Кінцевою метою управлінської діяльності є вибір ефективних засобів протидії загрозам при реалізації системи інформаційної безпеки, вартість витрат на яку не перевищує вартість втрат, очікуваних від реалізації загроз.

Архітектура інформаційної безпеки логічно поділяє складний комплекс мережі між її кінцевими пунктами на окремі архітектурні компоненти інформаційної безпеки. Такий поділ враховує систематичний комплексний підхід до інформаційної безпеки з'єднання з кінця в кінець, який може використовуватись для планування засобів безпеки, а також для оцінки безпеки існуючих мереж.

Архітектура інформаційної безпеки будується з урахуванням загроз, проти яких необхідний захист, особливостей типів обладнання мереж, властивості групового обладнання та типів функцій мереж, які необхідно захищати.

Архітектура інформаційної безпеки розглядається у трьох архітектурних компонентах: механізмах безпеки, рівнях забезпечення безпеки та площинах забезпечення безпеки. Принципи, що описані архітектурою інформаційної безпеки, можуть бути застосовані до широкого різноманіття телекомунікаційних мереж незалежно від застосованої технології або розміщення в протокольному стеку.

Рекомендація ITU X.800 поділяє загрози на навмисні й випадкові і описує наступні загрози інформаційним ресурсам телекомунікаційних мереж [218]:

– знищення інформації і/або інших ресурсів;

– спотворення (псування) або модифікація інформації;

– розкрадання, видалення або втрата інформації і/або інших ресурсів;

– розкриття (компрометація) інформації;

– переривання послуг.

ITU прийняв модель мережної безпеки, розроблену в лабораторіях Белла, за основу нового стандарту забезпечення безпеки комп'ютерних та телекомунікаційних мереж, які передають інформацію за принципом „з кінця в кінець" [219].

5.2 Механізми забезпечення інформаційної безпеки

У рекомендації ITU-805 [218] наведена архітектура інформаційної безпеки у телекомунікаційних мережах загального користування (рис. 5.1) яка є концепцією захисту мережі механізмами захисту в кожній площині інформаційної безпеки з кожним рівнем забезпечення інформаційної безпеки для того щоб протидіяти визначеним загрозам безпеки і зменшити уразливості, які існують на кожному рівні та площині і, таким чином, послабити атаки на безпеку.

Рекомендація ITU X.805 [219] є функціональною багаторівневою наскрізною рамочною структурою. Основними її *компонентами* є:

– механізми захисту, які відносяться до конкретних аспектів забезпечення мережної безпеки, такі як автентифікація, або цілісність даних, що охоплюють ресурси, застосування мережі та інформацію користувачів;

– рівні захисту, які включають такі рівні, як інфраструктурний, послуг та застосувань, які розрізняються з точки зору вразливостей, що повинні блокуватись у відповідності з вимогами конкретного рівня;

– площини захисту, які охоплюють процеси менеджменту, мережного управління (сигналізації, контролю) з використанням різноманітних протоколів, наприклад, організацію віртуальних приватних мереж.

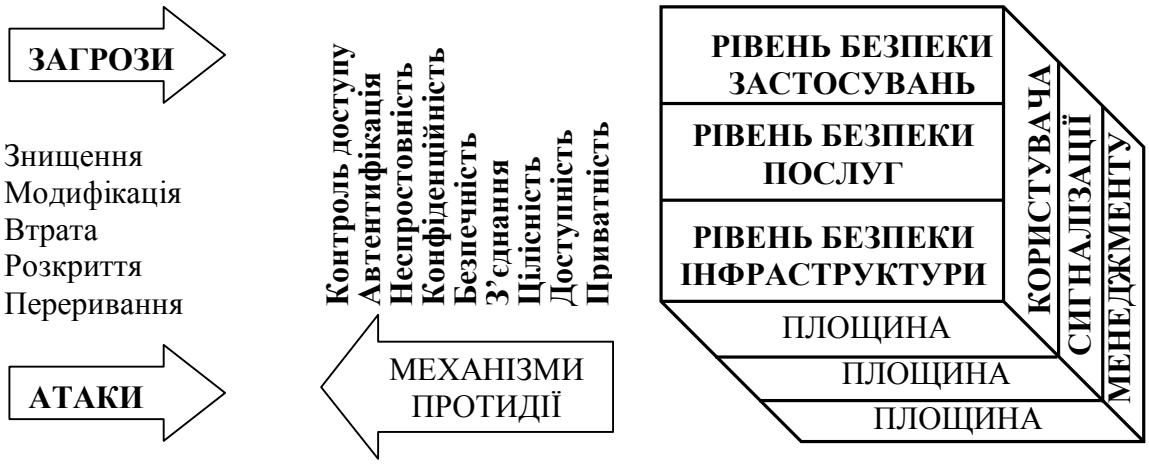


Рисунок 5.1 – Архітектура інформаційної безпеки телекомунікаційної мережі

Механізмами забезпечення інформаційної безпеки є набір заходів безпеки, які захищають проти всіх головних загроз безпеки, підтримують політику безпеки, яка визначена для окремої мережі, і сприяють дотриманню набору правил менеджменту безпеки. Такі механізми інформаційної безпеки не обмежуються мережею, а розповсюджуються на застосування, кінцевих користувачів та використовуються провайдерами служб або підприємствами, які надають послуги безпеки, відповідно до ліцензії на цей вид діяльності. *Механізмами забезпечення інформаційної безпеки є*: управління доступом, автентифікація, неспростовність причетності до участі в обміні, конфіденційність даних, безпечність комунікацій (з'єднання), цілісність даних, доступність, приватність.

Механізми забезпечення інформаційної безпеки застосовуються для протидії певній множині загроз. У табл. 5.1 відображається низка загроз, яким протистоять кожен з механізмів інформаційної безпеки.

Механізми забезпечення контролю доступу захищають проти неавторизованого використання ресурсів мережі. Контроль доступу гарантує, що лише авторизованим суб'єктам або пристроям дозволений доступ до елементів мереж, інформації, інформаційних потоків, послуг та застосувань. Зокрема, роле-орієнтований контроль доступу забезпечує різні рівні доступу, який гарантує, що суб'єкти можуть отримати доступ і виконувати дії з

елементами мереж, інформацією і потоками інформації, відповідно до своїх уповноважень.

Таблиця 5.1 – Матриця відповідності механізмів безпеки загрозам безпеки

Механізми інформаційної безпеки	Загрози безпеці інформації та іншим ресурсам				
	Знищення	Спотворення чи модифікація	Крадіжка або втрата	Розкриття (компрометація)	Перери-вання послуг
Управління доступом	Так	Так	Так	Так	-
Автентифікація	-	-	Так	Так	-
Неспростовність	Так	Так	Так	Так	Так
Конфіденційність	-	-	Так	Так	-
Безпечність з'єднання	-	-	Так	Так	-
Цілісність	Так	Так	-	-	-
Доступність	Так	-	-	-	Так
Приватність	-	-	-	Так	-

Механізми забезпечення автентифікації служать для підтвердження ідентичності взаємодіючих суб'єктів. Автентифікація гарантує валідність та законність об'єктів та суб'єктів, які беруть участь у взаємодії (наприклад, осіб, пристроїв, служб або застосувань), і забезпечує гарантію, що суб'єкт не робить спробу „маскараду" (маскування під авторизованого користувача), або неправомочного повтору попереднього зв'язку.

Механізми забезпечення неспростовності участі у обміні забезпечують засоби для попередження спроби відмови суб'єкта від виконаних специфічних дій відносно даних, а також доступності доказів різних дій, пов'язаних з телекомунікаційною мережею (таких як доказ зобов'язання, намірів або вручення, доказів авторства (джерела) даних, доказів володіння, доказів використання ресурсу). Ці механізми гарантують доступність свідчень, які можуть бути подані третьою стороною і використані для доказу того, що мав місце деякий випадок або деякий наслідок події.

Механізм забезпечення конфіденційності даних захищає дані від неавторизованого розкриття. Конфіденційність даних гарантує, що зміст даних не може бути зрозумілим неавторизованому суб'єкту. Для забезпечення конфіденційності даних часто використовуються методи шифрування, списки контролю доступу і допустимих файлів.

Механізми забезпечення безпечності зв'язку гарантують, що потоки інформації протікають лише між авторизованими кінцевими пунктами, що інформація не витікає або не перехоплюється з інформаційного потоку між цими кінцевими пунктами.

Механізми забезпечення цілісності даних гарантують коректність або точність даних. Дані захищені від неправомочної модифікації, вилучення, створення та копіювання даних і, крім того, забезпечується індикація цих не правочинних дій.

Механізми забезпечення доступності гарантують, що події, які впливають на мережу, не призводять до відмови від авторизованого доступу до елементів мережі, інформації, інформаційних потоків, послуг і застосувань. До цієї категорії включені засоби відновлення після катастроф, аварій та відмов обладнання телекомунікаційної мережі.

Механізми забезпечення приватності (Privacy) забезпечують захист інформації, яка може бути отримана від спостереження за функціонуванням мережі. Прикладом такої інформації можуть бути WEB-сторінки, які відвідав користувач, географічне місце розташування користувача, IP-адреси або DNS-імена пристроїв у телекомунікаційній мережі провайдера послуг. У вітчизняних нормативно-правових документах сфери ТЗІ механізми забезпечення приватності не визначаються, що певно є наслідком відсутності в Україні традицій недоторканості приватної власності. Конституцією України, Законом України „Про телекомунікації", (ст. 9), Ліцензійними умовами та іншими нормативними актами закріплена норма захисту таємниці зв'язку. Забезпечення конфіденційності інформації, яке стосується споживача, забезпечення і відповідальності за збереження відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, їх оплати, маршрутів передавання тощо" [96]. Механізми забезпечення приватності інформації щодо споживача повинні застосовуватись навіть в тому випадку, коли договором не передбачається надавання послуги забезпечення конфіденційності інформації споживача.

Механізми забезпечення інформаційної безпеки тісно пов'язані з механізмами забезпечення якості, надійності, стабільності та іншими показниками. З практичної точки важливо, що в рамках системи технічної експлуатації телекомунікаційних мереж вироблено розвинені засоби підтримки заданого рівня таких техногенних показників.

Як свідчить аналіз [99, 103], носії загроз безпеки поділяють на потенційні техногенні або стихійні і антропогенні. Як джерела загроз можуть бути як об'єктивні прояви, так і суб'єкти (особи). Джерела загроз можуть діяти як усередині систем, так і ззовні. Методи протидії внутрішнім і зовнішнім загрозам можуть бути різними. Зовнішня безпека передбачає захист телекомунікацій від стихійного лиха (пожежі, повені, землетрусу тощо) та від проникнення до телекомунікаційної мережі й вузлів з метою викрадення, одержання доступу до каналів та носіїв інформації, або виведення мережі з ладу. Внутрішня безпека має гарантувати надійну та коректну роботу телекомунікаційної мережі і вузлів, цілісність програмного забезпечення, інформації і технологічних даних.

Техногенні фактори впливають на зовнішню і внутрішню безпеку, вони порівняно добре вивчені, місця їхньої дії локалізовані і в системі технічної

експлуатації організовані заходи протидії завадам передаванню сигналів, збоям, відмовам обладнання тощо. Техногенні джерела загроз безпосередньо залежать від властивостей техніки та системи технічної експлуатації. Технічні засоби, що є джерелами потенційних загроз безпеці інформації також можуть бути зовнішніми та внутрішніми. До зовнішніх відносять: мережі зв'язку, високовольтні лінії електропередачі, мережі інженерних комунікацій (електро- і водопостачання), стихійні лиха тощо. До внутрішніх відносять: неякісні технічні засоби передавання і оброблення інформації, неякісні програмні засоби комутації та оброблення інформації, допоміжні засоби (охорони, сигналізації, службового зв'язку), інші технічні засоби, які застосовуються в інформаційно-телекомунікаційних системах.

Взаємозалежність і взаємозв'язок задач безпеки й якості технології відносно загроз техногенного і стихійного характеру можна проілюструвати таким чином (рис. 5.2), де суцільними стрілками показані відношення взаємозалежності та взаємозв'язку, а пунктирними – відношення опосередкованого входження.

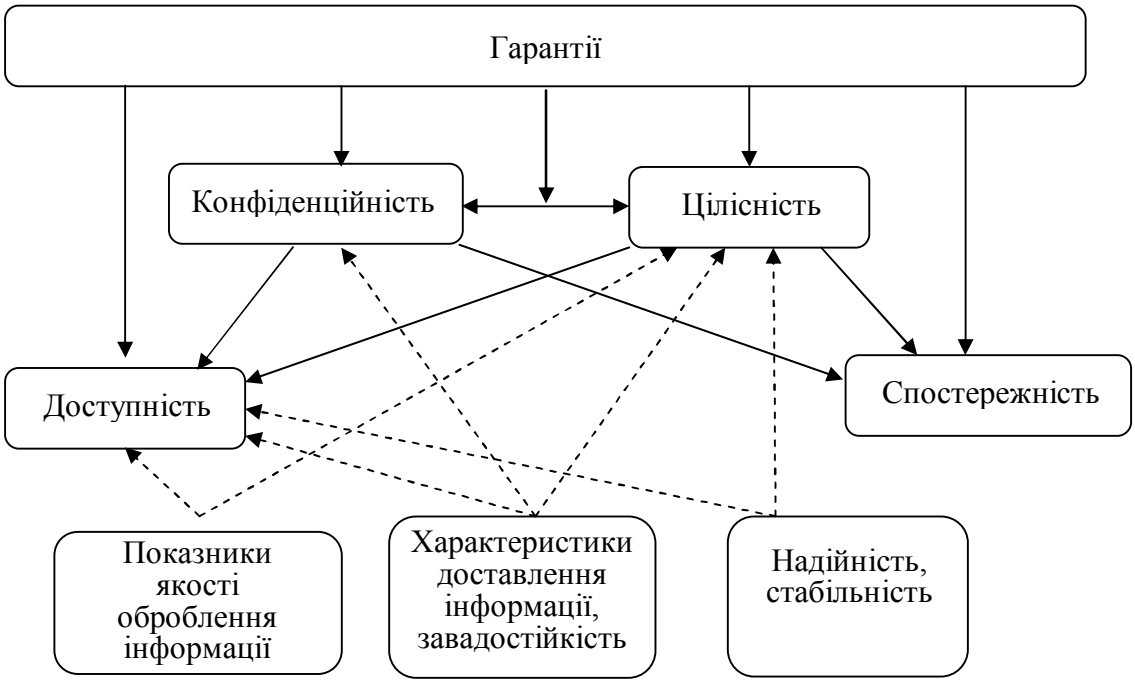


Рисунок 5.2 – Взаємозалежність задач безпеки й якості технологій

Конфіденційність залежить від цілісності і, у свою чергу, від надійності. Якщо цілісність і надійність системи буде порушена, знизиться ефективність механізмів конфіденційності [11]. Навпаки, порушення конфіденційності, наприклад, технологічної інформації, призведе до можливості „обходу" механізмів цілісності, доступності і спостережності.

Поняття „цілісность" включає в себе не лише збереження кількісних характеристик інформації – бітів і байтів, а й семантичних характеристик інформації – змісту повідомлень. У сфері безпеки властивості інформації розглядаються з точки зору техногенного й антропогенного впливів. Показник

цілісності є складною функцією надійності, спостережності й доступності. Якщо буде порушена цілісність системи, то це приведе до компрометації механізмів доступності і спостережності.

Показники доставляння інформації – ймовірність втрат і перекручувань повідомлень (достовірність), час затримки, помилки адресації споживача і джерела повідомлень – впливають на ефективність механізмів конфіденційності і цілісності. Характеристики доставляння інформації споживачеві та інших інформаційно-телекомунікаційних послуг в узагальненому вигляді входять до показників доступності і, частково, до показників конфіденційності й цілісності [11].

Показники якості в узагальненому вигляді входять до характеристик цілісності й доступності. Характеристики доставляння інформації споживачеві та інших інформаційно-телекомунікаційних послуг в узагальненому вигляді входять до показників доступності і, частково, до показників конфіденційності й цілісності [139]. Достовірність і надійність опосередковано взаємопов'язані з властивостями конфіденційності, цілісності, доступності. Кількісна або якісна недостатність компонентів системи впливає на показники ефективності захисту інформаційних ресурсів.

Вищезазначене підтверджується тим, що у міжнародних стандартах (BS ISO/IEC 7799:2000) спостерігається тенденція до поєднання сертифікації системи інформаційної безпеки із сертифікацією на відповідність стандартам якості ISO 9001 [42].

Усі задачі інформаційної безпеки й якості залежать від розв'язання задач забезпечення гарантій. При розробці й створенні системи необхідно забезпечити певний рівень гарантованості того, що для виконання кожної з задач безпеки визначені функціональні вимоги, а система розроблена і створена з потрібним рівнем якості.

Розглянемо тепер деякі варіанти постановки задачі управління розподілом послуг та механізмів захисту в залежності від простору (середовища) розподілу. На основі систематизації підходів можна виділити чотири варіанти розподілу [101, 125, 148]:

1) між рівнями архітектури взаємодії відкритих систем;

2) між компонентами, на які декомпозується інформаційно-телекомунікаційна система. Тут можливі різні підваріанти:

– між вузлами, каналами, локальними мережами, системами оброблення інформації, системами управління базами даних тощо;

– між прикінцевим обладнанням, елементами мережі доступу, цифровими комутаційними системами та транспортною мережею;

– між прикінцевими пунктами і мережею (системою) передавання;

3) між рівнями стеку мережних протоколів;

4) між процесами оброблення інформації.

Розподіл засобів і систем захисту за стадіями життєвого циклу та інші такого виду способи розподілу тут не розглядаються. Існуюча нормативно-правова база чітко визначає розподіл заходів захисту у рамках комплексного підходу [110, 111, 114].

Комплексний підхід реалізується через конкретні заходи на законодавчому, адміністративному, процедурному, програмно-технічному, фізичному рівнях.

На законодавчому рівні напрацьовані закони, нормативні акти, інструкції та розпорядження щодо правових основ використання, збереження, організації доступу до інформаційних ресурсів та телекомунікаційних послуг.

На адміністративному рівні визначаються вимоги політики безпеки, адміністративні інструкції, політика роботи з персоналом та споживачами.

На процедурному рівні визначаються способи реалізації політики безпеки, організаційні заходи і процедури захисту, контроль за роботою персоналу.

На програмно-технічному рівні реалізуються технічні рішення щодо захисту конкретних інформаційних ресурсів, засобів захисту й контролю.

Систематичний підхід до забезпечення інформаційної безпеки. Розглянемо деякі з варіантів розподілу послуг і механізмів захисту. На основі аналізу, можна виділити чотири варіанти розподілу:

Найбільш детально розв'язана задача розподілу послуг та механізмів безпеки у еталонній моделі архітектури ВВС. У моделі ВВС виокремлюються сім рівнів опрацювання інформації: 1 – фізичний; 2 – канальний; 3 – мережний; 4 – транспортний; 5 – сеансовий; 6 – представний; 7 – прикладний.

Кожен рівень виконує певні завдання та функції й забезпечує умови функціонування суміжних рівнів.

Архітектура безпеки також будується на принципах ієрархічної рівневої безпеки, тобто безпека забезпечується на кожному з рівнів моделі ВВС і функціональні послуги безпеки розподілено за цими рівнями й етапами зв'язку. В табл. 5.2 показано на яких рівнях може бути надано сервіс безпеки [217].

Сервіс фізичного рівня є основоположним. Сервіс безпеки мережного рівня має велике значення за своєю природою. Тому розглянемо його детальніше.

Мета захисту фізичного рівня полягає в повному захисті фізичного потоку бітів даних (сервіс засекречування з'єднання) і забезпечуванні конфіденційності трафіку (сервіс засекречування потоку даних).

Сервіс безпеки фізичного рівня використовується окремо чи в комбінації. Повну конфіденційність з'єднання може бути забезпечено, наприклад за дуплексного режиму синхронного, двоточкового передавання.

За інших видів передавання, наприклад за асинхронного передавання може бути забезпечено обмежену конфіденційність з'єднання.

Захист фізичного рівня забезпечується за допомогою пристрою шифрування.

Мережний рівень внутрішньо організовано для забезпечування виконання протоколами таких операцій: доступ до мереж; злиття залежних підмереж; злиття незалежних підмереж; передавання і маршрутизація. Протоколи мережної служби ВВС, які виконують доступ до мереж, операції з'єднання й маршрутизації, застосовують ідентичні механізми безпеки.

Таблиця 5.2 – Розподіл послуг безпеки за рівнями моделі архітектури Взаємодії Відкритих Систем

№ пп.	Послуги	Рівні ВВС						
		1	2	3	4	5	6	7*
1	Автентифікування однорівневих об’єктів	·	·	+	+	·	·	+
2	Автентифікування джерела даних	·	·	+	+	·	·	+
3	Контроль доступу	·	·	+	+	·	·	+
4	Конфіденційність (засекречування) з’єднання	+	+	+	+	·	+	+
5	Конфіденційність (засекречування) без установлення з’єднання	·	+	+	+	·	+	+
6	Конфіденційність (засекречування) обраних полів	·	·	·	·	·	+	+
7	Конфіденційність (засекречування) трафіку (потоку даних)	+	·	+	·	·	·	+
8	ілісність з’єднання з відновлюванням	·	·	·	+	·	·	+
9	ілісність з’єднання без відновлювання	·	·	+	+	·	·	+
10	ілісність обраних полів даних з’єднання	·	·	·	·	·	·	+
11	ілісність без установлення з’єднання	·	·	+	+	·	·	+
12	Цілісність обраних полів без установлення з’єднання	·	·	·	·	·	·	+
13	Захист від відмовлення партнерів зв’язку від факту прийняття-передавання повідомлення з доказом щодо джерела	·	·	·	·	·	·	+
14	Захист від відмовлення партнерів зв’язку від факту прийняття-передавання повідомлення з доказом щодо доставляння	·	·	·	·	·	·	+

У таблиці уведені позначки:

1 ... 7 – номери рівнів від 1-го – фізичного до 7-го – прикладного;

+ – сервіс має бути включено до стандартів для рівня як надавана опція;

- – сервіс не надається;

* – даний сервіс записано до 7-го рівня тому, що прикладні процеси в прикінцевих пристроях можуть самі надавати сервіс безпеки, користуючись при цьому й сервісом безпеки прикладного рівня. Розподіл функцій безпеки між прикладним та іншими рівнями має вирішуватись у результаті оптимізації витрат.

Послуги безпеки забезпечуються у такий спосіб:

– послуга автентифікації однорівневих об’єктів забезпечується обміном захищеною автентифікацією, чи обміном захищеними паролями й механізмами цифрового (електронного) підпису;

– послуга автентифікації джерела даних може бути забезпечена шифруванням чи механізмами підпису;

– послуга контролю доступу забезпечується використанням механізмів контролю доступом;

– послуга конфіденційності з'єднання забезпечується механізмом шифрування та/чи контролем маршрутизації;

– послуга конфіденційності без установлення з'єднання забезпечується механізмом шифрування та/чи керування маршрутизацією;

– послуга конфіденційності трафіку досягається механізмом заповнення трафіку фоновою інформацією в поданні з послугою конфіденційності на мережному чи канальному рівні та/чи контролем маршрутизації;

– послуга цілісності з'єднання без відновлювання забезпечується використанням механізму цілісності даних, іноді в поєднанні з механізмом шифрування;

– послуга цілісності без встановлення з'єднання забезпечується використанням механізму цілісності даних, іноді у поєднанні з механізмом шифрування.

Характеристики даних, які передаються між двома або більше об'єктами, такі як цілісність, джерело, час і одержувач, можуть підтверджуватись за допомогою механізму нотаріального засвідчення, що має бути засвідчено третьою довіреною стороною.

Керування доступом на мережному рівні дозволяє прикінцевій системі контролювати шифрування мережного з'єднання, а підмережам – контролювати використання ресурсів мережного рівня тощо. Механізми контролю доступом можуть використовуватися для контролю доступу до підмереж суб'єктів зв'язку і контролю доступу до прикінцевих систем.

Досягнення високих рівнів безпеки неможливе без загальних механізмів безпеки, які застосовуються у будь-яких системах безпеки. Їх вибір залежить від рівня потенційних загроз й цінності інформації, яка захищається. Окрім того, має застосовуватись низка механізмів, які повинні бути забезпечені поза межами відкритої системи, зокрема: довірче функціонування та фізична безпека, грифи таємності, виявлення подій, які порушують безпеку, журнал реєстрування з безпеки, відновлювання нормального функціонування служби безпеки після порушення.

Довіра до методів, зазвичай, установлюється за межами середовища ВВС. Процедури, використовувані для забезпечування довіри, можуть бути розміщені в апаратних засобах та програмному забезпеченні. Ці процедури, в основному, дорогі й важко здійснювані. Проблеми можуть бути мінімізовані при виборі архітектури, яка дозволяє здійснювати функції безпеки в окремих модулях, які можуть бути забезпечені функціями, що не пов'язані з безпекою. Фізичні заходи захисту та захист від персоналу будуть завжди потрібні для гарантування повної безпеки. Всі системи в решті-решт покладаються на певну форму фізичного захисту й на довіру персоналу, що використовує системи. Чинні процедури мають бути визначені відповідними операціями й доведені до відповідального персоналу.

Розглянемо *розподіл окремих послуг безпеки між елементами архітектури*, на які декомпозуються інформаційно-телекомунікаційні системи.

Конфіденційність забезпечує недоступність семантичної складової інформації для несанкціонованого доступу. Механізми забезпечення конфіденційності можна концентрувати на прикінцевих пунктах та/або вузлах чи розподіляти за складовими системи передавання. Довгий час інформаційній безпеці телекомунікаційних мереж приділялось недостатньо уваги. Компенсаційний метод захисту був єдиною концепцією створення захищених каналів зв'язку. Це стало закріплюватись і у нормативній базі. Установлено, що конфіденційність інформації, яка є державними інформаційними ресурсами, під час передавання мережею передачі даних забезпечує власник автоматизованої системи (АС) або оператор, але за договором з власником АС [4].

При застосуванні шифрування адреса повинна бути виокремлена явно в пункті передавання й пункті доступу. За цією прикметою розрізнюють між канальне шифрування й між кінцеве (неперервне) шифрування. За між канального шифрування дані зашифровуються в кожному каналі й дешифруються (і тому є уразливі) у транзитних пунктах передавання чи пункті доступу. За між кінцевого шифрування лише адреса (чи подібні управлінські дані) є наявні в чистому вигляді в пункті передавання чи пункті доступу. Текст залишається зашифрованим. Між кінцеве шифрування є більш бажане, але має більш складне архітектурне виконання, особливо якщо включено розподіл електронних ключів (функцію керування ключами). Між канальне й між кінцеве шифрування може бути об'єднано.

Засоби захисту деяких властивостей безпеки принципово необхідно розподіляти по системі. Порушення доступності внаслідок, наприклад, перенавантаження мережі при DoS-атаках неможливо компенсувати в прикінцевих пунктах. Послуги забезпечення доступності мають розподілятись по мережі рівномірно. Недостатність апаратних та програмних засобів мережі має бути усунена, а критичні за пропускною спроможністю ланки мережі мають бути доповнені необхідними додатковими ресурсами. Аналогічно рівномірно мають розподілятись засоби забезпечення спостережності. Постійний аудит мереж зв'язку з метою виявлення їх вразливості та можливих загроз, забезпечує виявлення слабкої ланки, а рівень захищеності слабкої ланки визначає, врешті-решт, рівень інформаційної безпеки в цілому.

Телекомунікаційні мережі розвиваються в бік універсальності, мультисервісності. При цьому кількість і якість телекомунікаційних послуг невпинно зростає. Є деякі особливості в задачі розподілу систем захисту у мережах наступного покоління (Next Generation Network – NGN), в яких на мережному рівні передбачається застосування IP-орієнтованих протоколів. В NGN виділяють такі шари (площини): шар абонентського доступу, що базується на трьох середовищах передавання – металевому кабелі, оптоволокні і радіоканалах; шар комутації, – комутації каналів чи комутації пакетів; шар транспортного рівня з програмним управлінням, побудований на Softswitch – програмних комутаторах за технологією IP; шар інтелектуальних послуг та різноманітного сервісу; шар експлуатаційного керування. Створення в NGN фактичного єдиного централізованого експлуатаційного керування мережею гостро ставить проблеми інформаційної безпеки. NGN – це мережа, яка

підтримує механізми якості обслуговування (QoS) та інформаційної безпеки. Відповідні елементи установлюються, здебільшого, у шарі керування, а контрольовані параметри визначаються у транспортній мережі [92]. Слабким місцем поки що є низька захищеність протоколів сигналізації мереж IP. Стандарти безпеки сигнальної мережі, побудованої на основі IP-технологій, знаходяться у стадії розробки.

На кожному рівні і різних рівнях можуть взаємодіяти різні оператори. Зверху послуг оператора інфраструктури може знаходитись шар послуг сервіс-провайдера. Розподіл послуг та механізмів безпеки має забезпечити безпеку за будь-якої взаємодії суб'єктів відносин у мережі. Маємо задачу розподілу послуг безпеки між рівнями стеку мережних протоколів.

Розподіл окремих послуг безпеки, а саме, контролю інваріантів коректного оброблення інформації в корпоративній системі та моніторингу стану захищеності, між процесами оброблення інформації розглянуті в [125].

Методичний підхід до управління інформаційною безпекою телекомунікаційної мережі полягає у розгляді кожного механізму безпеки на кожному рівні забезпечення інформаційної безпеки та кожній площині інформаційної безпеки. Утворюється дев'ять модулів безпеки, кожен з яких комбінує вісім механізмів безпеки, які застосовуються до окремого рівня забезпечення безпеки в окремій площині інформаційної безпеки. При цьому ясно, що в залежності від вимог до даної мережі, можливо не потрібно мати всі запроваджені архітектурні елементи, тобто інколи не потрібно мати повний набір механізмів безпеки, рівнів забезпечення інформаційної безпеки або площин забезпечення інформаційної безпеки. Розподіл механізмів безпеки за рівнями моделі архітектури ВВС та площинами моделі мереж наступного покоління, наведено в табл. 5.3. Площини архітектури мережі наступного покоління NGN наведені у відповідності з науковою працею В. Теслі, А. Бабасюка, Сікорського В.А. Рудниченка [191].

Площина абонентського доступу базується на трьох середовищах передачі: металевому кабелі, оптоволокні та радіоканалах.

У площині комутації реалізується комутація пакетів та/або (на перших етапах) комутація каналів і знаходиться структура мультисервісних вузлів доступу.

Площину програмного управління складають програмні комутатори (Softswitch).

Верхня площина забезпечує реалізацію інтелектуальних послуг та експлуатаційного управління.

Для забезпечення інформаційної безпеки телекомунікаційних мереж з кінця в кінець механізми безпеки повинні застосовуватись до ієрархії обладнання мережі з групуванням їх у сімейства засобів, які описуються як рівні забезпечення безпеки.

У свою чергу, на кожному з рівнів функціонують деякі типи механізмів інформаційної безпеки, які кваліфікуються як площини інформаційної безпеки.

Визначено такі ієрархічні рівні мережно-орієнтованих засобів забезпечення інформаційної безпеки:

– рівень забезпечення інформаційної безпеки інфраструктур;
– рівень забезпечення безпеки послуг;
– рівень забезпечення безпеки застосувань.

Таблиця 5.3 – Розподіл механізмів безпеки за Рекомендаціями ITU X.800, X.805 та моделлю мереж наступного покоління

Механізми безпеки		Площини моделі мереж наступного покоління						
		абонентського доступу		комутації	програмного управління	інтелектуальних послуг та експлуатаційного управління		
Рекомендації ITU		Рівні моделі архітектури ВВС						
X.800	X.805	1	2	3	4	5	6	7
Керування доступом		Ні	Ні	Так	Так	Ні	Ні	Так
(Обмін) автентифікацією		Ні	Ні	Так	Так	Ні	Ні	Так
Цифровий підпис	Неспростовність	Ні	Ні	Так	Так	Ні	Ні	Так
Нотаріальне засвідчування		Ні	Ні	Ні	Ні	Ні	Ні	Так
Шифрування	Конфіденційність	Так	Так	Так	Так	Ні	Так	Так
Заповнення трафіку	Безпечність з'єднання	Так	Ні	Так	Ні	Ні	Ні	Так
Контроль маршрутизації		Так	Так	Так	Так	Ні	Так	Так
Цілісність (даних та) ресурсів		Ні	Ні	Так	Так	Ні	Ні	Так
Доступність		Так	Так	Так	Так	Ні	Так	Так
Приватність		Ні	Ні	Так	Так	Ні	Ні	Так

Кожен рівень має різні уразливості безпеки. Механізми інформаційної безпеки застосовуються до рівнів забезпечення безпеки, щоб зменшити уразливості, які існують на кожному рівні та, таким чином, послабити атаки на безпеку. На кожному з рівнів пропонується така гнучкість механізмів протидії потенційним загрозам, яка найбільш придатна для окремого рівня інформаційної безпеки. У Рекомендації ITU X.805 [219] підкреслюється, що всі три рівні забезпечення інформаційної безпеки можуть бути застосовані до кожного з семи рівнів моделі взаємодії ВВС, оскільки кожен рівень моделі ВВС має свою інфраструктуру, надає свої послуги і має свої застосування.

Площина інформаційної безпеки – це деякий тип механізмів інформаційної безпеки, функціонуючих у захищеній мережі. Визначаються такі площини безпеки інформації для представлення трьох типів захищеного функціонування, яке має місце у мережі: площина безпеки менеджменту, площина безпеки сигналізації та контролю, площина безпеки кінцевого користувача. Ці площини безпеки характеризують специфічні потреби

інформаційної безпеки, пов’язані з виконанням менеджменту мережі, організацією контролю і сигналізації мережі та відповідними діями кінцевого користувача. Мережі повинні проектуватись таким чином, щоб події на одній площині безпеки були б повністю ізольовані від подій в інших площинах безпеки. Наприклад, потік запитів до служби доменних імен у площині кінцевого користувача, ініційованих запитами кінцевого користувача, не повинні блокувати інтерфейс керування, адміністрування, технічного обслуговування та забезпечення у площині менеджменту, який дозволяв би адміністратору виправляти проблему. Кожен тип описаних функцій мережі має свої власні специфічні потреби безпеки. Концепція площин інформаційної безпеки дозволяє диференціювати специфіку безпеки відносно до пов’язаних з ними дій і можливістю розглядати їх незалежно.

На основі розглянутих особливостей побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки та розподілу послуг безпеки за рівнями моделі архітектури взаємодії відкритих систем, можна ставити конкретні задачі щодо визначення організаційно-правових складових регламентування управлінської діяльності інформаційної безпеки та розробки основних принципів і засад інформаційної безпеки телекомунікаційних мереж загального користування (ТМЗК).

5.3 Принципи та засади інформаційної безпеки телекомунікаційних мереж загального користування

Стрімкий розвиток використання інформаційно-комунікаційних технологій в органах державного управління ініціює необхідність інформаційної безпеки держави. Критично важливим державним ресурсом, який все більше впливає на національну безпеку, стає інформація, що циркулює в автоматизованих системах управління та телекомунікаціях. Ці системи є невід’ємним компонентом структури управління державою, економікою, фінансами й обороною. Захист інформації у телекомунікаційних мережах набуває найважливішого значення.

Телекомунікації є важливою інфраструктурою суспільства, яка забезпечує оперативне та інтерактивне транспортування інформації в процесі соціальної й економічної діяльності суспільства. Проблема інформаційної безпеки телекомунікаційних мереж та систем займає одне з особливих місць у загальній системі інформаційної безпеки України. Вона не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації та інформаційної безпеки. Загальнонаціональний рівень важливості інформаційної безпеки країни, її комплексний характер потребують забезпечення безпечного функціонування телекомунікаційних мереж загального користування.

Проблеми технічного захисту інформації мають своє продовження у проблемах захисту інформаційних ресурсів та інформаційної інфраструктури, переростаючи у проблеми інформаційної безпеки інформаційно-

комунікаційних технологій. Замість концепції ТЗІ в галузі зв'язку [89], не відміняючи, а доповнюючи та розвиваючи її, став чинним Закон України „Про основи національної безпеки України" [58], внесені зміни до Закону України „Про захист інформації в автоматизованих системах" [53], задіяний новий Закон України „Про телекомунікації" [61], прийняті закони, укази, постанови щодо електронних документів, електронного документообігу, електронного цифрового підпису, електронної інформаційної системи „Електронний Уряд".

Розробка основних положень (організаційно-правових засад) системи інформаційної безпеки ТМЗК дасть змогу створити і запровадити політику інформаційної безпеки ТМЗК та її елементів. Засади стосовно організації інформаційної безпеки телекомунікаційних мереж загального користування складаються з основних положень, відображених на рис. 5.3.

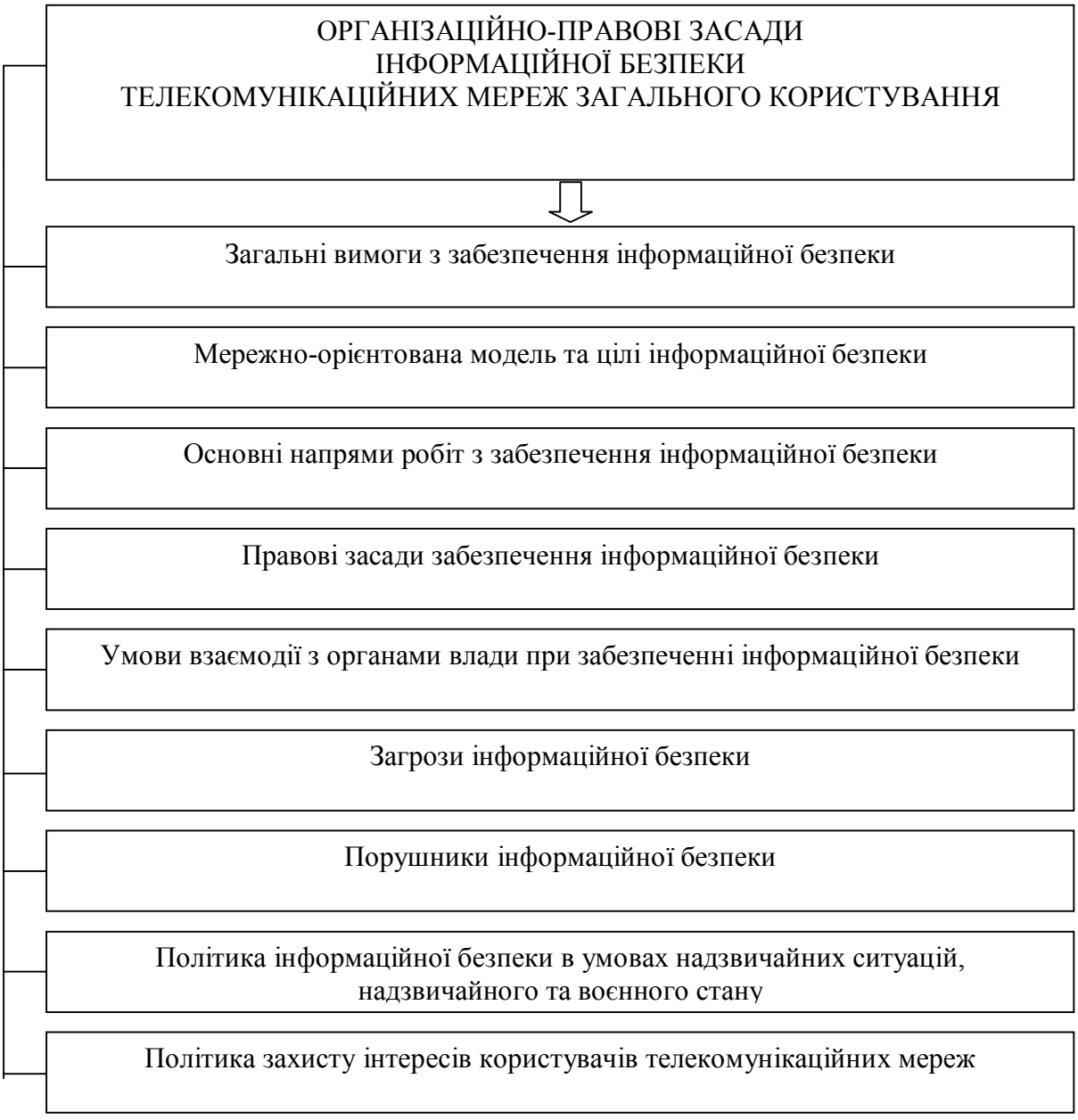


Рисунок 5.3 – Засади стосовно організації інформаційної безпеки телекомунікаційних мереж загального користування

Викладення основних положень засад стосовно організації інформаційної безпеки ТМЗК та їх обґрунтування. Засади щодо організації інформаційної безпеки ТМЗК викладають систему поглядів, основних принципів, розкривають основні напрями забезпечення безпеки інформаційної сфери ТМЗК. Розроблення засад інформаційної безпеки телекомунікаційних мереж загального користування включається в методологію розробки політики інформаційної безпеки інформаційно-телекомунікаційних мереж.

Розроблення засад виконано на підставі аналізу наступних факторів:

– правових засад; вимог до забезпечення інформаційної безпеки згідно з завданнями і функціями телекомунікаційних мереж як частини інформаційно-комунікаційних технологій;

– загроз, від яких зазнають впливу інформація, інформаційні ресурси та інформаційна інфраструктура ТМЗК, що підлягають захисту.

Загальні вимоги з забезпечення інформаційної безпеки ТМЗК. Загальні вимоги до інформаційної безпеки повинні виходити із переліку найбільш небезпечних загроз інформаційній безпеці ТМЗК, отримання на основі аналізу уразливості ТМЗК або політики інформаційної безпеки ТМЗК і можливих впливів порушника на інформаційну сферу ТМЗК з точки зору ризику інформаційної безпеки і можливого збитку користувачу, оператору ТМЗК або державі, який може бути нанесений ТМЗК появою того чи іншого наслідку впливів порушника.

Загальні вимоги повинні включати: вимоги з забезпечення інформаційної безпеки ТМЗК та вимоги при взаємодії ТМЗК між собою.

Вимоги з забезпечення інформаційної безпеки ТМЗК повинні включати: вимоги з забезпечення взаємодії з користувачами; вимоги з забезпечення інформаційної безпеки процесів функціонування мережі; вимоги до взаємодії елементів мережі між собою; вимоги до процесу керування ТМЗК; вимоги до процесу моніторингу ТМЗК.

Вимоги по забезпеченню інформаційної безпеки взаємодії ТМЗК між собою повинні включати: вимоги до взаємодії систем забезпечення інформаційної безпеки між собою; вимоги з захисту інформаційних сфер кожної з мереж від впливу порушника з боку взаємодіючої мережі.

Оператор ТМЗК може забезпечити реалізацію додаткових вимог з забезпечення надаваних послуг зв’язку з захисту інформації користувача на договірній основі.

Основою інформаційної безпеки ТМЗК є система забезпечення інформаційної безпеки (СЗІБ). При розробці, створенні й експлуатації СЗІБ ТМЗК необхідно керуватись наступними принципами:

1. Створення СЗІБ, у першу чергу, повинно передбачати забезпечення базового рівня інформаційної безпеки ТМЗК. Загальні вимоги до базового рівня інформаційної безпеки ТМЗК визначаються політикою інформаційної безпеки галузі.

2. Додаткові вимоги інформаційної безпеки в інтересах державної системи урядового зв’язку, національної системи конфіденційного зв’язку,

органів з надзвичайних ситуацій, безпеки, оборони й охорони правопорядку підприємство забезпечує у відповідності з Законом „Про телекомунікації” [61] та чинними нормативно-правовими актами [109…123].

3. Уведення додаткових вимог до інформаційної безпеки ТМЗК в інтересах користувачів МЗК може здійснюватись відповідно з вимогами користувачів на договірній основі.

4. Рівень інформаційної безпеки ТМЗК повинен визначатись на основі вимог органів державної влади та користувачів МЗК.

5. Рівні інформаційної безпеки ТМЗК, методи, дії, процедури і вартість СЗІБ повинні відповідати ступеню потенційної можливості нанесення збитків державі, оператору або користувачу ТМЗК певними діями порушника на інформаційну безпеку.

6. Розробка СЗІБ повинна здійснюватись на основі чинних нормативно-правових актів України в області зв’язку, зокрема наказів ДССЗЗІ України.

7. Забезпечення інформаційної безпеки повинно досягатись комплексним використанням усієї сукупності нормативних, правових, організаційно-технічних, програмних і криптографічних методів захисту, а також організацією неперервного, всебічного контролю за ефективністю реалізованих заходів захисту.

8. У складі СЗІБ повинні використовуватись тільки атестовані на відповідність вимогам інформаційної безпеки ТМЗК механізми безпеки і засоби захисту.

9. Використання у складі СЗІБ імпортних технічних і програмних засобів зв’язку з урахуванням запроваджених заходів захисту не повинно погіршувати характеристики інформаційної безпеки ТМЗК.

10. Проектування і створення механізмів безпеки і засобів захисту для ТМЗК повинні проводитись виключно підприємствами, які мають ліцензію на цей вид діяльності.

11. Проектування СЗІБ повинне здійснюватись, як правило, одночасно з проектуванням ТМЗК.

12. Повинна бути розроблена політика безпеки, вимог до інформаційної безпеки ТМЗК, процедур контролю якості процесів передавання інформації та їх відновлення в умовах впливу порушника на інформаційну сферу ТМЗК і засоби оцінки ступеня забезпечення інформаційної безпеки ТМЗК.

13. Прийняті заходи забезпечення інформаційної безпеки ТМЗК не повинні перешкоджати доступу правоохоронних органів у передбачених законодавством України випадках до інформації конкретних користувачів.

14. Прийняті заходи забезпечення інформаційної безпеки ТМЗК повинні забезпечити відсутність можливості обходу засобів захисту і «потаємних» входів у об’єкти МЗК.

15. СЗІБ повинна забезпечувати взаємодію із СЗІБ системи керування ТМЗК.

16. Забезпечення інформаційної безпеки ТМЗК при взаємодії з мережами зв’язку інших операторів ТМЗК повинне здійснюватись на основі єдиної технічної політики галузі.

17. Своєчасне запобігання і ліквідація наслідків впливу порушника повинні забезпечуватись узгодженими діями з органами державної влади, іншими операторами і користувачами ТМЗК, які мають обов'язки згідно з Законом України „Про телекомунікації".

18. Методи, дії і процедури забезпечення інформаційної безпеки ТМЗК повинні бути скоординовані з заходами, діями і процедурами системи керування ТМЗК.

19. У ТМЗК необхідно забезпечити контроль та облік ефективності СЗІБ, а також удосконалення критеріїв і методів оцінки ефективності СЗІБ.

20. У функціонуванні СЗІБ ТМЗК не повинно бути перерв у роботі, викликаних ремонтом засобів захисту, зміни паролів, відключення електроживлення тощо.

21. Доступ персоналу до захищених ресурсів має бути розмежованим у відповідності з політикою інформаційної безпеки, втіленою у виконувані посадові інструкції.

Мережно-орієнтована модель та цілі інформаційної безпеки. При формуванні цілей та задач системи інформаційної безпеки ТМЗК необхідно врахувати її особливу роль у рамках національної безпеки держави та тенденцію до розширення об'єкта захисту. В інформаційно-телекомунікаційних системах повинен забезпечуватись захист не тільки таємної, а й відкритої інформації, яка є власністю держави, також інформації про особу (персональних даних).

Виключна роль телекомунікацій в сучасних інфраструктурах країни проявляється в тому, що національна безпека України залежить від цілісності, надійності й готовності критичних фізичних та інформаційних інфраструктур. Поняття „критичної інфраструктури" включає в себе сукупність фізичних або віртуальних систем і засобів, важливих для держави настільки, що їх вихід з ладу або знищення можуть призвести до згубних наслідків в області економіки, оборони, охорони здоров'я та національної безпеки. Телекомунікаційні мережі, інформаційна інфраструктура яких є сукупністю центрів зберігання, оброблення і передавання інформації, каналів інформаційного обміну, ліній зв'язку, систем і засобів забезпечення інформаційної безпеки, можна вважати найкритичнішою інфраструктурою країни. Вирішальне значення має розробка заходів з захисту, дублювання, мобільності, поєднання, відновлення й безпеки телекомунікаційних систем країни для використання в інтересах управління державою критичних інформаційних послуг та телекомунікаційних ресурсів, як у надзвичайних умовах, так і в режимі нормального функціонування. Тому, до інформаційної безпеки інформаційної інфраструктури ТМЗК законом України „Про телекомунікації" ставляться вимоги забезпечення живучості, що передбачає підтримання таких властивостей, як надійність функціонування мережі, її готовність, працездатність, стабільність, доступність до інформаційних ресурсів та інформаційних систем, цілісність структури, відновлюваність.

Критичність телекомунікацій зв'язана також з проблемою забезпечення безпеки суспільно політичних відносин, зокрема з виникненням загроз нового

типу – впливів на системи зв'язку, збирання й обробленню інформації. Такі засоби впливу базуються на автоматизованому аналізі структури повідомлень, слідкуванні за ключовими словами, синтезуванні мови у реальному масштабі часу. Результатом впливу є створення непомітних завад інтелектуального впливу шляхом блокування, підміни у повідомленнях ключових елементів і навіть уведення у повідомлення несправжніх хибних або фальшивих ключових елементів. Небезпека таких загроз у тому, що фальсифікація може проводитись не лише власником чи розпорядником інформації, за що він несе відповідальність перед законом, а і противником, приховано, під час передавання інформації телекомунікаційною мережею. Навмисне руйнування, переривання або перекручення даних у цифровій формі або потоків інформації, мають широкомасштабні наслідки у політичному, релігійному або ідеологічному планах. Інформація викрадається, перекручується, обмежується, фільтрується з метою впливу (або виключення впливу) на психіку людини, психологію великих мас людей, суспільну свідомість з метою примусити їх думати і діяти в потрібному для того, хто організовує та здійснює цей вплив, напрямі. Рівень небезпечності загроз цільового інформаційного впливу прямо пропорційні рівню технологічного розвитку мереж та масштабам застосування комп'ютерів у системах управління мережею, галуззю і державою в цілому. В зв'язку з цим, для телекомунікаційних мереж зростає важливість вимог забезпечення цілісності та достовірності переданої інформації, захисту від порушень правил маршрутизації, точності й своєчасності доставки інформації (мінімальної затримки повідомлень), а також захисту від несанкціонованого доступу до інформаційних ресурсів мереж та забезпечення фізичної безпеки інформаційної інфраструктури.

Телекомунікації забезпечують транспортування інформації в інтересах її оброблення автоматизованими системами на об'єктах інформаційної діяльності – і, як наслідок, у телекомунікаціях маємо дещо інший підхід до оцінки цінності (вартості й ціни) інформації, ніж на звичайних об'єктах інформаційної діяльності. При цьому, під транспортуванням інформації, у відповідності з рекомендаціями ITU-T, розуміється не тільки функції перенесення (передавання) інформації в просторі, а й мережні функції, такі як моніторинг процесу перенесення інформації, аудит і оперативне перемикання каналів і маршрутів, своєчасне відновлення порушеного процесу передавання інформації, керування мережами зв'язку, адміністрування. Вартість транспортування (доставляння) інформації не залежить від цінності інформації, точніше цінність інформації визначається не оператором, а клієнтом, який обирає відповідні якість і вид телекомунікаційних послуг. Оператор надає телекомунікаційні послуги згідно з певною шкалою якості послуг або певного рівня захищеності інформації під час її передавання мережею. А клієнт сам обирає на договірних засадах рівень якості телекомунікаційної послуги і захищеності своєї інформації. В телекомунікаційній мережі відсутні засоби визначення категорії інформації, яка передається нею. Категорію інформації призначає, явно (як в телеграфному зв'язку) чи приховано, відправник (власник чи розпорядник) інформації. Згідно з нормативно-правовими документами

сфери ТЗІ, відповідальність за забезпечення конфіденційності інформації несе власник інформації. Оператор може надавати послуги забезпечення конфіденційності лише за договором з власником інформації. В результаті склався такий підхід до побудови системи інформаційної безпеки телекомунікаційних мереж. Конфіденційність інформації, яка передається телекомунікаційною мережею, забезпечує власник інформації, а інші властивості інформації, яка передається мережею – цілісність, доступність та спостережність – захищає оператор мережі чи провайдер телекомунікаційних послуг. Що стосується технологічної інформації, інформації керування, сигналізації та технологічних інформаційних ресурсів, то в інтересах оператора чи провайдера в них мають захищатись усі властивості інформаційних ресурсів: конфіденційність, цілісність, доступність технологічної інформації та спостережність процесів надавання послуг.

З впровадженням електронного документообігу, електронного цифрового підпису, електронного уряду, електронної торгівлі тощо, телекомунікаційна мережа, яка використовується для побудови цих систем, повинна забезпечувати новий рівень інформаційної безпеки і, зокрема забезпечувати приватність, взаємну автентифікацію і неспростовність. Останнє означає забезпечення неможливості відмови від факту передавання або приймання повідомлень (даних) у процесі взаємодії між мережею і користувачами та між взаємодіючими елементами мережі. Забезпечення інформаційної безпеки ТМЗК має включати в себе поняття, які за ступенем важливості розташовуються в такому порядку: цілісність (integrity) інформації; конфіденційність (confidentiality); захищеність від несанкціонованого доступу (authentication) до інформації, інформаційних ресурсів та обладнання мережі; неспростовність факту передавання або приймання інформації (non-repudiation); забезпечення надійності (availability) функціонування ТМЗК та її живучості. Такий підхід дає гарантію, що, навіть при випадковому або зловмисному спотворенні інформації, несанкціонованому проникненні в контур керування, втрати частини ресурсів та перенавантаження мережі внаслідок екстремального трафіка, комплекс організаційно-технічних заходів захисту забезпечить виконання найбільш важливих задач.

Основними цілями забезпечення інформаційної безпеки ТМЗК є підтримка та збереження в умовах впливу порушника на інформаційну сферу ТМЗК наступних основних характеристик інформаційної безпеки ТМЗК:

– цілісності інформаційної сфери ТМЗК;

– конфіденційності інформаційної сфери ТМЗК, в тому числі і конфіденційності інформації системи керування;

– доступності інформаційної сфери ТМЗК;

– спостережності (підзвітності) інформаційної сфери ТМЗК;

– неспростовності факту передавання або приймання інформації;

– непорушності порядку маршрутизації трафіка;

– таємниці зв’язку та приватності (пункт 3.35 „Ліцензійних умов…” [96]);

– недопущення несанкціонованого доступу до інформаційної сфери ТМЗК (пункт 3.34 „Ліцензійних умов…” [96]).

Забезпечення інформаційної безпеки ТМЗК повинно досягатись комплексним використанням організаційних, технічних, апаратно-програмних і криптографічних засобів захисту інформаційної сфери ТМЗК, а також здійсненням неперервного контролю за ефективністю реалізованих заходів із забезпечення інформаційної безпеки ТМЗК. Забезпечення інформаційної безпеки ТМЗК передбачає створення перешкод для можливого несанкціонованого втручання в процес функціонування. В цьому смислі проблема забезпечення інформаційної безпеки ТМЗК включає в себе як задачу захисту інформаційної сфери від несанкціонованого доступу, так і низку інших задач забезпечення процесів функціонування ТМЗК, зокрема, забезпечення надійності функціонування телекомунікаційних систем, їх живучості та забезпечення узгодженої між оператором та користувачем ТМЗК якості обслуговування в умовах впливу порушника на інформаційну сферу ТМЗК.

У зв'язку з цим з'явились нові задачі, зв'язані з необхідністю:

– захисту мереж, вузлів і центру керування мережею від несанкціонованого доступу користувачів до послуг зв'язку (телекомунікаційних послуг), які надаються мережею;

– посилення захисту систем управління ТМЗК, зокрема підсистеми керування інформаційною безпекою від можливості несанкціонованого доступу до процесів управління по різних каналах доступу, із забезпеченням конфіденційності та цілісності інформації управління (команд, донесень та інформації маршрутизації) які циркулюють у різних каналах зв'язку мережі, в умовах можливих навмисних дій (впливів) порушника;

– забезпечення заданої (гарантованої мережею) якості процесу передавання даних користувача (наприклад, вірність даних користувача, які передаються мережею) в умовах можливих навмисних впливів порушника на інформаційну сферу ТМЗК;

– забезпечення своєчасного виявлення спроби блокування порушником процесу передавання даних користувача з локалізацією місця впливу порушника та ліквідацією в заданий проміжок часу наслідків впливу порушника;

– захисту інформаційної сфери ТМЗК від можливості активізації порушником шкодоносних програм („закладок", „вірусів" тощо) за допомогою спеціальних команд, які посилаються порушником різними „легальними" та „нелегальними" каналами доступу (в тому числі каналами зв'язку при взаємоз'єднанні з іншими мережами телекомунікацій, зокрема, з мережею Інтернет);

– забезпечення можливості створення в ТМЗК надійного шляху (тракту) транспортування інформації (даних) для визначеної (окремої) групи користувачів, в тому числі в умовах навмисних впливів порушника на інформаційну сферу ТМЗК.

Забезпечення транспортних функцій ТМЗК в умовах можливих впливів порушника на її інформаційну сферу зв'язано зі специфічними проблемами, які відносяться, здебільшого до організації ефективного управління (на базі моніторингу стану мереж зв'язку), та взаємодією окремих апаратно-програмних

засобів зв'язку ТМЗК, розподілених на великих відстанях один від одного. Транспортування повідомлень каналами зв'язку за допомогою засобів зв'язку ТМЗК (маршрутизаторів, комутаторів, центрів комутації пакетів тощо) пов'язане з необхідністю забезпечення рівня основних характеристик якості обслуговування: надійного доведення отриманого від відправника повідомлення до одержувача, продуктивності, стабільності інформаційної безпеки.

Проблема забезпечення інформаційної безпеки у ТМЗК повинна бути вирішена при створенні в МЗК СЗІБ, яка спрямована на:

– формування єдиної політики в області забезпечення інформаційної безпеки при створенні, розвитку, модернізації й експлуатації ТМЗК;

– вироблення підходів до забезпечення інформаційної безпеки в умовах навмисних і ненавмисних впливів порушника;

– виявлення уразливості ТМЗК та здійснення комплексу адекватних і економічно обґрунтованих заходів по їх зменшенню, запобіганню впливів порушника та ліквідацію наслідків цих впливів на інформаційну сферу ТМЗК;

– координацію діяльності підприємств по забезпеченню інформаційної безпеки ТМЗК з контрольними органами державної влади, іншими операторами й організаціями;

– урахування вимог системи державного регулювання в області забезпечення інформаційної безпеки ТМЗК (ліцензування, сертифікації й атестації);

– обґрунтування економічної доцільності забезпечення інформаційної безпеки;

– знаходження балансу між рівнем безпеки мережі і рівнем безпеки користувачів;

– впровадження управління ризиками та страхування відповідальності оператора ТМЗК;

– використання механізмів страхування інформаційних ризиків;

– створення системи підготовки та перепідготовки кадрів в області забезпечення інформаційної безпеки ТМЗК;

– розроблення, удосконалення і стандартизація методів, способів, алгоритмів та засобів (механізмів) забезпечення інформаційної безпеки ТМЗК.

Система забезпечення інформаційної безпеки (СЗІБ) ТМЗК є складовою частиною Єдиної системи національної безпеки України і є сукупністю служб інформаційної безпеки, які реалізують організаційні і технічні заходи, визначені комплексом нормативно-правових документів. Архітектура СЗІБ ТМЗК розробляється у відповідності з принципами і положеннями, які містяться в нормативно-правових документах України, з урахуванням рекомендацій і стандартів Міжнародних організацій електрозв'язку.

Безпосереднє забезпечення інформаційної безпеки ТМЗК реалізується *службами інформаційної безпеки ТМЗК* і об'єктів зв'язку, які забезпечують виконання основних *функцій інформаційної безпеки*: автентифікації (користувача, об'єкта та джерела даних); контролю доступу; забезпечення цілісності повідомлень; забезпечення конфіденційності; забезпечення

доступності; неспростовності відправки/доставки та участі в обміні; локалізації місця впливу порушника; моніторингу й аудиту; повідомлення про порушення і відновлення порушеного процесу функціонування; адаптації до змінних умов функціонування ТМЗК.

Вказані функції виконуються за допомогою відповідних механізмів безпеки: керування доступом, обміну інформацією автентифікації, неспростовності, конфіденційності, безпечності з'єднання та керування маршрутизацією, цілісності (даних та інфраструктури) і захисту трафіка, доступності, приватності.

Безпосереднє керівництво заходами по забезпеченню інформаційної безпеки ТМЗК повинне здійснюватись службою безпеки ТМЗК.

Координацію роботи служб безпеки ТМЗК має здійснювати координаційний центр з питань безпеки ТМЗК та/або державні, або недержавні компетентні центри реагування на інциденти з інформаційною безпекою в ТМЗК.

Фінансові витрати на створення і технічну експлуатацію СЗІБ ТМЗК повинні бути економічно обґрунтованими і виходити з потенційно-можливого нанесення збитку діями порушника інформаційної безпеки користувачу, оператору ТМЗК і державі.

Забезпечення інформаційної безпеки ТМЗК при взаємоз'єднанні мереж зв'язку полягає у забезпеченні якості процесів функціонування ТМЗК, захисті її від несанкціонованого доступу і впливів порушника на систему управління ТМЗК.

Реалізація галузевої політики інформаційної безпеки повинна забезпечити взаємодію взаємо підключених мереж з заданою якістю обслуговування в умовах можливих дій порушників. При цьому рівень інформаційної безпеки взаємо підключених мереж зв'язку не повинен бути нижче базового рівня інформаційної безпеки ТМЗК.

Забезпечення інформаційної безпеки ТМЗК за приєднання і взаємоз'єднання мереж зв'язку України здійснюється в рамках розробки і реалізації розпорядчих і організаційно-технічних заходів по створенню СЗІБ ТМЗК. Забезпечення інформаційної безпеки ТМЗК при взаємоз'єднанні з глобальними інформаційно-телекомунікаційними мережами, зокрема з Інтернет, повинно базуватися на дотриманні сторонами міжнародних правових актів, які регламентують безпечний пропуск міжнародного трафіка, а також на застосуванні засобів захисту інформаційної сфери ТМЗК від несанкціонованого доступу з боку інших мереж, забезпеченні гарантованої якості функціонування ТМЗК в умовах можливих дій порушників.

Згідно з „Ліцензійних умов…" [96] правовою базою повинен бути договір про взаємо з'єднання телекомунікаційних мереж між операторами мереж, що взаємо підключаються. Предметом договору повинні бути: технічні, організаційні та економічні умови взаємоз'єднання мереж операторів; розрахункова такса за доступ до цих мереж; угода про порядок взаємодії операторів; угода про взаємний захист інформаційної сфери взаємоз'єднаних мереж; узгодження правил взаємодії та інтерфейси СЗІБ ТМЗК, що взаємо

підключаються; відповідальність за реалізацію заходів, які забезпечують задані вимоги інформаційної безпеки при взаємоз'єднанні мереж зв'язку.

Основні напрями робіт із забезпечення інформаційної безпеки. Робота по забезпеченню інформаційної безпеки ТМЗК поділяється на три групи.

1. Удосконалення нормативно-розпорядчої та нормативно-технічної бази забезпечення інформаційної безпеки, яка включає:

– принципи забезпечення інформаційної безпеки при взаємодії різних мереж електрозв'язку між собою та глобальними інфраструктурами зв'язку, зокрема, з Інтернет;

– порядок надавання послуг зв'язку спецкористувачам;

– порядок керування ТМЗК в „особливий період" та за надзвичайних ситуацій;

– перелік найбільш критичних з точки зору забезпечення інформаційної безпеки сегментів ТМЗК, які забезпечують передавання державних інформаційних ресурсів;

– вимоги інформаційної безпеки до об'єктів інформаційної безпеки ТМЗК;

– методи оцінки і контролю стану інформаційної безпеки ТМЗК;

– взаємодію, права й обов'язки суб'єктів СЗІБ на етапах її розробки створення;

– порядок підготовки до атестації та державної експертизи апаратних, програмно-апаратних і програмних засобів забезпечення інформаційної безпеки ТМЗК та атестації СЗІБ в цілому у відповідності з вимогами з інформаційної безпеки;

– організацію проведення робіт з виявлення закладок і не декларованих можливостей у технічних засобах ТМЗК;

– організацію роботи з впровадження державних і галузевих стандартів на технічні і програмні засоби і механізми забезпечення інформаційної безпеки ТМЗК.

2. Забезпечення технічного захисту процесів передавання даних в ТМЗК:

– виявлення та ліквідацію уразливості в інформаційній сфері ТМЗК;

– забезпечення конфіденційності інформації про інформаційну сферу ТМЗК;

– запобігання несанкціонованого доступу до ТМЗК та інформації, що передається нею;

– виявлення і запобігання впливів порушника на інформаційну сферу ТМЗК;

– аудит, контроль якості обслуговування й якісних характеристик процесу передаванню даних у ТМЗК в умовах навмисних дій порушника;

– своєчасне виявлення наслідків впливу порушника на інформаційну сферу ТМЗК;

– локалізація місця дій порушника;

– ліквідація наслідків впливу порушника на інформаційну сферу ТМЗК та відновлення порушеного процесу функціонування.

Реалізацію заходів технічного захисту повинні забезпечити:

– засоби криптографічного перетворення даних на канальному та мережному рівнях;

– засоби моніторингу і централізованого керування захистом процесів функціонування ТМЗК;

– система прихованого керування резервними каналами та засобами зв'язку, яка забезпечує оперативне відновлення порушеного процесу передавання даних в інтересах, передусім спецкористувачів.

3. Забезпечення організаційно-технічного захисту об'єктів і процесів передавання даних:

– розробку і реалізацію політик забезпечення інформаційної безпеки підприємств, філій, центів електрозв'язку, вузлів зв'язку тощо;

– організацію контролю стану інформаційної безпеки ТМЗК;

– технічне забезпечення інформаційної безпеки ТМЗК;

– розробку заходів по забезпеченню таємниці зв'язку;

– проведення заходів з ліквідації наслідків діяння порушників і відновленню порушеного процесу функціонування;

– забезпечення додержання установлених норм активно-правовими актами порядку маршрутизації трафіка;

– удосконалення фізичного та інженерно-технічного захисту об'єктів ТМЗК і недопущення несанкціонованого доступу до інформаційної сфери ТМЗК;

– підбір, навчання і робота з кадрами в інтересах забезпечення інформаційної безпеки ТМЗК.

Загальними задачами підприємства з забезпечення інформаційної безпеки ТМЗК є:

1. Розробка і проведення єдиної технічної політики в області забезпечення інформаційної безпеки ТМЗК, які включають:

– розробку вимог політики інформаційної безпеки ТМЗК та її складових частин;

– розробку критеріїв оцінки ефективності систем і засобів інформаційної безпеки ТМЗК;

– розробку критеріїв і методів оцінки стану інформаційної безпеки ТМЗК;

– установлення відповідальності посадових осіб і операторів ТМЗК за дотримання вимог інформаційної безпеки;

– навчання, підвищення кваліфікації й атестацію фахівців в області забезпечення інформаційної безпеки;

– створення системи моніторингу стану інформаційної безпеки ТМЗК;

– визначення політики по відношенню до закупок та використання імпортних і вітчизняних засобів захисту і програмної продукції.

2. Організація і проведення робіт із забезпечення інформаційної безпеки ТМЗК, зв'язаних з обробленням, зберіганням і передаванням інформації, віднесеної законодавством України до державної таємниці та інформації для службового користування.

3. Створення умов для дотримання установлених законодавством обмежень на доступ до конфіденційної інформації.

4. Організація взаємодії з органами державної влади та іншими операторами в області забезпечення інформаційної безпеки систем і мереж зв'язку.

5. Розробка механізмів протидії екстремістської діяльності на ТМЗК.

6. Проведення галузевої політики розвитку засобів зв'язку і засобів забезпечення інформаційної безпеки ТМЗК.

7. Контроль виконання вимог до інформаційної безпеки ТМЗК. Проведення моніторингу стану процесів функціонування ТМЗК за вимогами інформаційної безпеки.

8. Створення і розвиток системи керування ризиками і страхування відповідальності.

9. Забезпечення інформаційної безпеки інформаційних, ідентифікаційних і розрахункових систем з використанням ідентифікаційних карт.

10. Проведення робіт з підготовки атестації і державної експертизи ТМЗК, систем і засобів зв'язку у відповідності з вимогами до інформаційної безпеки ТМЗК.

11. Залучати до робіт із забезпечення інформаційної безпеки ТМЗК лише організації та підрозділи, які мають ліцензію на цей вид діяльності.

12. Забезпечення функціонування системи моніторингу і попередження інформаційних атак на критично важливі сегменти інформаційної інфраструктури ТМЗК. Реєстрування, аналіз та інформування відповідальних органів щодо інцидентів з інформаційною безпекою.

13. Забезпечення розробки розпорядчих та нормативних документів з інформаційної безпеки ТМЗК.

14. Створення служби інформаційної безпеки ТМЗК у складі системи технічної експлуатації і системи управління ТМЗК.

15. Забезпечення дотримування установленого нормативно-правовими актами порядку маршрутизації трафіка.

16. Удосконалення політики інформаційної безпеки оператора ТМЗК та її головних складових частин. Постійна модернізація системи забезпечення інформаційної безпеки ТМЗК у відповідності з розвитком технологій інформаційної безпеки.

17. Забезпечення вимог інформаційної безпеки ТМЗК при взаємодії з мережами зв'язку інших операторів ТМЗК.

Правові засади забезпечення інформаційної безпеки ТМЗК. Організаційно-економічні засади інформаційної безпеки ТМЗК є складовими Єдиної системи інформаційної безпеки телекомунікацій і успадковує основні її принципи. Вони розвивають положення Закону України „Про основи національної безпеки України", Закону України „Про телекомунікації", „Ліцензійних умов …" [58, 61, 96, 97], інших правових і нормативних актів України. У засадах враховані деякі стандарти міжнародних організацій електрозв'язку [218, 219], використання новітніх технологій та необхідність підвищення ефективності, стабільності функціонування та безпеки інформаційної сфери ТМЗК .

Організаційно-економічні засади служить основою для розробки комплексу організаційних і технічних заходів із забезпечення інформаційної безпеки ТМЗК, нормативних і методичних документів, які забезпечують їх реалізацію підприємствами усіх форм власності, причетних до розвитку телекомунікацій в Україні та їхнього використання. Організаційно-економічні засади не стосуються системи захисту інформації з обмеженим доступом, яка належить державі.

Умови взаємодії з органами влади при забезпеченні інформаційної безпеки. Відповідальність за забезпечення інформаційної безпеки ТМЗК несе ліцензіат-підприємство зв'язку. При здійсненні цієї діяльності підприємство взаємодіє із зацікавленими органами державної влади.

Ліцензіат зобов'язаний установлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їхнього проведення відповідно до діючого законодавства. Згідно з Законом України „Про телекомунікації" підприємство зобов'язано забезпечити захист зазначених засобів від несанкціонованого доступу. Контроль за застосуванням криптографічних заходів захисту при забезпеченні інформаційної безпеки ТМЗК здійснюється ДССЗЗІ України у відповідності з діючим законодавством.

На об'єктах телекомунікацій, а також в окремих структурних підрозділах операторів, провайдерів телекомунікацій, де передається, обробляється або зберігається інформація з обмеженим доступом, яка є власністю держави, установлюється спеціальний режим доступу відповідно до законодавства. Контроль за застосуванням засобів захисту від несанкціонованого доступу до інформації, віднесеної до інформації з обмеженим доступом, і захисту цієї інформації від побічних електромагнітних випромінювань та наведень (ПЕМВН) на ТМЗК, здійснюється ДССЗЗІ у відповідності з діючим законодавством. Підприємства мають складати план взаємодії з правоохоронними органами та органами влади у процесі ліквідації наслідків інцидентів з інформаційною безпекою.

Загрози інформаційній безпеці ТМЗК. Забезпечення інформаційної безпеки функціонування ТМЗК повинно базуватись на аналізі вразливостей, які можуть бути використані порушником для подолання системи захисту ТМЗК та призвести до нанесення збитків користувачу, підприємству або державі.

Загроза інформаційній безпеці ТМЗК – це можливий вплив порушника інформаційної безпеки на інформаційну сферу ТМЗК, не запобігання, не виявлення і не ліквідація наслідків якого засобами ТМЗК може привести до погіршення заданого рівня якості послуг або до погіршення заданих якісних характеристик функціонування ТМЗК і, як наслідок, до нанесення збитків державі, користувачу або оператору ТМЗК чи провайдеру послуг. Загрози реалізуються через можливі уразливості інформаційної сфери ТМЗК. Успішна атака порушника, спрямована на реалізацію загроз інформаційній безпеці

ТМЗК, опирається на одержані порушником знання про особливості побудови та уразливості ТМЗК.

Причинами появи вразливостей в ТМЗК можуть бути:

– порушення технології процесу передавання інформації користувача;

– порушення технології системи керування ТМЗК;

– впровадження в об'єкти ТМЗК компонентів, які реалізують не декларовані функції;

– впровадження в об'єкти ТМЗК програм, які порушують їх нормальне функціонування;

– незабезпеченість реалізованими механізмами захисту ТМЗК або пред'явлення до механізмів захисту ТМЗК непродуманого набору вимог, які роблять ТМЗК незахищеною;

– внесення порушником навмисної уразливості при розробці алгоритмів і програм ТМЗК, при розробці захищених процедур, протоколів і інтерфейсів взаємодії користувачів, операторів і адміністраторів з апаратно-програмним забезпеченням ТМЗК при реалізації проектних рішень по створенню СЗІБ ТМЗК, які роблять не ефективним реалізовані в СЗІБ ТМЗК механізми захисту;

– неадекватного реагування підсистеми управління СЗІБ ТМЗК на інформаційні впливи порушника в процесі експлуатації СЗІБ;

– використання не сертифікованих у відповідності з вимогами безпеки вітчизняних і зарубіжних інформаційних технологій, засобів інформатизації і зв'язку, а також не атестованих засобів захисту інформації і контролю їх ефективності тощо.

Проведення аналізу уразливості ТМЗК та можливих дій порушника дозволяє визначити перелік найбільш небезпечних наслідків дій порушників, загроз інформаційній безпеці ТМЗК, захист від реалізації яких і повинна бути забезпечена.

Порушники інформаційної безпеки ТМЗК. Як порушники інформаційної безпеки можуть виступати фізичні особи і/або структури, дії яких можуть привести до погіршення якості процесів функціонування ТМЗК. Впливи на інформаційну сферу ТМЗК можуть здійснюватись на кожному з етапів життєвого циклу ТМЗК – проектування, будівництва та експлуатації.

На етапі проектування та будівництва порушниками можуть бути наукові й інженерно-технічні працівники, які беруть участь у процесі проектування, розробки, установки і налагодження програмно-апаратного забезпечення мереж загального користування (МЗК).

На етапі експлуатації порушники можуть бути „зовнішніми" по відношенню до МЗК або „внутрішніми", які належать структурі МЗК.

Порушник на етапі експлуатації може здійснювати вплив на такі об'єкти інформаційної безпеки МЗК: центр управління мережею зв'язку, вузли МЗК (комутатори, маршрутизатори, шлюзи, сервери, цифрові автоматизовані телефонні станції тощо), канали зв'язку МЗК та повідомлення (пакети, кадри, комірки, контейнери тощо), які містять інформацію користувачів або інформацію керування.

Дії порушників можуть носити як навмисний, так і ненавмисний характер. Впливи порушників на об’єкт інформаційної безпеки можуть здійснюватись: через зовнішні лінії зв’язку; через внутрішні лінії зв’язку; з робочих місць системи керування; через не декларовані канали доступу. При цьому можуть використовуватись як штатні засоби мереж зв’язку, так і спеціальні засоби.

Впливи порушника на інформаційну сферу ТМЗК подаються у вигляді дій, спрямованих на виявлення вразливостей ТМЗК, на активізацію або використання наявної уразливості ТМЗК та дій, пов’язаних з внесенням уразливості в ТМЗК.

Внесення уразливості в інформаційну сферу ТМЗК можливе на етапах проектування при виборі алгоритмів і технології зберігання, оброблення і передавання інформації, які утруднюють або виключають реалізацію вимог інформаційної безпеки, а також вибору засобів захисту, які не забезпечують вимоги інформаційної безпеки ТМЗК.

На етапі експлуатації ТМЗК порушник може внести уразливості, які зв’язані з:

– помилками налаштування та використання програмно-апаратного забезпечення;

– помилками розробки і реалізації політики безпеки;

– помилками в реалізації організаційних методів захисту;

– навмисним впровадженням у компоненти апаратно-програмного забезпечення „люків”, „закладок”, „вірусів” тощо.

Виявлення уразливості здійснюється порушником шляхом збирання відомостей, які дозволяють йому здійснювати дії, спрямовані на погіршення характеристик інформаційної безпеки. Безпосередня активізація чи використання виявленої уразливості здійснюється порушником на етапі експлуатації шляхом:

1. Використання спеціального обладнання на зовнішніх і внутрішніх каналах зв’язку ТМЗК і здійснення за його допомогою: порушення цілісності повідомлень, які містять інформацію керування або інформацію користувачів; порушення конфіденційності інформації керування і параметрів передавання інформації користувачів; формування команд активізації і використання функцій „закладок” і „вірусів”, впроваджених в інформаційну сферу; формування інформаційного впливу з метою отримання аутентифікаційних параметрів, які забезпечують доступ до інформаційної сфери об’єктів та мереж зв’язку; несанкціонованої модифікації програмного забезпечення об’єктів та мереж зв’язку і порушення їхньої працездатності.

2. Установлення спеціального обладнання в канали мереж зв’язку для використання інформаційних „люків” або не декларованих можливостей.

3. Використання прикінцевого обладнання користувачів ТМЗК для отримання несанкціонованого доступу до інформаційної сфери об’єктів та мереж зв’язку.

4. Використання радіоканалів для активізації „закладок” і „вірусів”.

5. Використання робочих місць обслуговуючого персоналу.

Політика інформаційної безпеки в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Заходи забезпечення інформаційної безпеки ТМЗК в умовах надзвичайних ситуацій, надзвичайного та воєнного стану регулюються Законом України „Про телекомунікації" [61].

В умовах надзвичайних ситуацій, надзвичайного та воєнного стану підприємства зв'язку зобов'язані забезпечувати якісний зв'язок та оповіщення населення в порядку, визначеному Кабінетом Міністрів України.

Підприємство зв'язку повинне забезпечити готовність до виконання своїх функцій в умовах надзвичайних ситуацій, надзвичайного та воєнного стану. Під час надзвичайного стану всі засоби та телекомунікаційні мережі зв'язку, незалежно від форми власності, використовуються для забезпечення проведення мобілізації та задоволення потреб національної безпеки, оборони, охорони правопорядку. Оператори телекомунікацій взаємодіють при цьому з Національним центром оперативно-технічного управління мережами зв'язку в питаннях, віднесених до його компетенції.

В умовах надзвичайних ситуацій, надзвичайного стану оператори телекомунікацій з метою оповіщення та забезпечення телекомунікаційними послугами учасників ліквідації наслідків надзвичайних ситуацій, відбудовних робіт та здійснення відповідних заходів Радою міністрів Автономної Республіки Крим, обласними, Київською і Севастопольською міськими державними адміністраціями та органами місцевого самоврядування можуть установлювати тимчасові обмеження в наданні телекомунікаційних послуг споживачам до ліквідації наслідків надзвичайних ситуацій та скасування режиму надзвичайного стану.

Забезпечення інформаційної безпеки систем управління ТМЗК в умовах надзвичайних ситуацій, надзвичайного та воєнного стану необхідно передбачати завчасне створення запасних пунктів керування і резервування обхідних каналів зв'язку.

Політика захисту інтересів користувачів ТМЗК. Захист інтересів користувачів ТМЗК регулюється Законом України „Про телекомунікації", „Ліцензійними умовами …" [61, 96, 97] та іншими нормативно-правовими актами, де установлюються права, обов'язки користувачів та відповідальність за відповідні порушення.

Необхідно задовольняти вимоги споживачів щодо збереження конфіденційності інформації, яка стосується цього споживача, а також забезпечувати та нести відповідальність за схоронність відомостей щодо споживача, отриманих при укладенні договору, наданих телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, їх оплати, маршрутів передавання тощо.

Оператор ТМЗК приймає заходи, які забезпечують:

– право на доступ користувачів ТМЗК до відкритої інформації і обмеження доступу до інформації, яка підлягає захисту;

– виключення (недопущення) несанкціонованого доступу користувачів ТМЗК до ресурсів мережі і послугам зв'язку;

– захист персональних даних користувача ТМЗК, які стали йому відомі у процесі здійснення операторської діяльності, й інформації щодо наданих послуг зв’язку;

– захист білінгових систем;

– надавання додаткових послуг захисту інформації користувача ТМЗК і забезпечення інформаційної безпеки процесу передавання за договором з конкретним користувачем ТМЗК.

Користувачі ТМЗК повинні бути проінформовані оператором ТМЗК про послуги зв’язку з забезпечення інформаційної безпеки ТМЗК у частині, яка їх стосується.

З проведеного дослідження визначені та обґрунтовані основні принципи та засади інформаційної безпеки ТМЗК, які можуть бути застосовані в сфері телекомунікацій. Визначені принципи є основою чи фундаментом формування концепції системи інформаційної безпеки ТМЗК.

Ґрунтуючись на основних принципах та засадах інформаційної безпеки ТМЗК перейдемо до аналізу організаційних та економічних аспектів інформаційної безпеки, а саме розглянемо роль та місце персоналу в забезпеченні інформаційної безпеки та оцінку витрат на створення і впровадження системи забезпечення інформаційної безпеки.

Контрольні запитання та завдання

1. Що визначає та на яких принципах побудована архітектура інформаційної безпеки?
2. Які загрози інформаційним ресурсам телекомунікаційних мереж описує Рекомендація ITU X.800?
3. Дайте визначення компонентів системи інформаційної безпеки телекомунікаційних мереж: механізмів захисту, рівнів захисту, площини захисту.
4. Що є механізмами забезпечення інформаційної безпеки? Поясніть суть кожного з механізмів інформаційної безпеки.
5. Як впливають на зовнішню та внутрішню безпеку телекомунікаційних мереж техногенні та антропогенні фактори?
6. Поясніть взаємозалежність і взаємозв’язок задач безпеки й якості технології.
7. Поясніть розподіл послуг безпеки за рівнями моделі архітектури Взаємодії Відкритих Систем.
8. Розкрийте розподіл окремих послуг безпеки між елементами архітектури телекомунікаційної мережі.
9. Поясніть особливості в розподілу систем захисту у мережах наступного покоління Next Generation Network – NGN.
10. Наведіть загальні вимоги до інформаційної безпеки телекомунікаційних мереж загального користування (ТМЗК).

11. Чим досягається забезпечення інформаційної безпеки ТМЗК?

12. Для чого створюють служби інформаційної безпеки ТМЗК? Які їх функції?

13. На які групи поділяється робота із забезпечення інформаційної безпеки ТМЗК?

14. Які є правові засади забезпечення інформаційної безпеки ТМЗК?

15. Прокоментуйте політику захисту інтересів користувачів ТМЗК.

Завдання до самостійної роботи

1. Проаналізуйте роль кожного механізму безпеки на кожному рівні забезпечення інформаційної безпеки та кожній площині інформаційної безпеки, коли:

- утворюється дев’ять модулів безпеки,
- кожен модуль безпеки комбінує вісім механізмів безпеки,
- які застосовуються до окремого рівня забезпечення безпеки в окремій площині інформаційної безпеки.

2. Проаналізуйте значення інформаційної безпеки телекомунікаційних мереж як критичного елемента національної безпеки країни.

РОЗДІЛ 6

ЗАБЕЗПЕЧЕННЯ УСТАЛЕНОГО ВІДТВОРЕННЯ СОЦІАЛЬНОГО КАПІТАЛУ

6.1 Соціальний капітал, соціологічна та соціальна інформація

Даний розділ стосується сфери менеджменту персоналу, інформаційної безпеки і лежить в руслі задач виявлення закономірностей переходу суспільства до інформаційної та постінформаційної ери.

Особливістю сучасного етапу соціально-економічного розвитку стало широке застосування інформаційних технологій, яке викликало серйозні зміни структури суспільного виробництва, та визрівання нових технологій, серед них найбільш перспективних нано-, психо- та біотехнологій. В умовах становлення постіндустріального та постінформаційного суспільства, коли проходить зміна технологічного укладу, виникають проблеми впливу соціально-економічного розвитку на всі сторони життя суспільства і, зокрема, проблема відтворювання соціального капіталу та захисту соціальної інформації.

Одною з необхідних умов розвитку та технологічного злету є гуманітарні технології забезпечення й підтримки великих інноваційних проектів [6] та пошук адекватних соціальних технологій.

Сьогодні проходить революція у соціально-комутативній сфері. Кінець XX століття привів у багатьох країнах до втрати «зв'язків з ближніми», дефіциту уваги й порозуміння. З'явилось прагнення встановити *зв'язки з дальніми* через Інтернет – свого роду, сурогат особистого спілкування. Цей соціальний й технологічний ресурс кількісно стрімко зростає.

Нова ситуація полягає також у тому, що за сучасних технологій, складних технологічних комплексів, дії окремих людей, навіть не наділених державною владою, можуть мати глобальні наслідки типу Чорнобильської чи Саяно-Шушенської аварії. Постає серйозна проблема приведення у відповідність суспільної та індивідуальної свідомості новим технологічним можливостям та пов'язаним з ними рівнем відповідальності.

З іншого боку існує важлива задача – зайняти людей, для більшості з яких за сучасних технологіях немає місця у сфері виробництва та управління. Таких людей стає все більше і «зайвого часу» теж. Близько 3% зайнятих у сільському господарстві будуть здатні годувати всю країну [6], ще 10% зайнятих у високоавтоматизованому та роботизованому виробництві забезпечать потреби у промислових товарах (включаючи добування необхідних мінеральних ресурсів та енергії).

Кількість людей, здатних до формування нових проривних ідей, створення й експлуатації знань в науці, управлінні тощо, у будь-якій національній популяції вельми обмежено, і не перевищує 3-5% [132]. Інші мають перейти в сферу надавання послуг чи в сферу обслуговування інформаційних технологій і процесів обробки інформації. Девізом нового

інформаційного віку є інтелектуальна конкурентноздатність. В інформаційному суспільстві більше половини робочого часу буде використовуватись на зберігання, обробку й передачу інформації. Буде продаватись інформація, менеджмент, культура, нові технології, програмне забезпечення, послуги освіти, медицини, фінансів тощо.

Виявилась низка проблем, які можна характеризувати як такі, що мають соціально - технологічний характер. Соціальна поведінка складається з примушування та співробітництва. Співробітництво розглядається в рамках явищ, які об'єднують поняттям соціального капіталу та безпеки соціальної інформації.

Соціальним капіталом називається сума спільних суспільних вартостей, таких, що дійсно стали спільними – це набір неофіційних вартостей чи норм, які є спільними для членів групи і дозволяють їм взаємодіяти. Соціальний капітал відіграє суттєву роль у забезпеченні ефективності функціонування суспільства. Соціальний капітал формується добровільно, основується на неписаних законах, формується шляхом самоорганізації соціальних груп, для його підтримання не потрібно застосування сили чи примушування з боку держави, його проявами є соціальне партнерство. Соціальний капітал утворює сферу образу життя, відображає спосіб взаємодії соціальних груп і її членів в середині групи.

Поняття соціального капіталу було введено як економічна й, одночасно, соціологічна категорія до раніш існуючих фізичного та людського капіталу. Властивості соціального капіталу та його роль вивчаються у економічних, соціальних, політичних та культурних процесах[197, 198, 70].

Вперше поняття «соціального капіталу» було вжито Лайдою Джадсон Ганіфан у 1916 році для опису шкільних центрів сільських громад. Останнім часом (у 1988 році), поняття соціального капіталу відродив соціолог Джеймс Колмен. Стало очевидним, що соціальний капітал став реальною складовою як економічної науки, так і соціології.

Будемо розрізняти чотири види капіталу, які функціонують і взаємодіють в інформаційному та матеріальному полі (рис. 6.1). Як відомо, фізичний капітал складають земля, будівлі, машини. Людський капітал виражається у вміннях, знаннях у головах людей.

Соціальний капітал, подібно до фізичного і людського капіталу створює багатства, а тому має економічну цінність для національної економіки.

Інформація є необхідною складовою у процесах створення та функціонування фізичного, людського й соціального капіталу. У фізичному капіталі інформація присутня у вигляді документів, документації, інструкцій, маркерів, а також в управлінні фізичним капіталом. У людському капіталі інформація є знаннями, навчанням, використовується у розумовій інтелектуальній діяльності та управлінні. Крім того інформація утворює нову форму капіталу – інформаційний капітал – у якому інформація виступає як товар, сировина й засіб виробництва. В сучасних умовах виникнення нових і загострення старих проблем, у період переходу до інформаційного суспільства,

стає все більш вагомою роль інформаційних процесів і постає задача введення ще одної економічної категорії – інформаційного капіталу.

Рисунок 6.1 – Види та взаємодія

У формуванні соціального капіталу у людських спільнотах одну з провідних ролей відіграє соціальна інформація.

Під інформацією у Законі України «Про інформацію» розуміються документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому середовищі. Обмін інформацією може здійснюватись технічними та програмними засобами телекомунікаційної системи шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Основними видами інформації, у визначенні Закону України "Про інформацію", є статистична, правова, соціологічна інформація, інформація довідково-енциклопедичного характеру, яка використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернет, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами, а також масова інформація та інформація про особу.

Соціологічна інформація – це документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних

подій та явищ, процесів, фактів. Джерелами цієї інформації є відомості, в яких відображено результати соціологічних опитувань, спостережень та інших соціологічних досліджень.

На відміну від соціологічної інформації, *соціальна інформація* безпосередньо функціонує у людському суспільстві, відіграючи в ньому управляючу роль в процесах життєдіяльності та взаємодії з оточуючим середовищем. Соціальна інформація поділяється на атрибутивну, комунікативну та функціональну складові.

Атрибутивна складова соціальної інформації служить для задавання понять, визначень, правил, думок, цінностей, символів, міфів та інших атрибутів дійсності та життєдіяльності.

Комунікативна складова соціальної інформації є засобом встановлення, організації та здійснення взаємодії суб'єктів інформаційних відносин в процесі їх діяльності в умовах суспільних відносин та оточуючого середовища.

Функціональна складова соціальної інформації необхідна для повсякденної діяльності, праці, аналізу, прийняття рішень та задоволення нагальних фізичних, емоційних, інтелектуальних та психологічних потреб.

Класифікацію соціальної інформації надано в [132]. Соціальну інформацію поділяють на три типи: про сучасність, про минуле, про майбутнє.

Соціальна інформація може бути прогностичною (з функціями: орієнтовної, нормативної, попереджувальної) та плановою.

За видами соціальна інформація може бути внутрішня та зовнішня, горизонтальна та вертикальна (пряма – директивно-нормативна, зворотна – контрольно-звітна, зокрема соціологічна).

Функціонування соціальної інформації характеризують наступними ознаками:

- за рівнями циркуляції: національний, регіональний, континентальний, глобальний;
- за часом циркуляції: короткострокове, середньострокове, довгострокове;
- за коментарями до інформації: позитивними, негативними, нейтральними;
- за способом доведення інформації: за допомогою ЗМІ, через спецслужби, через неформальні зв'язки, за допомогою дипломатичних джерел, через бізнес-структури;
- за метою доведення інформації: переконання, вплив, реакція у відповідь, компрометація, створення нових цінностей та правил для спільнот чи еліти.

Економіка існує й повинна досліджуватись у комплексі взаємозв'язків, впливів та наслідків у соціальних, політичних, культурних процесах тощо. У гармонійно організованому суспільстві та державі функціонування економіки має бути тісно узгоджено з комплексом соціальних, політичних, культурних процесів. У сучасному суспільстві є ряд проблем, які мають тенденцію до загострення в умовах бурхливого розвитку інформаційних технологій та впливу їх практично на всі сфери життя індивіда, суспільства та держави. Динаміка негативних змін у суспільстві залежить від зсувів технологічних формацій, які приводять до змін у інших сферах відносин соціальних, культурних тощо [197].

У найбільш концентрованому вигляді негативні зміни простежуються у соціальному капіталі.

6.2. Залежність соціального капіталу від циклічності розвитку та зміни технологічних укладів

Сучасне економічне зростання може бути представлене як процес періодичного послідовного заміщення технологічних укладів. Будемо розрізняти поняття технологічного укладу і, власне окремі технології.

Технологічний уклад – це сукупність технологій: базових та вторинних, які разом забезпечують виробництво, підтримку існування й життєдіяльності суспільства та людини.

Базові технології складають ядро технологічного укладу. До них відносяться: основна рушійна фізична сила господарства; будівництво й виробництво, які займають провідний характер; технології матеріалів та сировини. Склад базових технологій може змінюватись в залежності від напряму науково-технічного прогресу й основних цілей та задач суспільства, які вирішуються в той, чи інший історичний період. Вторинні технології розвиваються на основі базових.

Розвиток кожної технології має свій життєвий цикл. Характерна властивість сучасних технологій полягає у швидкому скороченні та розмиванню їх життєвих циклів. Якщо раніше оновлення основних фондів займало десятиліття, то сьогодні обладнання може змінюватись на протязі декількох років. А багато видів інтелектуальної діяльності взагалі не потребують обладнання окрім персонального комп'ютера. Відбувається різке скорочення строків реалізації наукових відкриттів: середній період освоєння нововведень з 1885 по 1919 р. склали 37 років, з 1920 по 1944 р. – 24 роки, з 1945 по 1964 р. – 14 років, а в кінці 20 століття для найбільш перспективних відкриттів (електроніка, атомна енергетика, лазери) – 3-4 роки [26]. Фази життєвого циклу НДР, ДКР, проектування й освоєння масового виробництва суміщаються. Виробництво стає сферою реалізації наукових досягнень.

Прискорення науково-технічного прогресу позначається й на скороченні життєвого циклу технологічних укладів внаслідок нових технологій та інновацій, але технологічні уклади є більш інерційними завдяки фундаментальності базових технологій. Прискорення пов'язують з довгими хвилями Кондратьєва, яким початково приписували 55-річний період. На рис. 6.2, який запозичено з [3], на базі нових досліджень показано, що протяжність інноваційних хвиль, тобто період проходження життєвого циклу продуктів скорочується завдяки менеджменту й науковому насиченню процесів технологічного розвитку.

Для кожної з п'яти хвиль Кондратьєва на рис. 6.2 перелічені базові технології, впровадження яких забезпечувало прискорений розвиток економіки.

Рушійними силами були послідовно: енергія води, енергія пари, електроенергія та двигуни внутрішнього згорання. Під час четвертої хвилі механічна енергія не зникає, а переходить у розряд другорядних технологій,

хоча за кількісними характеристиками продовжує зростати. На її місце як рушійна сила виходить інформація, та засоби її транспортування – телекомунікаційні мережі.

Рисунок 6.2 – Прискорення довгих хвиль Кондратьєва

На етапі впровадження інформаційних технологій малі інформаційні впливи управляють по суті потужними інформаційними потоками, де доля енергетичних потоків стає все меншою, а інформація набуває «матеріального характеру». В майбутньому, за панування нано- та біотехнологій споживання енергії може стати зовсім мізерним.

Провідний характер послідовно займали *виробництво* тканин, *будівництво* залізничних доріг та виробництво парових машин, далі виробництво приладів та станків, електроніки та машино- й літакобудування, виробництво програмних продуктів та будівництво телекомунікаційних мереж.

В період інформаційних технологій машини, обладнання набувають властивостей універсальності своєї структури і мають, як правило, у своєму складі мікропроцесори чи обчислювальні системи. Основна задача виробництва полягає у програмуванні потрібних функцій, процесів, програмних і матеріальних продуктів та послуг.

В постінформаційний період програмування набуде нової якості – в нано- та біотехнологіях будуть програмуватись на молекулярному рівні властивості матеріалів, продуктів і матеріальних комплексів. Суспільство ставить ціллю загального підвищення якості життя і з’являється новий базовий компонент технологічного укладу – нові медичні засоби.

Матеріали та сировина, що використовувались, були: залізо, сталь, складні хімічні сполуки, електронні (універсальні) компоненти, а далі нано- й біокомпоненти молекулярного рівня.

В нинішній період економічного розвитку базовими компонентами є мікроелектроніка, програмне забезпечення. Його ядро формують виробництва електронних компонентів та пристроїв, електронно-обчислювальна техніка, радіо- та телекомунікаційне обладнання, лазерне обладнання, послуги обслуговування обчислювальної техніки.

П’ята хвиля інновацій зараз проходить свій максимум і її протяжність може скоротитись до 25 - 30 років. Нинішній п’ятий інформаційний технологічний уклад буде домінувати до 2020 - 2030 року і на його зміну прийде наступний нано- біотехнологічний уклад.

Життєвий цикл технологічного укладу охоплює період приблизно у сто років з двома явно вираженими стрибками у його розвитку. Його вид наведено на рис. 6.3.а [26]. На осі ординат відкладається показник обсягу виробництва, що забезпечується даним технологічним укладом, по осі абсцис – час у роках.

Життєві цикли технологічних укладів узгоджуються з циклами інноваційної активності Кондратьєва завдяки тому, що два сусідніх технологічних уклади частково перекриваються. Новий технологічний уклад по С. Ю. Глаз’єву зароджується, коли в економічній структурі ще домінує попередній (на рис. 6.3.а зародженню відповідає перший стрибок кривої). У цій фазі його розвиток стримується несприятливим технологічним та соціально-економічним середовищем. Необхідні професійні навики освоюються у цій фазі обмеженим колом вчених, винахідників, інженерів, ентузіастів нової справи.

Лише коли існуючий технологічний уклад досягає своїх меж росту та починається падіння прибутковості його виробництва, тоді започатковується другий стрибок росту нових технологій внаслідок перерозподілу ресурсів у технологічні ланцюги нового технологічного укладу. При цьому відбувається масове освоєння нових професій, перекваліфікація, перетікання робочої сили в нові галузі і витіснення старих професій з виробництва.

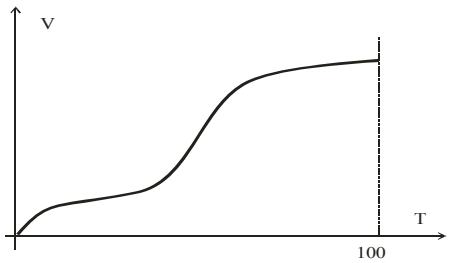


Рисунок 6.3.а – Життєвий цикл технологічного укладу

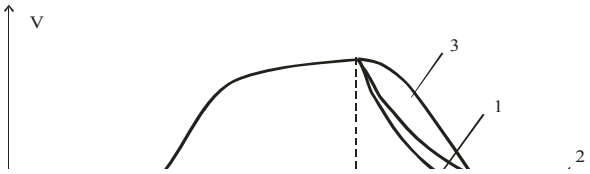


Рисунок 6.3.б – Характер перехідних процесів спадання технологічного укладу

Такий процес називають технологічною революцією, бо він супроводжується масовим обезцінюванням матеріального, фінансового й соціального капіталу, поглибленням зовнішньоторгових протиріч, загостренням соціальної й політичної напруженості.

Внаслідок того, що сусідні технологічні уклади частково перекриваються, набуває важливого значення їх взаємозалежність та характер перехідних процесів. Розглянемо докладніше перехідні процеси на заключному етапі спаду поточного технологічного укладу. Моделі спаду технологічного укладу, показані на рис. 6.3.б, характеризуються різною швидкістю спадання. Спад може приймати експоненційний (1), показниковий (2) чи нормальний (3)

характер і описуватись відповідними функціями розподілу ймовірностей випадкових величин показника обсягу виробництва.

Нормальному закону – розподілу Гауса – підпорядковується сума багатьох незалежних випадкових величин, кожна з яких відіграє незначну роль в утворенні всієї суми. В нашому випадку модель описується густиною ймовірностей

$$p(t) = \begin{cases} 1 \quad при \quad t \le 0; \\ \dfrac{1}{\sigma\sqrt{2\pi}} e^{-(t-m)^2 / 2\sigma^2} \quad при \quad t > 0, \end{cases} \tag{6.1}$$

де m – математичне очікування,

σ^2 – дисперсія випадкової величини t.

За нормального закону спочатку, при $t < \sigma$, спад виробництва незначний, потім, при $\sigma < t < 2\sigma$, крива швидко спадає, а при $t > 3\sigma$ значення показника обсягу виробництва вже настільки малі, що ними можна знехтувати. Це відоме інженерне «правило трьох сигм».

На практиці «об'єкти» та «суб'єкти» соціально-економічних відносин не бувають повністю незалежними. Сировина, матеріали й засоби виробництва об'єднуються у виробничі комплекси, а «суб'єкти» об'єднуються у людські колективи певного типу: сім'ї, общини, робітничі кооперативи (наприклад підрядні бригади), нації, корпоративні союзи, державні та світові спільноти тощо. Тому для моделі спадання може використовуватись функція розподілу з меншою швидкістю спадання – показникові функції $p(t) = a^{-t}$ (при основі $a > 0$, $a \neq 1$) та їх частковий випадок: експоненціальну функцію $p(t) = e^{-t/\lambda}$, де λ - математичне очікування функції розподілу.

Експоненціальна функція добре описує процеси зміни таких величин, у яких швидкість зміни є пропорційною цій величині. Часова кореляція мала, що означає швидке забування системою своєї історії та слабку взаємозалежність її частин.

Велике число закономірностей у природі описують показникові функції виду $p(t) = at^n$, де a та n будь-які дійсні числа. Для опису соціально-економічних процесів можуть застосовуватись показникові функції розподілу ймовірностей виду

$$p(t) = t^{-(1+\alpha)}, \tag{6.2}$$

де $\alpha \sim 1$.

Головною відмінністю показникової функції від нормальної та експоненціальної є швидкість спадання функції $p(t)$ з ростом аргументу та наявністю, так званого «важкого хвоста». Хвіст функції розподілу (6.2) спадає значно повільніше, математичне очікування випадкової величини стає нескінченним, а кореляційні залежності являються дальніми. Система, яка описується такою функцією, довго «пам'ятає» свій попередній стан.

Умовами другого сплеску життєвого циклу нової технології є відповідні зміни у соціальних, інституціональних й освітніх системах, які, знімаючи соціальну напруженість, встановлюють нові правила, принципи, норми, установки, права та сприяють масовому впровадженню технологій нового

укладу, відповідному йому типу споживання та способу життя. Внаслідок цього починається фаза швидкого розширення нового технологічного укладу і він займає домінуюче становище в структурі економіки.

У фазі зростання нового укладу більшість технологічних ланцюгів попереднього укладу перебудовуються у відповідностях з новими потребами. І в той же час, зароджується наступний, найновіший технологічний уклад, але після першого сплеску він не зростає, поки домінуючий технологічний уклад не досягне меж свого росту, після чого починається чергова технологічна революція.

Тепер нам буде більш ясним характер взаємодії між старими та новими технологічними укладами. На рис. 6.4 наглядно представлено процес послідовних змін технологічних укладів. Передумови першого сплеску розвитку нових технологій створюються в ході розвитку науки, науково-дослідно-конструкторських робіт та дослідних виробництв. До часу, коли традиційні технологічні можливості досягають межі в підвищенні ефективності виробництва вказані передумови реалізуються перетворюючись із потенційного способу вкладення капіталу у реальні.

Для початку другого сплеску – фази швидкого розширення технологічного укладу, крім науково-дослідно-конструкторських напрацювань, необхідні воля держави, суспільства, освітніх інституцій, а також відповідні транспортна інфраструктура й енергоносії. Кожен новий технологічний уклад у своєму розвитку спочатку використовує ту транспортну інфраструктуру й енергоносії, що склалися, чим стимулює їх подальше розширення.

За мірою розвитку чергового технологічного укладу створюється новий вид інфраструктури, який долає обмеження попереднього, а також здійснюється перехід на нові види енергоносії, які закладають основу для становлення нового технологічного укладу.

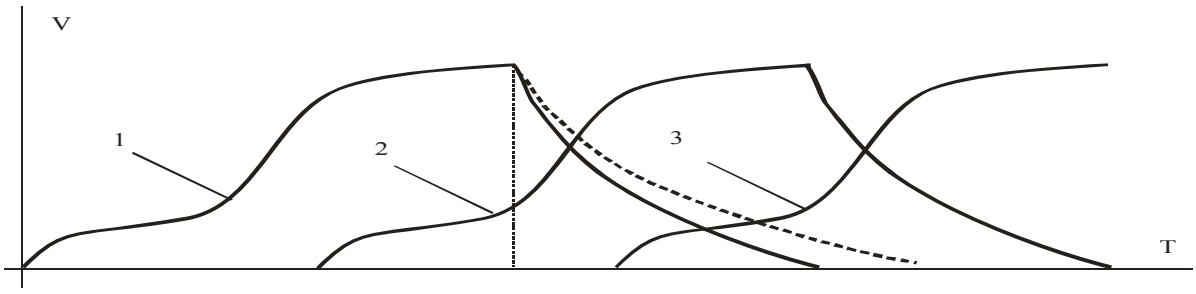


Рисунок 6.4 – Процес послідовних змін технологічних укладів
1 – домінуючий інформаційний технологічний уклад;
2 – новий біо-нано-технологічний уклад, що розвивається;
3 – насупний технологічний уклад, що буде зароджуватись.

Спадання старого технологічного укладу може відбуватися з різними швидкостями. Надто швидке спадання може привести до загального спаду виробництва, коли становлення нового укладу не встигає набрати свого розвитку. Коли спад старого технологічного укладу затягується, то виникає

багатоукладна економіка, де одночасно існують три-чотири уклади. Багатоукладність економіки приводить до розпорошування ресурсів, непродуктивних витрат на підтримування застарілої техніки, до недостатності ресурсів і коштів для розвитку нових технологій, на відтворення одночасно декількох технологічних укладів.

Якщо суспільство не консервативне і не допускає багатоукладності економіки, тоді маємо у кожен момент часу два уклади – стабільний домінуючий та новий, який розвивається.

Новий технологічний уклад зароджується й існує (в ембріональному стані) в рамках попереднього укладу, задовго (мінімум на протязі одного періоду зміни людського покоління) до завоювання ним свого домінуючого стану. Система освіти й соціальної перебудови має цілком достатньо часу для глибокого оволодіння новим технологічним укладом, щоб, в потрібний порівняно короткий історичний момент, забезпечити суспільство, виробництво й політику й державні інституції необхідними знаннями, навичками й засобами швидкого й усталеного переходу на новий вже дозрілий технологічний уклад [85].

6.3. Загрози соціальному капіталу та соціальній інформації в умовах зміни технологічних укладів

Соціальний капітал має циклічний характер розвитку та занепаду, а також тенденцію до прискорення розвитку. У порівнянні з технологічними укладами соціальний капітал суттєво більш інерційний. Найбільший вплив на розвиток людства мали і мають переходи у веденні господарства від одних науково-технологічних форм до нових, які можна назвати науково-технологічними революціями. Найбільш визначними з них були такі три переходи.

Близько десяти тисяч років тому, за часів неоліту відбувся перехід від мисливсько-збирального господарства до землеробства. Перехід тривав декілька тисячоліть, привів до соціалізації людини і став значним завоюванням у процесі завершення її зрілості. До цього переходу наші предки постають перед нами групами навколо вогню.

Невпинний прогрес розмноження привів до швидкого росту чисельності людей, вільна територія зменшилась. Групи зіштовхувались між собою. Постала необхідність здобування найбільших результатів із все менших територіальних володінь. Ймовірно за необхідністю виникла ідея збереження та репродукції того, що раніше доводилось шукати та переслідувати вдалечині [190]. У зростаючих поселеннях з’являється складна сукупність прав та обов’язків, яка вимушувала придумувати усякого роду общинні структури та закони. Стало зароджуватись і те, що тепер називають соціальним капіталом.

У другій половині 18-го століття почався перехід від землеробства до індустріальних культур. Зачатки цього переходу були підготовлені створенням мануфактурного виробництва, яке існувало в Західній Європі з середини 16 століття до останньої третини 18 століття. Стрибок у розвитку виробничих сил, що називають ще промисловим переворотом, почався у Великобританії в 60

роки 18 століття. Потім до кінця 19 століття на цей шлях вступили США, Франція, Німеччина, Італія, Японія.

У Росії цей процес розпочався 1885-1905 рр. і був перерваний революцією та громадянською війною, завше продовжився у 1927-1933 рр. могутніми темпами індустріалізації, масовим виходом селян до промислових міст. Робфаки, ліквідація неграмотності, загальна семирічна, а потім десятирічна освіта, виникнення нових індустріальних центрів є результатом переходу до індустріального суспільства, як економіко-технологічної формації. Все це не означало зменшення обсягів виробництва сільськогосподарської продукції. В результаті індустріалізації (механізації, хімізації, виробництва добрив, автоматизації тощо) у сфері землеробства залишилося мало людей, але продуктивність їх праці значно виросла\. Для соціальних норм наслідки переходу від землеробських до індустріальних суспільств були вельми кардинальними.

У наш час відбувається перехід від індустріальної до постіндустріальної економіки, який ще називають переходом до інформаційного суспільства, і який проходив у країнах Західної Європи приблизно з середини 1960-х до початку 1990-х років. Такий перехід підготовлений інтенсивним розвитком електроніки та мікроелектроніки, поширенням мініатюризації, зростанням ролі кібернетики, інформаційних технологій, інтелектуальної праці. Знову таки, це не означає значного згортання обсягів індустріального виробництва, а більш ефективну його організацію, впровадження економних технологій, автоматизацію та роботизацію виробництва. Все більше проявляються такі ознаки переходу до постіндустріального суспільства [197]:

- в економіці послуги щораз більше витісняють виробництво як джерело добробуту;
- щораз більше зростає роль інформації та інтелекту, якими тепер наділено і людей, і все розумніші машини, а розумова праця дедалі більше заступає фізичну;
- виробництво глобалізується, оскільки інформаційна техніка полегшує рух інформації через кордони;
- швидкий зв’язок розмиває межі давно сформованих культурних спільнот;
- інформаційне суспільство більш схильне продукувати свободу і рівність: зросла свобода вибору, телеканалів, магазинів чи друзів через Інтернет;
- зазнають тиску та починають розпадатися ієрархічні структури всіх видів, як державні так і корпоративні;
- економіка засновується на знаннях, особі надається повний доступ до інформації для ефективного виконання роботи.

Багато переваг інформаційного суспільства є очевидними, але на жаль, є й негативні наслідки перехідного періоду, який у Френциса Фукуями зветься Великим Крахом суспільних вартостей. Як і у попередні перехідні періоди, динаміка нинішніх негативних змін в суспільстві є результатом переходу та

технологічного прогресу, за яке суспільство платить численними та болісними розривами традиційних зв'язків.

У соціальному та моральному житті проявились недоліки:

- розпад ієрархічних політичних і корпоративних структур всіх видів;
- скорочення зайнятості у традиційному індустріальному виробництві, серйозне погіршення соціальних умов;
- зростання злочинності і порушень громадського порядку;
- прискорення занепаду такої соціальної інституції як родина; падіння народжуваності, народження дітей поза шлюбом;
- занепад довіри до державних інституцій і впевненості в них та у співгромадянах.

Зміни характеру праці призводили до заміни фізичної праці розумовою, що підштовхнуло мільйони жінок піти на роботу і зруйнувало традиційні уявлення про сім'ю. Новації в медицині призвели до зростання тривалості життя і применшили роль відтворення і сім'ї в житті людей. Культура глибокого індивідуалізму, яка вкоренилася в торгівлі, в лабораторії, у виробництві, перелилася також у сферу соціальних норм, де роз'їла майже всі форми підпорядкованості й послабила зв'язки, що цементували сім'ї, регіональні спільноти та нації.

Технологічні зміни призвели до «творчої руйнації» на ринку, зумовили також подібну руйнацію в світі соціальних стосунків. Але зруйнований соціальний порядок виявляє тенденцію до повторного відновлення. Люди за природою своєю є істотами соціальними, і найголовніші їхні прагнення та інстинкти ведуть їх до створення моральних норм, які об'єднують їх у спільноти. Люди за природою також раціональні, і їхня раціональність дозволяє їм створювати різні способи спонтанної взаємодії. При цьому важливим є громадянське суспільство, яке впорядковується за допомогою великої кількості моральних норм.

Науково-технологічний прогрес не зупиняється і його темпи людством ще не контролюються і не управляються. Як вже наголошувалось, в період від 2015 до 2030 років очікується перехід до наступних технологій: нанотехнологій, мікробіологічних технологій виробництва продовольства, досягнень генетичних методів, психології та управління поведінкою людей.

Нанотехнології напевне призведуть таку ж революцію у маніпулюванні матерією, яку призвели комп'ютери у маніпулюванні інформацією. Можна очікувати загального розповсюдження надскладних і надшвидкісних систем та конвергенції живої та неживої матерії. Якщо нинішні тенденції збережуться, то людство чекає життя в умовах постійно змінюваних технологій, що здається не цілком раціональним.

Поки що не зовсім ясно, наскільки наступні технології будуть революційними з точки зору впливу на соціальний капітал. Інформаційне та постінформаційне суспільство напевне будуть мати багато спільних рис: широке застосування комп'ютерів, програмування, тенденція до покращення якості життя. З іншого боку, у виробництві змінюється рівень маніпулювання з міні- й мікро-маніпулювання до наноманіпулювання.

Людина стає менш захищеною. Активно розвиваються методи соціальної психології та інформаційного впливу на людей.

Закон України «Про основи національної безпеки» визначає основні засади гарантування в Україні безпеки особи, суспільства і держави від зовнішніх і внутрішніх загроз національним інтересам і національній безпеці України в усіх сферах життєдіяльності. В інформаційній сфері виокремлено загрози:

- прояви обмеження свободи слова та доступу громадян до інформації;
- комп'ютерної злочинності та комп'ютерного тероризму;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Національна безпека України залежить від цілісності, доступності й спостережності соціальної інформації, надійності й готовності критичних фізичних та інформаційних інфраструктур. Соціальна та інша відкрита інформація важливі для держави настільки, що їх спотворення або знищення можуть привести до згубних наслідків в області економіки, оборони, охорони здоров'я та національної безпеки. Стає великою залежність всіх технологій від загроз інформаційним технологіям і вразливості останніх.

Програмно-математичний вплив на інформаційно-комунікаційні системи, так звані комп'ютерні атаки, засоби інформаційного протиборства направлені на використання, модифікацію, підміну або знищення інформації, яка міститься у комп'ютерах та інформаційних мережах, зниження ефективності функціонування або виведення з ладу самих комп'ютерів та інформаційних мереж. До них відносяться засоби несанкціонованого доступу, комп'ютерні віруси, програмні закладки, «логічні бомби» та «троянські коні», нейтралізатори тестових програм, навмисне створені приховані інтерфейси для входу в інформаційну систему з корисними або диверсійно-підривними намірами, створення непомітних завад інтелектуального впливу на системи зв'язку, збирання та обробка інформації шляхом блокування, підміни у повідомленнях ключових елементів, введення у повідомлення хибних ключових елементів.

Завади інтелектуального впливу треба враховувати у системах забезпечення безпеки суспільно політичних відносин в рамках забезпечення національної безпеки. Вони базуються на автоматизованому аналізі структури повідомлень, слідкуванні за ключовими словами, синтезі мови у реальному масштабі часу. Небезпека таких загроз у тому, що фальсифікація може проводитись не лише власником чи розпорядником інформації, за що він має нести відповідальність перед законом, а й противником, приховано, під час передачі інформації телекомунікаційною мережею.

Навмисне руйнування, переривання або перекручення даних у цифровій формі або потоків інформації приводять до широкомасштабних наслідків у

політичному, релігійному або ідеологічному планах. Інформація викрадається, перекручується, обмежується, фільтрується з метою впливу (або несанкціонованого виключення впливу) на психіку людини, психологію великих мас людей, суспільну свідомість з метою примусити їх думати і діяти в напрямі, потрібному для того, хто організує та здійснює цей вплив [84].

Рівень небезпечності загроз цільового інформаційного впливу прямо пропорційний рівню технологічного розвитку мереж та масштабам застосування комп'ютерів у системах управління мережею, галуззю і державою в цілому. Зростає важливість вимог забезпечення цілісності та достовірності передачі відкритої інформації, захисту від порушень правил маршрутизації, точності й своєчасності доставки інформації (мінімальної затримки повідомлень), а також захисту від несанкціонованого доступу до інформаційних ресурсів мереж та забезпечення фізичної безпеки інформаційної інфраструктури. Безпека інфраструктури держави в цілому залежить від рівня безпеки державних і комерційних інформаційних та телекомунікаційних систем.

З початком інформаційної ери з'явився й інформаційний тероризм, який має два різновиди: інформаційно-психологічний та інформаційно-технічний. Інформаційно-психологічний тероризм орієнтований на використання різних форм та методів впливу на інформаційно-психологічне середовище. Він характерний цілеспрямованим використанням ЗМІ для створення у суспільстві особливого психологічного становища, яке несе катастрофічні наслідки для життєдіяльності інформаційно-психологічного середовища суспільства й держави.

Інформаційно-технічний тероризм – це нанесення збитків окремим фізичним елементам інформаційного середовища держави: наведення завад, використання руйнівних програм проти систем управління, або зовнішнє несанкціоноване управління технічними об'єктами, хімічні та біологічні засоби руйнування, знищення ліній зв'язку, неправильна маршрутизація, штучне пере завантаження вузлів комутації тощо.

Сучасній цивілізації є такі загрози: руйнування середовища мешкання; ослаблення популяційного здоров'я, зокрема, порушення генома людини; руйнування налаштованих на протязі тисячоліть механізмів соціальної стабілізації. Останнє походить від того, що матеріальні умови життя змінюються швидше, ніж суспільство встигає відповідним чином модифікувати стабілізаційні механізми. Коли руйнуються традиційні механізми стабілізації, зокрема соціальний капітал), а нові запізнюються чи терплять поразку, то нагнітається соціальна напруженість, життєві цінності втрачаються, виникає тероризм, релігійні цінності збочуються, руйнується судова система, розквітає корупція.

Інформаційні ресурси мають бути надійно захищені від негативних інформаційних впливів: мають бути виключені можливості для підміни або знищення соціальної інформації з найважливіших питань образу життя народу України.

Необхідно управляти соціальним капіталом, а також управляти технічним прогресом, обираючи «розумні» темпи економічного розвитку, за яких встигають адаптуватись суспільні відносини. Нові технології необхідно впроваджувати з урахуванням соціально-політичних наслідків їх впливу на соціальний капітал.

6.4. Менеджмент соціальних технологій з відновлення соціального капіталу

З прискоренням технологічного та інформаційного прогресу змінюється рівень маніпулювання людьми, людина стає менш захищеною, розвиваються методи соціальної психології та інформаційного впливу на людей. Необхідно управляти соціальним капіталом та враховувати соціально-політичні наслідки впливу на соціальний капітал.

В системі діагностики соціального капіталу та соціальної інформації збирають дані стабільності соціальних показників суспільства: здоров'я, громадської безпеки, освіти, праці (вибір цінностей, вдоволеність працею), доходів, житла, дозвілля та відпочинку, демографії.

Мірою соціального капіталу може бути степінь довіри, яка є між членами-суб'єктами сім'ї, общини, групи, спільноти, суспільства, бізнесу, ринку, держави. Довіра – це паливо світової фінансової системи, а зовсім не гроші, які може друкувати будь-який державний чи приватний банк. Коли довіра вичерпується, система деградує. Довіра – це основа ринку, основа ринкового обміну. Довіра – це основа взаємодії між людьми.

Одиницею виміру може бути радіус довіри чи горизонт довіри, який може обмежуватись сім'єю, общиною або іншою групою. Якщо радіус довіри, необхідний сучасній економіці, зменшується, то скорочується горизонт інвестування, виробництва та споживання. Останні скорочуються до одного простого циклу відтворення – продовольства, простих предметів та послуг.

Стан соціального капіталу слід розглядати як один з показників національної безпеки. Національна безпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам. Національні інтереси – це життєво важливі матеріальні, інтелектуальні і духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства і держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток. Коротко формулюється завдання захисту національних інтересів у США – це захист народу, території та образу життя.

Інформаційні ресурси мають бути надійно захищені від негативних інформаційних впливів: мають бути виключені можливості для підміни або знищення соціальної інформації з найважливіших питань образу життя народу України. Системи захисту інформації мають забезпечувати соціально-психологічні організаційні засоби – роботу з персоналом, користувачами,

кадровим забезпеченням, в якій головна увага приділялась би людському факторові й соціальному капіталу. З численних статистичних даних випливає що до 60% інцидентів з інформаційною безпекою пов'язані з людським фактором: помилки чи некомпетентність персоналу та користувачів, зловмисні та незловмисні дії, підкуп персоналу, порушення корпоративної солідарності тощо.

Особливо важливим є захист і підтримка соціального капіталу при забезпеченні усталеного розвитку сучасної цивілізації. *Усталений розвиток* – це такий суспільний розвиток, за якого не руйнується його природна основа, створювані умови життя не тягнуть за собою деградацію людини й соціально-деструктивні процеси не розвиваються до масштабів, які загрожують безпеці суспільства [32].

Задачі менеджменту соціального капіталу ускладнюються під час переходу до нового технологічного укладу. З 20-х років цього століття шостий технологічний уклад вступить у фазу швидкого росту. Загальною прикметою цього росту буде розширення ділових послуг, телекомунікацій, культури, та освіти. З характеру моделей перехідних процесів зміни технологічних укладів витікають дві задачі стосовно маркетингу.

Перша задача – це менеджмент (управління) зсувами технологічних укладів. Ця задача вирішується у теорії стійкого розвитку.

Другою задачею є менеджмент стійкого відтворення соціального капіталу, що частково розробляється в теоріях соціальної психології та інформаційних війн. Обидві задачі торкаються великих та широких проблем. Намітимо тут основні контури їх вирішення.

Сучасний підхід може бути сформований на базі досягнень синергетики, яка виявила ряд універсальних закономірностей, притаманних різним галузям знань, зокрема в фізиці й соціальних науках. На цій базі вже ставиться задача «конструювання майбутнього»

Конструювання природної та соціальної дійсності породжує когерентний, взаємо узгоджений світ. Конструююча людина та світ, який він конструює, складають процесуальну єдність. Конструювання означає, що людина як суб'єкт пізнання та діяльності бере на себе весь тягар відповідальності за отриманий результат. Суспільство, яке само організується може стійко існувати і тривалий час динамічно розвиватися, якщо кожен його член веде себе так, якби він – у міру своїх можливостей – був відповідальний за ціле.

За сенергетичним принципом холізму, відносно прості структури мають резонансно об'єднуватися у складне стійко еволюціонуюче ціле. Тоді, в результаті резонансного об'єднання єдина структура набуває більш високий темп розвитку, ніж темп розвитку самої швидкої за розвитком структури до об'єднання. Вигідно розвиватись разом, бо це приводить до економії матеріальних, енергетичних, духовних витрат. Цей науковий факт збігається з основними постулатами соціального капіталу

Синергетичні принципи коеволюції можуть застосовуватись для вироблення розумної національної та державної політики у світі, що

глобалізується, для утвердження толерантності й збереження різноманіття у суспільствах. Ці принципи співзвучні принципам, що укріплюють соціальний капітал:

- жити один з одним, а не проти один одного;
- жити так, щоб не зменшувати шанси інших, зокрема майбутніх поколінь, жити так же добре;
- турбуватись при тих, хто бідний та безправний, а також про стан навколишнього середовища (тобто мати толерантність та екологічну свідомість).

Необхідно культивувати у кожного почуття відповідальності за ціле. Кожен елемент (особистість, сім'я, етнос, держава) підтримує свою ідентичність. Кожен елемент творить себе через ціле і перетворює ціле, творячи самого себе.

Сучасне економічне зростання характеризується провідним значенням науково-технічного прогресу та інтелектуалізації основних факторів виробництва. На долю нових знань, які утілюються у технологіях, обладнанні, освіті кадрів, організації виробництва припадає до 70-85% приросту ВВП [26]. Інформаційні технології розширили можливості генерування й передачі знань і науково-дослідних і конструкторських робіт (НДКР), різко збільшили потреби і можливості освіти та творчої діяльності. Проведення НДКР займає все більшу вагу в інвестиціях. Сьогодні мільйони людей використовують у якості засобів виробництва лише свій інтелект, підкріплений персональним комп'ютером.

Настане ще більша інтелектуалізація виробництва, перехід до безперервного інноваційного процесу у більшості галузей та до неперервної освіти у більшості професій. Завершиться перехід від «суспільства споживання» до «інтелектуального суспільства», якому будуть найважливішими вимоги до якості життя й комфортності середовища мешкання. Виробнича сфера перейде до екологічно чистих та безвідходних технологій. У структурі споживання домінуюче значення займуть інформаційні, освітні, медичні послуги.

Фахівцю доведеться постійно вчитись – навчання і застосування майже не розділяються й інтегруються. Навчання має бути: загальним, неперервним; самостійним; включати в себе елементи дослідно-експлуатаційної, дослідно-конструкторської та науково-дослідної роботи (НКДЕР); відображати практичні потреби нового технологічного укладу. Випускник навчального закладу має бути здатним працювати в ланцюзі НДР – ДКР – випробування – виробництво.

Для включення у освітній процес елементів НКДЕР та щоб відповідати потребам нового укладу типовий вищий навчальний заклад має бути перетворено у технологічно-дослідний та конструкторсько-дослідний навчальний заклад. Має бути реалізовано безперервний процес впровадження наукових результатів, де проектування, конструювання, випробування й виробництво пересікаються й інтегруються.

Однією з важливих задач менеджменту розвитку є задача оптимального темпу розвитку. Розвиток технологій на протязі усього розвитку технологій йшло, в основному, стихійно. Замовником технологій виступав ринок та армія.

Певне значення в історії розвитку техніки лежить на винахідниках, які часто прагнуть вгамувати власну спрагу іновацій. Ключовим суб'єктом прогресу завжди був і буде винахідник. Але критична ситуація, до якої наближається людство, вимагає переосмислити роль іновацій та винахідництва.

Головним винуватцем є не винахідник, а замовник. Критерієм відбору інновацій встановлюються замовниками. Ці критерії відображали ринкову чи військову ефективність. Сьогодні до критерію ефективності треба додати побічні наслідки впровадження новації – її вплив на стан оточуючого середовища, популяційне здоров'я та стійкість соціуму.

Тому важливою задачею є визначення області стійкості цивілізації: меж руйнування тих структур, які забезпечують відтворення та стабільність оточуючого середовища, популяції людства та людського суспільства.

Для управління соціальним капіталом необхідно знати закони його відтворювання, особливо у перехідні періоди змін технологічних укладів та аналізувати взаємозалежності між економічними процесами технологій та соціального капіталу.

Існує дві протилежні позиції щодо менеджменту соціального капіталу. Відомий автор концепції «кінця історії» Френцис Фукуяма вважає, що головне – це створення механізмів суспільного контролю за державними органами, які мають займатись регламентацією та моніторингом діяльності у сфері технологій [198], та що наслідування ліберальним настановам є головною умовою успіху. Інша думка висловлюється у роботах Максима Калашникова [70], який закликає рішуче й енергійно зламувати бар'єри та рухатись у напрямі створення зверх людини.

В цілому, наші знання про людське суспільство поки що край недостатні.

Принципи побудови, політика безпеки і стратегія соціального захисту інформації розглядаються в наступному розділі.

Контрольні запитання та завдання

1. Поясніть у чому полягають особливості сучасного соціально-економічного розвитку.
2. Дайте визначення поняття «соціального капіталу».
3. Порівняйте властивості і взаємозв'язок фізичного, людського, соціального та інформаційного капіталу.
4. Дайте визначення і поясніть властивості інформації взагалі та соціологічної й соціальної інформації.
5. Яке призначення атрибутивної, комунікативної та функціональної складових соціальної інформації?
6. Проведіть класифікацію соціальної інформації за її типами.
7. Поясніть, у чому полягає вплив циклічності розвитку та зміни технологічних укладів на соціальний капітал?

8. Яким загрозам піддається соціальний капітал під час зміни технологічних укладів?

9. Які загрози національній безпеці виокремлюються у інформаційній сфері?

10. Які загрози є безпеці соціальної інформації?

11 Які існують загрози програмно-математичного та інтелектуального впливу?

12. Які існують види тероризму?

13. Поясніть задачі менеджменту соціального капіталу.

14. Які синергетичні методи можна застосувати для забезпечення сталого відтворення соціального капіталу?

15. Поясніть проблеми та методи забезпечення сталого розвитку цивілізації.

Завдання до самостійної роботи

1. Проаналізуйте залежність соціального капіталу від циклічності розвитку та зміни технологічних укладів:

- що називають технологічним укладом та які технології складають ядро технологічного укладу?
- характер та причини скорочення життєвого циклу технологій на прикладі довгих хвиль Кондратьєва;
- як історично змінювались базові технології, рушійні сили, провідний характер виробництва, використані матеріали й сировина технологічних укладів?
- які є характерні фази життєвого циклу технологічного укладу?
- який характер мають перехідні процеси спадання технологічного укладу?
- охарактеризуйте математичні моделі процесів спадання технологічного укладу: нормального закону, показникової функції та функції з «важким хвостом»;
- який характер носить взаємодія між новим і старим технологічним укладом за їх послідовної зміни?
- яким загрозам піддається соціальний капітал під час зміни технологічних укладів?
- якими ознаками характеризується постіндустріальне (інформаційне) суспільство?
- який негативний вплив на соціальний капітал є від зміни технологічних укладів?

РОЗДІЛ 7

ЗАХИСТ СОЦІАЛЬНОЇ ІНФОРМАЦІЇ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ

7.1 Феномен та роль соціальної інформації у соціальній та інформаційній безпеці

Слідом за розвитком інформаційних технологій посилюється вплив інформації на життя та діяльність людських спільнот у державі. Роль захисту інформації, що використовуються в системах управління державою, суспільством, економікою, культурою значно зросла, але одночасно збільшились їх уразливість від різного роду загроз.

Ефективність систем захисту суттєво залежить як від технічних факторів, так і, значною й вирішальною мірою, від людського (антропогенного) фактору. Це ставить проблему більш уважного вивчення ролі персоналу, користувачів, і взагалі людини у процесах захисту інформації, забезпеченні інформаційної безпеки діяльності особи, суспільства, держави, її економіки та виробництва на всіх рівнях.

Основними принципами інформаційних відносин, визначеними Законом України “Про інформацію”, є «гарантованість права на інформацію; відкритість, доступність інформації та свобода її обміну; об’єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації».

Всі громадяни України, юридичні особи і державні органи мають право на інформацію, що передбачає можливість „вільного одержання, використання, поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій”.

Основи державної політики щодо безпеки України в інформаційній сфері визначені основоположним Законом “Про основи національної безпеки України” [58]. Закон передбачає такі основні напрями державної політики з питань національної безпеки в інформаційній сфері:

- забезпечення інформаційного суверенітету України;
- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну;
- вжиття комплексних заходів щодо захисту національного інформаційного простору та протидій монополізації інформаційної сфери України.

Системи захисту інформації багатьох країн – Китаю, Росії, США – розвиваються з урахуванням реалій інформаційних воєн [132]. В нормативних документах з технічного захисту інформації на програмно-керованих АТС загального користування передбачається низка механізмів і заходів

забезпечення гарантій захищеності інформації, які стосуються організаційних заходів роботи з персоналом [116, 118].

Серед специфікацій гарантій захисту визначені рівні довіри до персоналу і, зокрема, передбачається дотримання вимог: до безпеки середовищ персоналу, до системи та контролю організації праці, до поведінки та контролю поведінки персоналу в робочий час та неробочий час.

Методика оцінки захищеності інформації включає перевірку дотримання нормативних гарантій забезпечення захищеності інформаційних ресурсів експлуатаційного середовища, гарантій забезпечення інформаційної захищеності середовищ розробки та випробувань АТС, а також безпеки середовища творців АТС, середовища експлуатаційного персоналу.

В практику міжнародної стандартизації та в зарубіжних публікаціях введено поняття «соціальної безпеки» – societal security, обробки інцидентів з безпекою при забезпеченні безперервності функціонування та управлінні постійною готовністю [216].

Інформація відіграє провідну роль у всіх процесах функціонування інформаційного й постінформаційного суспільства. В сучасних умовах з'явився феномен, так званої «соціальної інформації», роль якої важлива в контексті інформаційного протиборства та національної безпеки.

Масове впровадження в усі сфери життєдіяльності людини, суспільства та держави новітніх інформаційних технологій, на жаль, супроводжується застосуванням нових технологій несанкціонованого доступу до інформації, її зняття та інформаційного впливу на об'єкти інформаційної діяльності. При цьому розширюються зовнішні й внутрішні загрози інформаційної безпеки держави та її суб'єктів. Це зумовило глибинні зміни в системі інформаційної безпеки, як важливої складової національної безпеки держави, а також обумовило формування нових видів діяльності у сфері захисту інформації.

7.2. Причини, за якими необхідно захищати відкриту інформацію

Слід відмітити, що проблема захисту відкритої інформації поставлена зовсім недавно і часто ігнорується. Вважалось, що захистом секретної інформації та деякими обмеженнями можна забезпечити національну безпеку країни. Гігантські масиви відкритої інформації, важливої для суспільства і держави, потребують свого захисту.

Існуючі системи захисту інформації орієнтовані, в основному, на захист інформації з обмеженим доступом. Відкрита інформація теж стає об'єктом захисту. Важливість її захисту та обсяги інформації, вимоги щодо захисту якої встановлені законом, мають тенденцію до збільшення.

Є принаймні п'ять причини для захисту відкритої інформації:

- впровадження систем «електронного уряду»,
- розвиток електронної торгівлі,
- застосування електронного документообігу й цифрового підпису,
- поширення операцій інформаційних війн;
- поява феномену соціальної інформації.

Перша причина пояснюється появою посередника у відносинах між державними органами управління й органами самоврядування та населенням у вигляді мережі передачі даних чи Інтернет. Інформація може втрачати в мережах свої властивості цілісності, доступності та спостережності внаслідок технічних недоліків обладнання, природних завад, помилок персоналу та навмисних атак зловмисників на мережу та інформацію. Це може приводити до серйозних негативних наслідків: втрати довіри до урядових установ, погіршенню керованості, порушенням громадського порядку тощо.

Одним з перших нормативно-правових документів, у якому поставлена вимога, що «об'єктом технічного захисту на програмно-керованих АТС (автоматичних телефонних станціях), а також на відомчих, корпоративних АТС є конфіденційна, а також відкрита важлива для особи, суспільства та держави інформація, яка зберігається та циркулює на цих АТС», став НД ТЗІ 1.1-001-99 [116].

На далі цю норму було закріплено в нормативно-правовому документі [146]. Визначено, що:

- «В автоматизованих системах повинен забезпечуватися захист від несанкціонованого доступу до державних інформаційних ресурсів з боку мереж передачі даних, зокрема глобальних мереж»;
- «Передавання державних інформаційних ресурсів дозволяється тільки через вузли комутації, що мають атестат відповідності комплексної системи захисту інформації (КСЗІ) вимогам із захисту інформації».

Складовими державного інформаційного ресурсу, який має захищатись згідно діючого законодавства, є:

- інформація, що становить державну або іншу передбачену законом таємницю;
- конфіденційна інформація, яка є власністю держави або вимога щодо захисту якої встановлена законом, зокрема конфіденційна інформація про фізичну особу;
- відкрита інформація, яка є власністю держави.

Друга причина витікає з потреб безпеки електронної торгівлі, яка використовується у комерційних відносинах не лише для торгівлі електронними товарами чи електронних платежів, а й торгівлі фізичними товарами. Вибір товару, замовлення й платежі виконуються електронними засобами, а доставка товару – фізичними засобами. У даному випадку, окрім захисту комерційної таємниці є необхідність захисту інформації, яка за своїм статусом відноситься до відкритої.

В електронних комерційних відносинах небезпечними є порушення правильності ідентифікації та автентифікації об'єктів та суб'єктів цих відносин, втрата цілісності й доступності інформації та інших інформаційних ресурсів.

Третьою причиною є застосування електронного документообігу та цифрового підпису, які будуть охоплювати не лише конфіденційні, а й відкриті документи. Мова йдеться про надання електронному документові тієї ж юридичної сили, що й власноручно підписаному паперовому документу з «мокрою» печаткою, завіреного нотаріусом.

Задачі підтримання цілісності, доступності електронного документа, невідмовності від авторства документа та невідмовності від його отримання, взаємної ідентифікації та автентифікації мають вирішуватись на всіх етапах створення, приймання-передавання, отримання, перетворення електронних документів у форму, придатну для сприймання та зберігання.

Четверту причину можна віднести до найважливіших. Війна, як висловлювався німецький військовий та політичний діяч К. Клаузевіц, «є продовженням політики іншими засобами». У 21 столітті зроблені висновки, що «інформаційна війна є основним засобом сучасної світової політики, домінуючим способом досягнення політичної та економічної влади і способом організації ноосфери й світового інформаційно-психологічного простору у своїх інтересах» [132].

Масова комп'ютеризація, впровадження й розвиток інформаційних технологій сприяють зростанню інформаційного протиборства у політичній сфері. Управління інформаційними потоками перетворилось у вирішальний фактор завоювання, зберігання та утримання влади. Інформація є основним інструментом влади.

Інформаційна війна, як і війна гаряча, має в своєму арсеналі й аморальні методи: обман, брехню, напівправду, підтасовку, замовчування та перекручування фактів тощо. Правдива інформація є лише засобом досягнення переваги та своїх цілей.

Метою інформаційного протиборства є порушення інформаційної безпеки ворожої держави, цілісності чи стійкості системи її державного й військового управління, ефективний інформаційний вплив на керівництво, політичну еліту (тобто індивіди, які володіють найбільшим багатством, впливом, найвищим статусом), системи формування суспільної думки та прийняття рішень, а також забезпечення власної інформаційної безпеки для завоювання інформаційної переваги у інформаційному просторі.

У інформаційному протиборстві в сфері світової політики захист відкритої і закритої інформації стає одним з вирішальних факторів. За висновком провідного китайського теоретика інформаційної війни Шень Вей Гуана: «Щоб захистити політичну безпеку країни, треба навчитись вести інформаційну війну з використанням різних засобів масової інформації (ЗМІ). Крім того, необхідні заходи, засоби й технології захисту від несанкціонованого несприятливого інформаційно-психологічного впливу.

Розрізняють два види інформаційної боротьби: інформаційно-технічну та інформаційно-психологічну.

За інформаційно-технічної боротьби головними об'єктами впливу і захисту є інформаційно-технічні системи: системи зв'язку, телекомунікації, радіоелектронні засоби тощо.

За інформаційно-психологічної боротьби головними об'єктами впливу й захисту є психіка політичної еліти, персонал стратегічно важливих об'єктів та населення, системи формування суспільної свідомості, думки та прийняття рішень, соціальні об'єкти: окремі індивіди, соціальні групи, суспільство, держава, світове співтовариство.

Інформаційна боротьба може вестись на трьох рівнях: стратегічному, оперативному, тактичному. На стратегічному рівні можуть діяти, в основному, органи державної влади, на оперативному рівні − спецслужби та великий капітал, на тактичному та оперативному рівнях − керівництво й підрозділи суспільних та виробничих формувань.

П'ята причина захисту відкритої інформації тісно зв'язана з попередньою причиною та появою феномена соціальної інформації. Девізом інформаційного суспільства є інтелектуальна конкурентно спроможність. У інформаційному суспільстві більше половини робочого часу буде використовуватись на зберігання, обробку й передачу інформації. Спостерігаються неймовірні прискорення приросту знань людства. У 70 роки 20 століття обсяг знань людства збільшувався вдвоє за 10 років, у 80-і роки – раз у 5 років, до кінця 90-х років обсяг знань людства подвоювався практично кожен рік [132]. Прискорення інформаційних процесів, посилення комунікативності й ціле направленості взаємодій підвищує живучість індивіда, спільнот, суспільства, соціальних систем, але й створює нові вразливості. В сучасних умовах з'явився феномен, так званої «соціальної інформації», роль якої важлива в контексті інформаційного протиборства та національної безпеки і яка потребує захисту.

7.3. Поняття про систему соціального захисту інформації

Законодавством визначені поняття криптографічного та технічного захисту інформації.

Криптографічний захист інформації (КЗІ) – це вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховання/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо.

Клас систем КЗІ можна представити рис. 7.1.а, на якому наглядно показано характерне співвідношення нерозривних складових класу:

- криптографічних засобів,
- технічних засобів та
- організаційних заходів захисту.

Криптографічний захист інформації застосовується для захисту інформації, яка передається каналами зв'язку або зберігається в базах даних, робочих станціях, міститься у парольних та ключових даних систем аутентифікації та розмежування доступу. Споживачами послуг системи КЗІ є суб'єкти органів державного управління, оборони, надзвичайних ситуацій, правопорядку, національної безпеки, розвідки тощо.

Технічний захист інформації (ТЗІ) – це вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

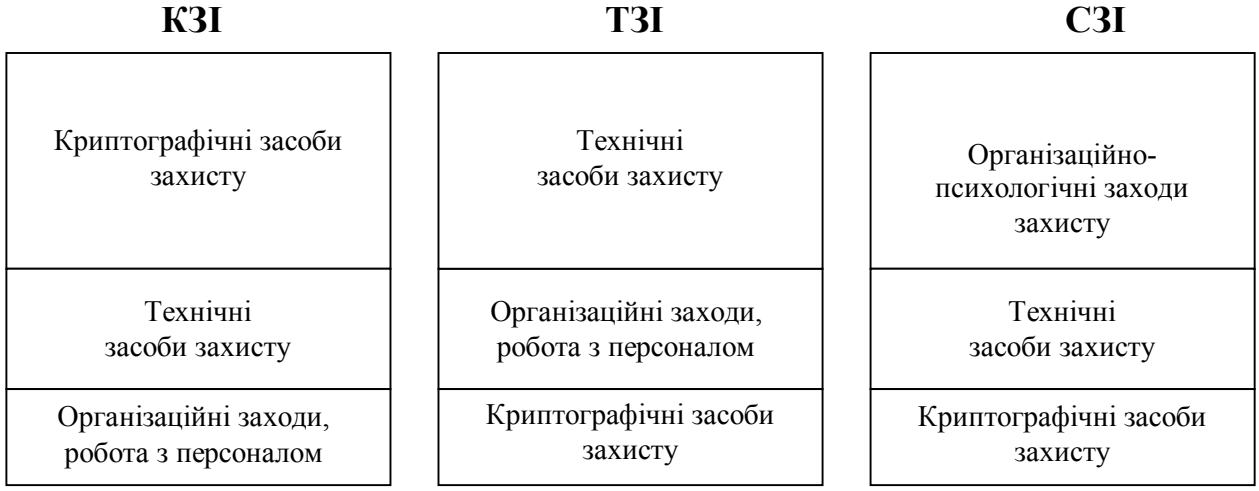


Рисунок 7.1 – Класи та складові класів систем захисту інформації

Він реалізується системою ТЗІ, яка згідно державного стандарту [38] є сукупністю організаційних структур, нормативно-правових документів та матеріально-технічної бази, що, в свою чергу, складається з таких елементів:

- захищені технічні засоби,
- засоби ТЗІ та
- засоби контролю за ефективністю ТЗІ.

Таким чином, клас систем ТЗІ можна представити рис. 7.1.б з характерним співвідношенням його складових:

- технічних засобів,
- організаційних заходів захисту та
- криптографічних засобів (за необхідності).

Криптографічні заходи ТЗІ мають тут обмежене, але невід'ємне застосування – для захисту інформації, що зберігається на носіях та передається каналами зв'язку між елементами інформаційної системи. Серед організаційних засобів захисту необхідну і суттєву роль відіграють послуги та механізми захисту, які пов'язані з персоналом.

Клас систем ТЗІ застосовується в інформаційно-технічній боротьбі з метою захисту інформаційного середовища суспільства та захисту об'єктів інформаційної діяльності (ОІД) за принципом «кругової оборони». Споживачами послуг системи ТЗІ є, в основному, підрозділи, які захищають інформацію з обмеженим доступом, комерційні структури, банки.

З міркувань симетричності, яка є одною із фундаментальних властивостей природи, та почуття естетичності функціональної повноти класів систем захисту інформації, яке по праву вважається критерієм правильності технічних рішень, а також потреб практичної діяльності має бути реалізований клас систем захисту інформації, в якому головну роль, поряд з технічним та криптографічним забезпеченням системи захисту, відігравали б соціально-психологічні організаційні засоби – робота з персоналом, користувачами, кадровим забезпеченням, тобто в якому головна увага приділялась би

людському факторові. Характерне співвідношення складових цього класу систем соціального захисту інформації (СЗІ) наведене на рис. 7.1.в.

Криптографічні засоби СЗІ забезпечують захист відкритої інформації в системах електронного документообігу, цифрового підпису, технологічної та приватної інформації.

У відповідності з методологічним принципом – бритвою Оккама – не слід створювати суттєвості без необхідності. Але в даному разі є вагомі обґрунтування введення поняття ще одного виду захисту – СЗІ. З численних статистичних даних випливає що до 60% інцидентів з інформаційною безпекою пов'язані з людським фактором:

- помилки чи некомпетентність персоналу та користувачів,
- зловмисні та незловмисні дії,
- підкуп персоналу,
- порушення корпоративної солідарності тощо.

Є особливості в методах захисту відкритої інформації у порівнянні із захистом інформації з обмеженим доступом. До цих особливостей можна віднести:

1) значний обсяг відкритої та закритої інформації, які підлягають захисту, що вимагає застосування автоматизованих систем і засобів захисту;

2) переважання короткоживучої інформації, що приводить до зменшення строків її обробки та запам'ятовування в системі;

3) зростання ролі соціальної інформації в підтримці і забезпеченні національної безпеки, що посилює необхідність її захисту.

СЗІ забезпечують проведення організаційно-психологічних заходів для захисту соціальної інформації. Системи СЗІ мають функціонувати на об'єктах інформаційної діяльності органів державного управління та самоврядування, фірмах та підприємствах будь-якої форми власності, суспільних організаціях, об'єднаннях громадян тощо.

Споживачами послуг системи СЗІ є суб'єкти системи національної безпеки, органів державного управління, систем інформаційної безпеки комунікацій (транспорту, енергетичних мереж, паливо-проводів, зв'язку), систем забезпечення життєдіяльності, оборони, надзвичайних ситуацій, правопорядку, промислових об'єктів тощо.

Системи КЗІ, ТЗІ, СЗІ взаємо зв'язані одна з одною. Вони можуть бути складовою частиною інших систем безпеки: економічної безпеки, екологічної безпеки, енергетичної, продовольчої безпеки тощо.

Найбільш важливою є взаємодія головних систем безпеки держави: національної безпеки, безпеки інформаційного простору, криптографічного, технічного і соціального захисту інформації (рис. 7.2).

Політика безпеки соціальної інформації має передбачати наступні задачі захисту:

- підтримка властивостей цілісності і доступності соціальної інформації;
- попередження негативних впливів інформації з точки зору інформаційного протиборства;

- інформаційне забезпечення процесів відтворення соціального капіталу в державі.

Рисунок 7.2 – Головні системи безпеки держави

7.4. Основи стратегії управління соціальним захистом інформації

Для захисту соціальних об'єктів та суб'єктів від негативних наслідків впливу в ході глобальної чи локальної інформаційної боротьби створюється система СЗІ та інформаційно-психологічного забезпечення як складова частина національної безпеки України.

Соціальний захист інформації (СЦЗІ) – це вид захисту інформації, спрямований на забезпечення за допомогою організаційних та психологічних заходів, а за необхідності інженерно-технічних та криптографічних засобів, унеможливлення впливу на інформацію, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації. Спосіб реалізації СЦЗІ та його склад потребують подальшого уточнення.

СЦЗІ призначена забезпечити інформаційну безпеку особи, суспільства та держави. Інформаційна безпека суспільства – це стан захищеності інформаційного середовища суспільства, яке забезпечує його формування й усталений розвиток в інтересах громадян та держави. При цьому, під інформаційним середовищем розуміють сукупність інформаційної інфраструктури, інформаційних ресурсів, систему формування, зберігання, розповсюдження, використання і захисту інформації.

Загроза інформаційні безпеці – це фактори чи їх сукупність, які створюють небезпеку функціонуванню та розвитку інформаційного середовища суспільства, організації, підприємства. Подібно тому, як ТЗІ є необхідним при забезпеченні правил обробки документів, які містять державну таємницю, так і СЦЗІ є необхідною при забезпеченні правил обігу й обробки соціальної й іншої відкритої інформації, та організації роботи з персоналом.

СЗІ захищає соціальну інформацію при забезпеченні психологічної безпеки еліти, персоналу та населення України. Система СЦЗІ не є ні ідеологічною системою, ні політичним органом. Хоча одним із її побічних

призначень є необхідність, хоча би частково, замістити вакуум, який утворився після краху соціалістичної ідеології та радянської політичної системи, у питаннях організаційно-психологічної роботи з персоналом, захисту соціальної інформації і підтримки соціального капіталу суспільства та забезпечення відтворення соціального капіталу в рамках інформаційної безпеки країни та її суб'єктів.

Система СЦЗІ не підміняє собою керування персоналом чи соціальний захист суб'єктів. Соціальний захист населення (СЗН), на відміну від СЦЗІ, – це система заходів й відповідних інститутів, призначених для захисту різних прошарків населення від економічної і соціальної деградації, пов'язаної з безробіттям, втратою або різким скороченням доходу, виробничою травмою, або професійним захворюванням, хворобою, інвалідністю, старістю, втратою годувальника, народженням дитини і т. п. Система СЦЗІ в рамках СЗН забезпечує захист соціальної і зокрема соціологічної інформації.

Система СЦЗІ відіграє не другорядну роль у веденні інформаційного протиборства і складає його невід'ємну частину. Інформаційне протиборство – це форма боротьби сторін, при якій використовується спеціальні – політичні, економічні, дипломатичні, військові тощо – методи, способи й засоби для впливу на інформаційне середовище противної сторони та захисту власної в інтересах досягнення поставлених цілей.

Інакше кажучи, система СЦЗІ відіграє у інформаційному протиборстві приблизну ту ж роль, що громадянська оборона відіграє у військові сфері. При цьому у СЦЗІ є і самостійна роль – роль фактору забезпечення відтворення соціального капіталу й захисту соціальної інформації за нормального функціонування суспільства.

Інформаційно-психологічний вплив – це є ціле направлене виробництво та розповсюдження спеціальної інформації, яка спричиняє безпосередній позитивний чи негативний вплив на соціальний капітал, на функціонування та розвиток інформаційно-психологічного середовища суспільства, психіку та поведінку політичної еліти, персонал економічної й технічної інфраструктури та населення країни.

Завданням і цілями управління СЦЗІ є захист інформаційних ресурсів в інформаційній сфері від несанкціонованого доступу, зокрема соціальної інформації, та забезпечення розумно достатнього рівня безпеки інформаційно-телекомунікаційних та електронних систем, де вона циркулює.

Місце СЗІ серед систем протидії загрозам безпеки держави показано на рис. 7.3. Відносно захисту від інформаційних впливів та захисту інформаційного простору системи КЗІ, ТЗІ, СЦЗІ займають рівноправне положення. При цьому система СЦЗІ має завдання захисту, головним чином, соціальної інформації та соціального капіталу.

Сфера СЦЗІ нормується державою, підконтрольна державі та суспільству і створюється для забезпечення національної безпеки, усталеного розвитку суспільства і людини в умовах інформаційних воєн та інформаційного впливу.

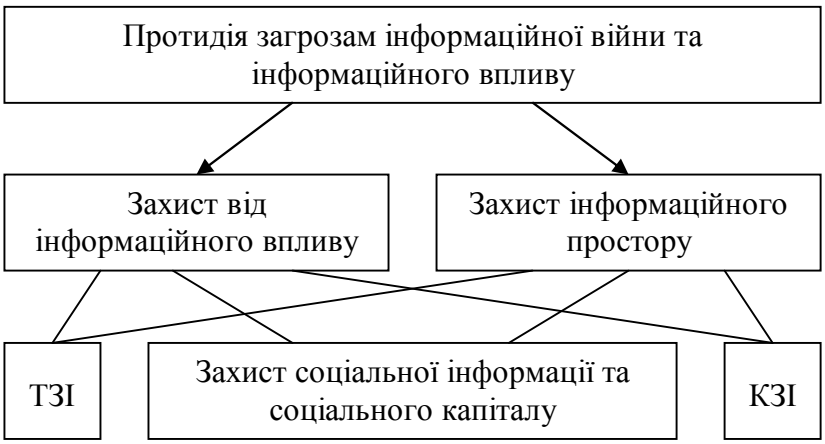


Рисунок 7.3 – Місце СЦЗІ в системі протидії загрозам безпеки держави

Задачами управління СЦЗІ на державному рівні є:

- захист від засобів небезпечного впливу на інформаційну сферу;
- протидія маніпуляціям суспільної свідомості та формування очікувань суспільної свідомості;
- протидія (виявлення та обробка інцидентів) з порушенням нормального функціонування інформаційно-телекомунікаційних систем;
- забезпечення цілості інформаційних ресурсів, включаючи цілість захищаємої інформації, цілісності засобів обробки, зберігання та передачі інформації, прийнятного рівня соціального капіталу та персональних соціальних показників персоналу;
- протидії отриманню несанкціонованого доступу до інформаційних ресурсів;
- протидія порушенням прав та свобод громадян та юридичних осіб;
- сприяння створенню соціально-економічних умов для здійснення творчої діяльності;
- вироблення форм та засобів суспільного контролю за формуванням у спільнотах духовних цінностей, які відповідають національним інтересам країни, вихованням громадянської та корпоративної відповідальності;
- розробка дійових організаційно-правових механізмів доступу ЗМІ, співробітників та громадян до відкритої інформації про діяльність органів державного управління та місцевого самоврядування, підприємств, організацій;
- розробка спеціальних правових , організаційних і технічних механізмів недопущення протиправних інформаційно-психологічних впливів на масову свідомість суспільства, спільнот і колективів, раціонального використання накопичених суспільством інформаційних ресурсів;
- протидія пропаганді насилля й жорстокості, анти суспільній поведінці, впливу іноземних релігійних організацій;
- діагностика та захист соціальної інформації;
- аналіз та збирання даних оцінки соціальної інформації, соціального капіталу та процесів які проходять у зовнішньому середовищі.

Місце СЦЗІ серед систем забезпечення безпеки показано на рис. 7.4.

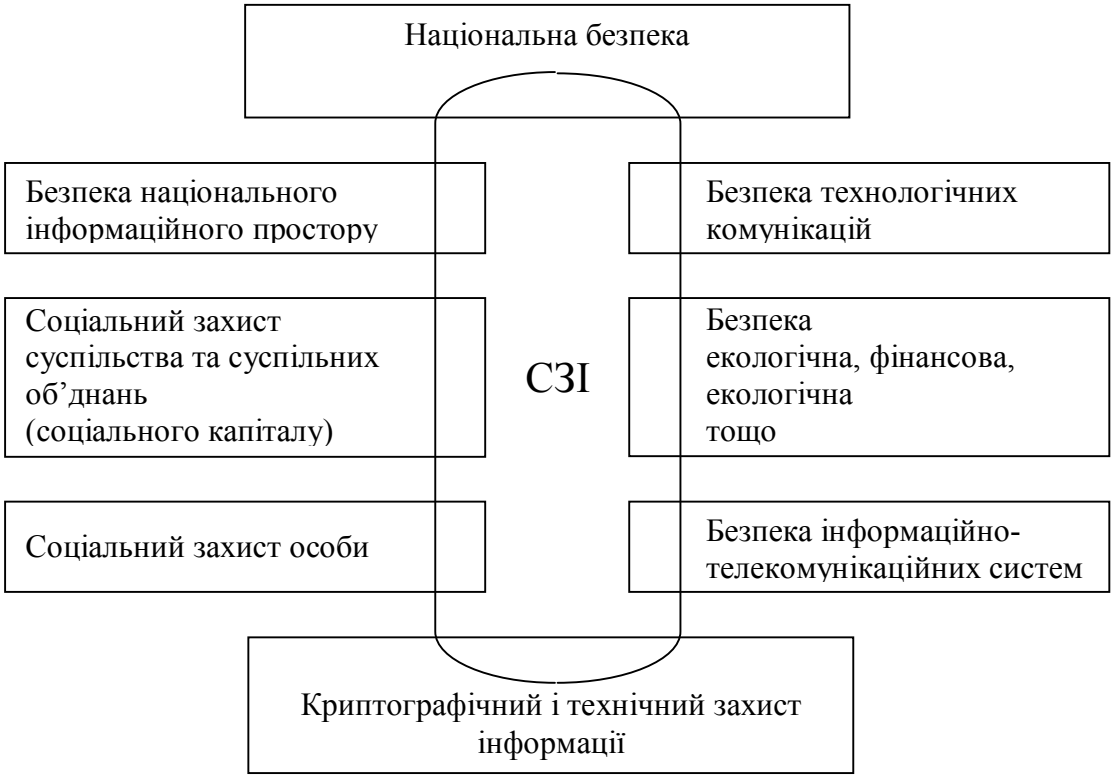


Рисунок 7.4 – Місце системи СЦЗІ серед систем забезпечення безпеки

Системи КЗІ та ТЗІ є складовими систем забезпечення:
- національної безпеки;
- безпеки технологічних комунікацій;
- безпеки економічної фінансової, екологічної тощо;
- безпеки інформаційно-телекомунікаційних систем.

Система СЦЗІ, крім того, є складовою частиною безпеки національного інформаційного простору, соціального захисту суспільства та суспільних об'єднань (соціального капіталу) та соціального захисту особи.

В класі систем ТЗІ розглядаються канали витоку інформації та канали впливу на інформаційні ресурси. Каналами витоку інформації є технічні, антропогенні канали витоку та канали несанкціонованого доступу. Вплив на інформацію та інші інформаційні ресурси здійснюється технічними каналами. Захисту підлягають інформаційні ресурси і, зокрема, інформація.

В класі СЦЗІ І, крім технічних каналів впливу на інформаційні ресурси, розглядаються інформаційно-психологічні канали впливу на суб'єкти інформаційних відносин. Захисту підлягають інформаційний простір держави, інформаційне середовище суспільства та людини, а також інформаційні ресурси.

Мірою ефективності СЦЗІ можуть бути показники якості соціального капіталу та його відтворювання, результати аналізу соціальної інформації.

СЦЗІ створюється на всіх рівнях: держави, суспільних організаціях та спільнотах, підприємствах, організаціях, фірмах.

Фахівець системи СЦЗІ має бути відповідним таким вимогам:

- здійснювати постійний контроль своїх дій, вчинків та можливостей;
- дотримуватись вимог конфіденційності;
- бути впевненим у собі, у своїх силах та можливостях;
- дотримуватись обережності та прихованості;
- мати власну систему отримання та аналізу інформації.

Система соціального захисту інформації, формально замикає класи захисту інформації в симетричні та функціонально повні відносно вирішуваних задач класи систем захисту. Практично СЦЗІ забезпечує виконання завдань захисту соціальної та інших видів відкритої інформації на підприємствах та установах будь-якої форми власності, суспільних організаціях та державі в рамках системи національної безпеки та захисту інформаційного простору України.

Контрольні запитання та завдання

1. Поясніть основні принципи інформаційних відносин, що визначені Законом України “Про інформацію”.
2. Які основні напрями державної політики щодо безпеки України в інформаційній сфері визначені основоположним Законом “Про основи національної безпеки України.
3. За якими причинами необхідно захищати відкриту інформацію.
4. Дайте визначення криптографічного захисту інформації. Хто є споживачем послуг криптографічного захисту інформації?
5. Дайте визначення технічного захисту інформації. Хто є споживачем послуг технічного захисту інформації?
6. Що називають соціальним захистом інформації?
7. Чому є необхідним соціальний захист інформації?
8. Хто є споживачем послуг соціального захисту інформації?
9. Які задачі соціального захисту мають бути у політиці захисту?
10. Сформулюйте призначення системи соціального захисту інформації.
11. Яка роль соціального захисту інформації у інформаційному протиборстві.
12. Наведіть основні положення стратегії управління соціальним захистом інформації.
13. У чому полягають завдання і цілі управління соціальним захистом інформації.
14. Поясніть місце соціального захисту інформації в системі протидії загрозам безпеки держави.
15. Поясніть місце системи соціального захисту інформації серед систем забезпечення безпеки.
16. Що може служити мірою ефективності системи соціального захисту інформації?
17. Які вимоги пред’являються до фахівців системи соціального захисту інформації?

Завдання до самостійної роботи

1. Проаналізуйте причини, за якими необхідно захищати відкриту інформацію:

- впровадження систем «електронного уряду». Що відноситься до державного інформаційного ресурсу? Які вимоги до інформаційної безпеки системи «електронного уряду»? Які загрози існують у телекомунікаційній мережі державним інформаційним ресурсам та які наслідки їх реалізації?;
- розвиток електронної торгівлі. Які вимоги до інформаційної безпеки системи «електронної торгівлі»? Які додаткові загрози інформаційним ресурсам існують у системи «електронної торгівлі»?;
- застосування електронного документообігу й цифрового підпису. Які задачі інформаційної безпеки електронних документів мають вирішуватись на всіх етапах їх створення, передавання, приймання, отримання, перетворення ;
- поширення операцій інформаційних війн. Поняття «інформаційна війна» та інформаційне протиборство. Що є метою інформаційних війн? Що є об'єктами інформаційно-технічної та інформаційно-психологічної війни? Як проводиться інформаційна боротьба на стратегічному, оперативному, тактичному:
- поява феномену соціальної інформації. Дати поняття «соціальної» інформації. Роль соціальної інформації в житті інформаційного суспільства.

РОЗДІЛ 8

ТЕХНОЛОГІЧНЕ УПРАВЛІННЯ МЕХАНІЗМАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

8.1 Загальні принципи управління безпекою об'єкта інформаційної діяльності

Управління інформаційною безпекою об'єкта інформаційної діяльності (ОІД) поділяється на:

- адміністративне управління інформаційною безпекою ОІД;
- технологічне управління інформаційною безпекою ОІД.

Адміністративне управління забезпечує організацію, супроводження контроль ефективної технічної і економічної діяльності підприємства чи організації, зокрема організацію та контроль діяльності служби безпеки та її матеріально-технічного забезпечення.

Технологічне управління інформаційною безпекою ОІД передбачає надання послуг службою безпеки та підтримання функціонування механізмів безпеки для забезпечення розумно достатнього нормативного рівня безпеки ОІД на всіх етапах життєвого циклу ОІД. Технологічне управління інформаційної безпеки є однією з головних завдань технічної експлуатації механізмів безпеки.

Управління безпекою у ОІД опікується власне управлінням безпекою ОІД та безпекою управління ОІД. Операції управління безпекою ОІД не належать до операцій нормального зв'язку, але вони є необхідні, аби підтримувати й управляти захистом цього зв'язку. Управління включає розподіл та опрацювання інформації управління і збирання інформації щодо дії послуг та механізмів безпеки. Прикладами цього є розподіл криптографічних ключів, установлення адміністративно призначених параметрів, фіксація нормальних і ненормальних подій безпеки (контрольний журнал) та послуг активації й деактивації.

База управління безпекою інформації (SMIB) є сховищем для всієї інформації, стосовної безпеки ОІД. Кожна кінцева система може містити необхідну локальну інформацію, аби давати можливість здійснювати відповідну політику. SMIB є базою розподілу інформації, котра необхідна для здійснення послідовної політики безпеки в кінцевих системах.

SMIB може бути реалізовано, наприклад, у вигляді:

- таблиці даних;
- файлу;
- даних чи правил, впроваджених в межах програмного забезпечення чи апаратних засобів реальних відкритих систем.

Управління безпекою може обмінюватись інформацією стосовно безпеки поміж різними адміністративними системами, для того аби встановити SMIB. Локальні системні адміністратори можуть модифікувати SMIB нестандартними методами. Прикладні програми управління безпекою користуються

інформацією з'єднання для модифікування SMIB. Це може потребувати попереднього дозволу відповідного адміністратора безпеки.

Типи функцій управління безпекою ОІД:

- управління системою безпеки в цілому;
- управління послугами безпеки;
- управління механізмами безпеки;
- управління безпекою системи управління ОІД.

Окрім того, має бути забезпечено й безпеку системи управління безпекою, включаючи довірче функціонування управління безпекою.

Управління системою безпеки в цілому займається управлінням безпекою загального середовища ОІД. Застосовуються такі типові функції:

- управління загальною політикою безпеки, включаючи відновлювання й технічне обслуговування процесів;
- взаємодію з іншими функціями управління ОІД;
- взаємодію з управлінням послугами безпеки й управлінням механізмами безпеки;
- управління опрацюванням подій;
- управління контролем безпеки;
- управління відновлюванням безпеки.

Управління послугами безпеки виконує такі функції:

- визначення і призначення мети захисту безпеки для послуг;
- призначення й вибір з альтернативних специфічних механізмів безпеки, які запитуються;
- узгодження локально чи дистанційно доступних механізмів безпеки, які потребують попереднього узгодження управління;
- звертання до спеціальних механізмів безпеки через функцію управління механізмами безпеки, наприклад для надавання адміністративно-призначених послуг безпеки;
- взаємодію з іншими функціями управління послугами безпеки й функціями управління механізмами безпеки.

Управління механізмами безпеки виконує такі функції, список яких є типовим, але не вичерпним:

- управління ключами;
- управлінням шифруванням;
- управління цифровим підписом;
- управління контролем доступу;
- управління цілісністю даних;
- управління автентифікацією;
- управління заповненням трафіка фоновою інформацією;
- управління контролем маршрутизації;
- управління нотаризацією.

Кожна з цих перелічених функцій обговорюється докладніше далі.

Управління безпекою системи управління ОІД. Безпека всіх функцій управління ОІД і передавання інформації управління ОІД є важливою частиною безпеки ОІД. Цей тип функції управління безпекою використовує відповідні

послуги й механізми безпеки ОІД, аби гарантувати, що протоколи та інформацію управління ОІД відповідно захищено. Протоколи управління, особливо протоколи управління безпекою й канали зв'язку, де циркулює інформація управління, є потенційно уразливими. Це потребує особливих заходів захисту і гарантій захищеності протоколів та інформації управління для будь-яких з'єднань.

8.2 Система управління інформаційною безпекою

Управління інформаційною безпекою ОІД включає в себе управління опрацюванням подій, перевіркою (аудит) безпеки та відновлюванням безпеки.

Система *управління опрацюванням подій*, виявлених у ОІД, дистанційно повідомляє про спроби порушування системи безпеки й модифікування умов для запускання процесів.

Управління перевіркою (аудит) безпеки може включати:

- вибір подій, які буде внесено до журналу та/чи зібрано дистанційно;
- долучення/вилучення контрольного реєстрування обраних подій;
- дистанційне збирання обраних перевірних записів;
- підготовку звітів про перевірення безпеки.

Управління відновлюванням безпеки може включати: технічне обслуговування правил реагування на реальні чи підозрювані порушування безпеки; дистанційний запис виявлених порушень системи безпеки; взаємодію адміністраторів безпеки.

Адміністратори розподілених відкритих систем мають підтримувати політики безпеки та їхні рекомендації з управління безпекою ОІД. Об'єкти, що є предметом окремої політики безпеки, керовані окремим джерелом, іноді поєднують терміном *домен безпеки*. Домени безпеки можуть взаємодіяти один з одним.

8.3 Функції технологічного управління механізмами безпеки

Управління механізмами безпеки є головною частиною завдань технічної експлуатації механізмів безпеки. Послуги й механізми безпеки може бути активізовано управлінням об'єкта через інтерфейс управління та/чи через послугу звертання.

Управління ключами може включати:

- генерацію актуальних ключів з періодичністю, яка відповідає необхідному рівню безпеки;
- визначення, відповідно до вимог управління доступом, яким саме суб'єктам слід мати копію кожного ключа;
- створення у безпечний спосіб доступних чи розподілених ключів для суб'єктів у реальних відкритих системах.

Певні функції управління ключами мають виконуватись за межами середовища ОІД. Вони включають фізичний розподіл ключів довірчими засобами. Обмін робочими ключами для використання в перебігу взаємодії є

нормальною функцією мережного протоколу. Вибір робочих ключів може також бути здійснено шляхом доступу через протоколи управління до центру розподілу ключів.

Види управління ключами

Управління ключами застосовується за використання криптографічних алгоритмів. Управління ключами охоплює генерацію, розподіл (постачання) та контроль за криптографічними ключами. Вибір методу управління ключами залежить від учасників та оцінювання середовища, в якому ключі використовуватимуться. При розгляданні середовища враховують загрози внутрішнього й зовнішнього походження, проти яких треба захищати, застосовані технології, архітектурні структури, місця розташовування надаваних криптографічних послуг, а також фізичні структури й місця розташовування провайдерів криптографічних послуг.

Управління ключами здійснюється з урахуванням таких принципів, як:

- витримування життєвого циклу використання віднайденого явно чи неявно ключа. *Життєвий цикл* ключа обмежується часом чи іншими критеріями і включає в себе етапи генерації, розподілу, використання, архівування, вилучання та знищення;
- належна ідентифікація ключів згідно з їхніми функціями. Ключ має використовуватись лише для належних саме йому функцій. Приміром, ключі, призначені для послуг конфіденційності, не можуть використовуватися для послуг цілісності чи навпаки;
- організація поза ОІД служб фізичного постачання й архівація ключів.

Принципи управління ключами для симетричних алгоритмів включають:

- використання послуг конфіденційності в протоколі управління ключами для передавання ключів;
- використання ієрархії ключів. Мають враховуватися такі ситуації, як:
- “плоска” ієрархія ключів використовує лише ключі, які шифрують дані, явно чи неявно обрані з множини чинних ключів чи їхніх покажчиків;
- багаторівнева ієрархія ключів;
- ключі для шифрування ключів ніколи не повинні використовуватися для захисту даних, а ключі для шифрування даних ніколи не повинні використовуватися для захисту ключів, що їх шифрують;
- розподіл обов’язків у такий спосіб, що жодна особа не має повну копію важливого ключа.

Принципи управління ключами для асиметричних алгоритмів включають:

- використання послуг конфіденційності в протоколі управління ключами для передавання таємних ключів;
- використання послуг цілісності чи послуг захисту від невизнання участі (у процесі чи прийманні повідомлення) з доведенням походження в протоколі управління ключами для передавання відкритих ключів. Ці послуги може бути надано через використання симетричних та/чи асиметричних алгоритмів криптографії.

Управління шифруванням включає:

- взаємодію з управлінням ключами;

- установлення параметрів криптографії;
- синхронізацію криптографії.

Застосовування механізму шифрування потребує використання управління ключами і у правочинний спосіб інформації щодо алгоритмів криптографії.

Управління цифровим підписом. Цифровий підпис може включати:
- взаємодію з управлінням ключами;
- установлення параметрів та алгоритмів криптографії;
- використання протоколу поміж з'єднуваними об'єктами і можливою третьою стороною.

Як правило, управління цифровим підписом є строго подібно до управління шифруванням.

Управління контролем доступу може включати розподіл атрибутів безпеки, в тому числі паролі, чи відновлювання списків контролю доступу чи списків можливостей. Можуть також використовуватись протоколи, які забезпечують послуги управління доступом поміж взаємодіючими об'єктами.

Управління цілісністю даних може включати:
- взаємодію з управлінням ключами;
- установлення параметрів та алгоритмів криптографії;
- використання протоколу поміж взаємодіючими об'єктами.

Коли використовується техніка криптографії для цілісності даних, то управління цілісністю є строго подібне до управління шифруванням.

Управління автентифікуванням може включати розподіл поміж відповідними суб'єктами, які здійснюють автентифікування, описової інформації, паролів чи ключів, використовуючи управління ключами. Також може використовуватись протокол поміж взаємодіючими об'єктами й іншими об'єктами, які забезпечують послуги автентифікування.

Управління заповненням трафіка може включати технічне обслуговування засобів та правил, використовуваних для заповнення трафіка. Наприклад:
- попереднє визначення швидкості опрацювання чи передавання даних;
- визначення поточної швидкості передавання даних;
- визначення характеристик повідомлення, таких як довжина;
- змінення технічних вимог у відповідності з часом дня та/чи календарем.

Управління контролем маршрутизації може включати визначення каналів зв'язку чи під мереж, які мають бути чи безпечними чи довірчими, відповідно до притаманних критеріїв.

Управління нотаризацією може включати в себе:
- поширення інформації стосовно нотаріусів;
- використання протоколу поміж нотаріусом та об'єктами, що пов'язуються;
- взаємодію з нотаріусами.

Послуги й механізми безпеки можуть бути активовані управлінням об'єкта через інтерфейс управління та/чи звертанням до послуг.

Отже, архітектура безпеки в моделі взаємодії відкритих систем описує принципи, завдання та функції системи безпеки у найзагальнішому вигляді. Далі буде розглянуто більш детально особливості побудови системи безпеки інформаційних та телекомунікаційних систем з точки зору їхньої технічної експлуатації.

Контрольні запитання та завдання

1. Загальні принципи управління безпекою.
2. Які розрізнюють типи функцій управління безпекою?
3. Функції управління системою безпеки в цілому.
4. Функції управління послугами безпеки.
5. Функції управління механізмами безпеки.
6. Функції управління безпекою системи управління відкритої системи.
7. Функції специфічної системи управління безпекою діяльності.
8. Поясніть коротко особливості механізму управління ключами.

Завдання до самостійної роботи

Провести аналіз процедур управління послугами та механізмами захисту у ОІД типу телекомунікаційній мережі.

РОЗДІЛ 9

ПЛАНУВАННЯ ЗАХИСТУ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

9.1 Принципи управління інформаційною безпекою інформаційних систем

Управління інформаційною безпекою є важливою функцією технічної експлуатації і охоплює більшість її завдань. Гнучкість процесу планування інформаційних систем є необхідною умовою успішної їх роботи. Зважаючи на практичне значення цих питань для практичної роботи, ця частина підручника викладається у вигляді довідника функцій управління та механізмів управління, необхідних для більшості ситуацій. Не слід плутати механізми управління з механізмами захисту. Механізм управління – це засіб управління, а механізм захисту – це є, в даному разі, об'єкт управління. Мета інформаційної безпеки – забезпечувати безперебійну роботу підприємства і звести до мінімуму збитки від подій, які приховують загрозу безпеки, за допомогою їхнього запобігання і зведення наслідків до мінімуму.

Певні теоретичні положення й теореми щодо інформаційної безпеки залишаються таємними. Тому результати теоретичних досліджень та аналізування практики побудови систем інформаційної безпеки узвичаєно викладати у вигляді стандартів. Стандарти містять основні практичні правила, вичерпний набір засобів управління інформаційною безпекою та процедури забезпечування інформаційної безпеки. Стосовно управління інформаційною безпекою першим найбільш відомим є британський стандарт BS 7799 "Практичні правила управління інформаційною безпекою". Стандарт розроблено як керівництво й рекомендації. Набір засобів управління безпекою ґрунтується на реальних заходах захисту інформації. Здійснення положень стандарту має доручатись особам, які мають належну кваліфікацію й досвід роботи.

Управління інформаційною безпекою – це забезпечування механізмів, які дозволяють реалізовувати інформаційну безпеку. Управління забезпечує використання інформації, її захист та захист обчислювальних ресурсів. Нагадаємо, що інформаційна безпека полягає у зберіганні основних властивостей інформації за критеріями: конфіденційності, цілісності й доступності інформації.

Інформація зберігає конфіденційність в разі дотримування встановлених правил ознайомлення з нею, тобто її захищено від несанкціонованого розкривання чи перехоплення.

Інформація та інформаційні ресурси зберігають цілісність в разі дотримування встановлених правил її модифікування чи вилучання й забезпечування при цьому точності й повноти інформації та комп'ютерних програм.

Інформація й важливі для користувачів послуги зберігають доступність, якщо зберігається можливість ознайомлення чи модифікування інформації чи використання послуг відповідно до встановлених правил упродовж якого завгодно, порівняно малого, проміжку часу.

Управління інформаційною безпекою провадиться на усіх етапах життєвого циклу: планування, створення й експлуатації системи інформаційної безпеки.

Захисні заходи стають значно дешевшими й ефективнішими, якщо їх вмонтовано в інформаційні системи та послуги на стадіях завдання вимог і проектування. Згодом вживані заходи захисту інформаційних систем будуть ще більш дешевими й ефективними. На стадії розробляння метою процесу управління інформаційною безпекою є створення засобів захисту, які могли б ефективно протистояти ймовірним загрозам і забезпечували б надалі дотримання політики безпеки під час опрацювання інформації.

На стадії технічної експлуатації інформаційно-обчислювальної системи метою процесу управління інформаційною безпекою є оцінювання ефективності створеної системи захисту інформації й вироблення додаткових уточнюючих вимог для дороблянння системи захисту з метою забезпечування її адекватності за змінення умов функціонування: характеристик обчислювальної системи, опрацьовуваної інформації, фізичного середовища, персоналу, призначення системи, політики безпеки тощо.

Управління інформаційною безпекою базується на практичних правилах, котрі групуються в такі складові:

1. Загальні положення з управління інформаційною безпекою:

- політика безпеки;
- організація захисту;
- класифікація ресурсів та їхній контроль;

2. Безпека персоналу, фізична безпека й безпека навколишнього середовища;

3. Адміністрування комп'ютерних систем та обчислювальних мереж;

4. Управління доступом до систем;

5. Розроблення й супроводження інформаційних систем;

6. Планування захисту:

- планування безперебійної роботи підприємства;
- виконання вимог.

Завдання управління інформаційною безпекою розв'язуються із застосовуванням засобів контролю. Засоби контролю загального використання часто називають базовими засобами управління безпекою, оскільки всі вони в сукупності визначають базовий стандарт на підтримування режиму безпеки, зрозуміло, з урахуванням місцевих умов, обмежень, які накладені технологією й навколишнім середовищем.

За надто важливі вважаються десять *ключових* засобів контролю, які є обов'язковими вимогами чи основними структурними елементами інформаційної безпеки. Ключовими є такі засоби контролю:

- документ про політику інформаційної безпеки;

- розподіл обов’язків щодо забезпечування інформаційної безпеки;

- навчання й підготовка персоналу до підтримування режиму інформаційної безпеки;

- повідомлення про випадки порушування захисту чи інциденти в системі безпеки;

- засоби захисту від вірусів;

- процес планування безперебійної роботи підприємства;

- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;

- захист документації підприємства;

- захист даних;

- відповідність політиці безпеки.

Уточнимо об’єкт управління безпекою.

Є три групи основних вимог до інформаційної системи безпеки:

- набір ризиків порушування безпеки, котрий складається із загроз, яким піддаються інформаційні ресурси, їхніх слабостей і можливого впливу цих ризиків на роботу підприємства. Більшість ризиків та засобів протистояння ним описано в правилах. Однак існують ризики для кожного конкретного компонента системи, які потребують спеціальних заходів;

- набір правових та договірних вимог, яким має задовольняти підприємство, його партнери й постачальники послуг;

- набір принципів, цілей та вимог щодо опрацювання інформації, розроблений підприємством з виробничою метою.

Управління інформаційною безпекою має бути ефективним. Реалізація засобів управління безпекою в інформаційній інфраструктурі не повинна заважати виробничій діяльності. Витрати на систему захисту інформації слід привести у відповідність з цінністю інформації, яка захищається, й інших інформаційних ресурсів, підданих ризикові, а також зі збитками, що їх може бути нанесено підприємству через збої в системі захисту. Тому в процесі управління мають оцінюватись ризики порушування безпеки.

Оцінювання ризиків є необхідне для розробляння основної стратегії й вибору належних дій та пріоритетів для управління ризиками порушування інформаційної безпеки, а також для створення засобів контролю й оптимізації капіталовкладень у заходи для забезпечування інформаційної безпеки. Для оцінювання ризиків слід:

- визначати й аналізувати потенційні загрози, яким піддаються комп’ютерні системи, та їхні уразливості;

- розглядати збитки, котрі можуть нанести діяльності підприємства серйозне порушування інформаційної безпеки, з урахуванням можливих наслідків порушування конфіденційності, цілісності й доступності інформації;

- розглядати реальну ймовірність такого порушування захисту від суттєвих загроз за наявності засобів контролю.

Оцінка ризику залежить від таких чинників:

- характеру виробничої інформації та систем;

- виробничої мети, для якої інформація використовується;

- середовища, в якому система використовується й скеровується;
- захисту, забезпечуваного існуючими засобами контролю.

Успішне здійснення системи інформаційної безпеки визначається таким:
- забезпечування безпеки має ґрунтуватися на виробничих цілях і вимогах;
- функції управління безпекою має взяти на себе керівництво підприємства;
- оцінювання ризиків порушування безпеки, загроз і слабостей інформаційних ресурсів та рівня їхньої захищеності має ґрунтуватися на цінності й важливості цих ресурсів;
- ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;
- вивчання співробітниками політики та стандартів інформаційної безпеки;
- врахування конкретних інформаційних технологій, функцій підприємства та виробничого чи обчислювального середовища.

9.2 Загальні положення з управління інформаційною безпекою

Політика інформаційної безпеки. Політика інформаційної безпеки має сформулювати мету й забезпечувати підтримування інформаційної безпеки керівництвом підприємства за допомогою впровадження цієї політики серед співробітників підприємства. Письмовий документ про політику інформаційної безпеки має бути надано всім підрозділам підприємства і доступним для всіх співробітників, які відповідають за забезпечування режиму інформаційної безпеки. Документ має містити:

1. Визначення інформаційної безпеки, її мету й область застосовування;
2. Засоби здійснення цілей та принципів інформаційної безпеки;
3. Роз'яснення конкретних варіантів політики безпеки, принципів, стандартів та вимог щодо її дотримання, включаючи:
   - виконання правових та договірних вимог;
   - вимоги щодо навчання персоналу правилам безпеки;
   - політика попереджання й виявлення вірусів;
   - політика забезпечування безперебійної роботи підприємства;
4. Загальні й конкретні обов'язки щодо забезпечення режиму інформаційної безпеки;
5. Порядок повідомлення про події, які несуть загрозу безпеці.

Слід розробити процес перевіряння, визначати обов'язки і задати терміни перевірянь щодо дотримання вимог з політики безпеки.

Організація захисту та інфраструктура інформаційної безпеки. З метою ініціювати й контролювати процес забезпечування інформаційної безпеки на підприємстві створюється структура управління. Для ефективного розв'язання проблем доцільно запроваджувати комплексний підхід і організувати спільну роботу аудиторів, користувачів та адміністраторів. Також слід установити правила відносно розглядання випадків порушування захисту.

Відповідальність за забезпечування інформаційної безпеки, згідно з чинним законодавством, несе керівництво підприємства. На підприємстві мають провадитись регулярні наради щодо розробляння і впровадження політики безпеки, розподілу обов'язків щодо забезпечування захисту й координації дій з підтримування режиму безпеки. На таких нарадах мають розглядатися такі питання:

- аналізування й затвердження змінень політики інформаційної безпеки й розподіл загальних обов'язків;
- відстеження основних загроз, яким піддаються інформаційні ресурси;
- аналізування і спостерігання за інцидентами в системі безпеки;
- затвердження ініціатив, спрямованих на посилення захисту інформації.

Один з керівників має бути відповідальним за впровадження політики безпеки.

На великому підприємстві потрібне є координування *дій щодо захисту інформації*. Координування є стосовне:

- узгодження конкретних функцій та обов'язків посадових осіб щодо забезпечування інформаційної безпеки;
- узгодження конкретних методик та процесів захисту інформації, наприклад оцінювання ризиків, застосовуваних засобів захисту;
- узгодження й підтримування ініціатив щодо захисту інформації;
- залучення заходів захисту до процесу планування опрацювання інформації;
- координування дій здійснення конкретних заходів для забезпечування інформаційної безпеки нових систем чи послуг.

Політика інформаційної безпеки має давати загальні рекомендації з *розподілу функцій та обов'язків щодо захисту інформації*. Слід чітко визначати обов'язки щодо захисту окремих ресурсів і виконання конкретних процесів забезпечування безпеки. Призначаються відповідальні за конкретні ресурси, як фізичні, так й інформаційні, й за процеси забезпечування захисту, наприклад за планування безперебійної роботи підприємства.

Захист інформаційної системи, згідно із Законом України "Про інформацію", є обов'язком її власника. Власники інформаційних систем можуть делегувати свої повноваження із захисту окремим користувачам-адміністраторам чи постачальникам послуг. Проте власники все одно несуть відповідальність за забезпечування безпеки системи.

Аби уникати непорозумінь, важливо чітко визначати зони відповідальності кожного адміністратора й, зокрема, слід:

1. Ідентифікувати й чітко визначати різні ресурси і процеси забезпечування безпеки, пов'язані з кожною системою;
2. Погоджувати кандидатуру адміністратора, котрий відповідатиме за кожен ресурс чи процес забезпечування захисту, а його обов'язки задокументувати;
3. Чітко окреслювати й задокументувати рівні повноважень.

Процедура впровадження нових інформаційних систем має гарантувати, що встановлене устаткування забезпечує достатній рівень захисту й що воно

не справляє шкідливого впливу на безпеку наявної інфраструктури. Кожна модернізація систем має бути затверджена відповідним керівником та узгоджена з адміністратором, який відповідає за підтримування режиму локальної інформаційної безпеки. Це гарантує, що встановлені системи відповідатимуть вимогам з політики безпеки. Слід перевіряти, надто в мережному середовищі, що всі пристрої, приєднані до комунікаційних мереж, мають саме той тип, що його було затверджено.

Реальні процедури забезпечування інформаційної безпеки має бути піддане незалежному аналізові, аби бути упевненими, що використовувані підприємством процедури захисту відповідають ухваленій політиці безпеки, а також є реалізованими й ефективними.

Безпека доступу сторонніх організацій. Захист інформаційних систем підприємства може бути порушено через доступ, здійснюваний сторонніми організаціями, орендарями та іншими операторами зв'язку без належного контролю. Там, де доступ сторонніх організацій є необхідний з виробничих причин, провадять аналізування ризиків порушування захисту, визначають їхні наслідки й вимоги стосовно заходів для захисту інформації й засобів контролю.

При аналізуванні ризику беруть до уваги тип надаваного доступу, цінність інформації, вживані сторонньою організацією заходи захисту й наслідки від доступу для безпеки інформаційної інфраструктури підприємства.

Доступ сторонніх організацій до інформаційних ресурсів даного підприємства може бути дозволено лише після того, як вжито всіх необхідних захисних заходів і підписано договір, який визначає умови приєднання.

Угоди, які передбачають доступ сторонніх організацій до інформаційних ресурсів даного підприємства, мають ґрунтуватись на договорі, в котрому має бути перелічено всі необхідні умови безпеки, аби убезпечувати відповідність політиці і стандартам безпеки, прийнятими на підприємстві. Всі засоби контролю має бути погоджено й зазначено в договорі, укладеному зі сторонньою організацією. В договорі мають міститись правила й умови стосовно доступу. При укладанні контрактів розглядаються такі питання:

- загальна політика інформаційної безпеки;
- дозволені способи доступу, а також контроль і використання унікальних ідентифікаторів користувачів та паролів;
- опис кожного надаваної інформаційної послуги;
- вимога вести список осіб, яким дозволено використовувати послугу;
- час і дата, коли послуга буде доступною;
- плани дій у надзвичайних ситуаціях;
- процедури, стосовні захисту інформаційних ресурсів підприємства;
- право відстежувати дії користувачів;
- обов'язки з встановлення устаткування й програмного забезпечення та їхнього супроводження;
- право перевіряти договірні зобов'язання;
- обмеження на копіювання й розкривання інформації;

- заходи щодо забезпечування повернення чи знищення інформації й ресурсів після закінчення терміну чинності контракту;

- необхідні заходи для фізичного захисту;

- механізми для забезпечування здійснення захисних заходів;

- навчання користувачів методам, процедурам та правилам безпеки;

- заходи щодо забезпечування захисту від комп'ютерних вірусів;

- процедура надавання дозволу на доступ користувачів;

- процедури повідомлення про інциденти в системі безпеки та їхнього розслідування;

- участь сторонніх організацій, субпідрядників та інших учасників.

Класифікація ресурсів та їхній контроль. Всі основні інформаційні ресурси підлягають обліку і повинні мати призначеного відповідального за ресурси та здійснення відповідних захисних заходів. Відповідальність за ресурси дозволяє забезпечувати їхній належний захист.

Інвентаризація інформаційних ресурсів надає змогу переконатися, що забезпечується їхній ефективний захист, і вони можуть використовуватись для виробничих цілей. Кожен ресурс має бути чітко ідентифіковано, а його власник і категорія таємності погоджені й задокументовані. Приклади ресурсів:

- інформаційні ресурси: бази даних і файли даних, системна документація, інструкції користувача, навчальні матеріали, операційні процедури й процедури експлуатації, плани забезпечування безперебійної роботи підприємства, процедури переходу на аварійний режим;

- програмні ресурси: прикладне програмне забезпечення, системне програмне забезпечення, інструментальні засоби й утиліти;

- фізичні ресурси: комп'ютери й комунікаційне устаткування, магнітні носії даних, стрічки й диски, інше технічне устаткування, блоки живлення, кондиціонери, меблі, приміщення;

- послуги: обчислювальні й комунікаційні послуги, інші технічні послуги: опалення, освітлення, енергопостачання, кондиціонування повітря, сигналізації.

Класифікація інформації. Кожен різновид інформації має різний ступінь конфіденційності і важливості, притаманний для неї. Певні види інформації можуть мати необхідність додаткового захисту чи спеціального доступу. Категорії таємності й пов'язані з ними захисні засоби для виробничої інформації мають враховувати виробничу необхідність у використанні інформації чи обмежуванні доступу до неї, а також збитки для підприємства, спричинений несанкціонованим доступом чи ушкодженням інформації. Розглядають виробничу необхідність забезпечування таких заходів:

- конфіденційності: необхідність обмеження доступу до конфіденційної інформації й засобів, використовуваних для обмеження доступу до інформації;

- цілісності: необхідність здійснення контролю за внесенням змінень в інформацію й засоби, використовувані для забезпечування точності й повноти інформації;

- доступності: необхідність забезпечування доступу до інформації й потрібні для цього засоби контролю.

У цьому посібнику категорія таємності розглядається лише для

комерційної інформації. Відповідальність за надання категорії таємності документові, файлові даних чи дискеті, а також за періодичне перевіряння цієї категорії, покладають на особу, котра створила ці дані.

Надавання грифів таємності. Таємна інформація й вихідні дані систем, які підтримують таємну інформацію, мають відповідні грифи таємності. Часто інформація перестає бути конфіденційною через певний проміжок часу, наприклад коли вона стає загальнодоступною. Надмірне засекречування інформації може призвести до невиправданих додаткових витрат підприємства.

Вихідні дані інформаційних систем, які містять таємну інформацію, мають мати відповідний гриф таємності. Цей гриф має відбивати категорію таємності найбільш уразливої інформації у виведених даних. Прикладами таких вихідних даних є друковані звіти; інформація, виведена на екрани дисплеїв; дані, які зберігають на магнітних носіях, стрічках, дисках, касетах; електронні повідомлення й передані файли.

9.3 Фізична безпека й безпека навколишнього середовища

Для запобігання несанкціонованому доступові до інформаційних послуг, ушкодженню й створенню перешкод у їхній роботі утворюють захищені території. Інформаційні системи, які підтримують критично важливі чи вразливі послуги підприємства, має бути розміщено в захищених областях й захищено фізично від несанкціонованого доступу, ушкодження та перешкод. Захищена територія обмежується певним *фізичним периметром безпеки* й має належні контроль доступу до приміщень і захисні бар'єри.

Фізичний захист має ґрунтуватись на певних периметрах безпеки і забезпечуватися шляхом встановлення на підприємстві низки бар'єрів, розташованих у стратегічно важливих місцях. Вимоги до кожного захисного бар'єру і його місце розташування мають визначатися цінністю ресурсів та послуг, а також ризиками порушування безпеки й існуючих захисних заходів. Кожен рівень фізичного захисту має мати визначений периметр безпеки, в межах якого має бути забезпечено належний рівень захисту.

Для комп'ютерів та інших інформаційних ресурсів периметр безпеки може обмежувати область підвищеної безпеки: комп'ютерний зал, який замикається офіс, який замикається. Периметр безпеки може ґрунтуватися і на інших різновидах фізичних границь.

Пропоновані такі рекомендації:

- периметр безпеки має відповідати цінності захищених ресурсів та послуг;
- периметр безпеки має бути чітко окреслений;
- фізичні бар'єри мають за потреби простягатись від стелі до стелі, аби запобігти несанкціонованому доступові до приміщення;
- не слід без потреби надавати стороннім особам інформацію про те, що відбувається в захищених областях;

- можливе встановлення заборони на роботу поодинці без належного контролю. Це необхідно для безпеки праці й для запобігання зловмисним діям;

- комп'ютерне устаткування, яке належить підприємству, розміщують в спеціально призначених для цього місцях, окремо від устаткування, контрольованого сторонніми організаціями;

- у неробочий час захищені області мають бути фізично неприступні - замкнені й періодично перевірятися охороною;

- персоналові, який здійснює технічне обслуговування послуг, доступ до захищеної території надається лише в разі потреби й після одержання дозволу. За наявності конфіденційних даних дії такого персоналу відстежують;

- у межах периметра безпеки використання фотографічної, звукозаписувальної й відео апаратури має бути заборонено, за винятком санкціонованих випадків.

У захищених областях слід установити належний *контроль доступу до приміщення*, аби лише персонал, який має відповідні повноваження, мав до них доступ. Пропонується ввести такі засоби контролю:

- за відвідувачами захищених областей слід установити нагляд, а термін і час їхнього входу й виходу мають реєструватися. Відвідувачам має бути надано доступ до конкретних дозволених об'єктів;

- весь персонал, який працює в захищених областях, має носити на одязі добре помітні ідентифікаційні картки; окрім того, слід рекомендувати їм запитувати перепустку у незнайомих осіб;

- слід негайно вилучати права доступу до захищених областей у співробітників, котрі звільняються з даного місця роботи.

Центри даних та комп'ютерні зали, які підтримують критично важливі послуги підприємства, мають мати надійний фізичний захист. При виборі й облаштуванні відповідних приміщень слід брати до уваги можливість ушкодження устаткування внаслідок пожежі, повені, вибухів, громадських заворушень, інших аварій. Слід також розглядати загрози безпеці, можливі від сусідніх приміщень.

Слід розглядати такі заходи:

- розміщувати ключові системи якомога далі від загальнодоступних місць і місць руху суспільного транспорту;

- будівлі не повинні за можливістю привертати увагу і виявляти своє призначення. Не повинно бути явних ознак як зовні, так і всередині будинку, які свідчили б про присутність обчислювальних ресурсів;

- внутрішні телефонні довідники не повинні зазначати місцезнаходження обчислювальних ресурсів;

- небезпечні й легкозаймисті матеріали слід зберігати відповідно до інструкцій на безпечній відстані від місць розташовування обчислювальних ресурсів. Не слід зберігати витрачувані матеріали для комп'ютерів, наприклад папір для принтерів, у комп'ютерних залах;

- резервне устаткування й носії інформації, на яких зберігаються резервні копії, слід розміщувати на безпечній відстані, аби уникнути їхнього ушкодження в разі аварії чи стихійного лиха на основному робочому місці;

- слід встановлювати сертифіковане сигнальне й захисне устаткування, наприклад теплові й димові детектори, пожежну сигналізацію, засоби пожежегасіння, а також передбачати пожежну драбину. Сигнальне і захисне устаткування слід регулярно перевіряти відповідно до інструкцій виробників. Співробітники мають бути належним чином підготовлені до використання цього устаткування;

- процедури реагування на надзвичайні ситуації слід повністю задокументувати й регулярно тестувати;

- двері і вікна має бути замкнено, коли в приміщенні нікого немає. Слід розглядати можливість захисту вікон зовні.

Ізольовані місця розвантаження й завантаження устаткування та матеріалів. Комп'ютерні зали має бути захищено від несанкціонованого доступу. Рекомендовано надавати приміщення для розвантаження й завантаження матеріалів та устаткування для зменшення ймовірності несанкціонованого доступу до комп'ютерних залів. Вимоги щодо безпеки такого приміщення визначати, виходячи з оцінювання ризиків. Пропоновані такі рекомендації:

- доступ до складських приміщень ззовні будинку має надаватися лише перевіреному персоналові, який має відповідні повноваження;

- складське приміщення має бути так сплановано, аби матеріали можна було розвантажувати без одержання доступу до інших приміщень будівлі;

- зовнішні двері до складського приміщення має бути замкнено, коли відкрито внутрішні двері;

- слід установити, яку потенційну небезпеку являють собою матеріали, перш ніж їх переміщувати зі складського приміщення до місця призначення.

Наполегливо рекомендовано запровадити правила *використання робочих місць*, аби зменшити ризик несанкціонованого доступу, втрати й ушкодження інформації неробочого часу. Носії інформації, залишені на робочих столах, може бути ушкоджено чи знищено внаслідок аварії, пожежі, повені чи вибуху.

Пропоновані такі рекомендації:

- паперова документація і дискети, коли вони не використовуються, мають зберігатися в спеціальних шафах, особливо неробочого часу;

- конфіденційна чи критично важлива виробнича інформація, коли вона не використовується, має зберігатися окремо, найкраще у вогнетривкій шафі;

- персональні комп'ютери й комп'ютерні термінали, коли вони не використовуються, слід захищати за допомогою заблокування з ключем, паролів чи інших засобів контролю.

Співробітникам заборонено *виносити устаткування, дані та програми за межі підприємства* без письмового дозволу керівництва.

Захист устаткування. Устаткування захищають з метою запобігти втратам, ушкодженню й компрометації ресурсів та перебоям в роботі підприємства. Слід також приділити увагу проблемам *розміщення устаткування та його утилізації*. Устаткування інформаційних систем має бути так розміщено й фізично захищено, аби зменшити ризик впливу навколишнього середовища й несанкціонованого доступу. Пропоновані такі

рекомендації:

- устаткування розміщувати у такий спосіб, аби за можливістю звести до мінімуму зайвий доступ до робочих приміщень. Робочі станції, які підтримують конфіденційні дані, має бути розташовано так, аби вони були завжди на очах;

- доцільно розглянути можливість ізоляції областей, які потребують спеціального захисту, аби применшити необхідний рівень загального захисту;

- для ідентифікації можливих небезпек пропонується використовувати такий контрольний список: пожежа, задимлення, затоплення, запилення, вібрація, вплив хімічних речовин, перешкоди в електроживленні, електромагнітна радіація;

- забороняється прийняття їжі й паління в місцях розміщення комп'ютерів.

Устаткування слід захищати від збоїв у *системі електроживлення* й інших несправностей в електричній мережі. Джерело живлення має відповідати специфікаціям виробника устаткування.

Для устаткування, яке підтримує критично важливі виробничі послуги, рекомендовано встановлювати джерело безперебійного живлення. План дій у надзвичайних ситуаціях має включати заходи, яких слід вживати по закінченні терміну придатності джерел безперебійного живлення. Устаткування, що працює з джерелами безперебійного живлення, слід регулярно тестувати відповідно до рекомендацій виробника.

Захист кабельного розведення. Кабелі електроживлення й мережні кабелі для передавання даних слід захищати від їхнього несанкціонованого розкривання для цілей перехоплення інформації й ушкодження. Для зменшення цього ризику пропонується здійснювати таких захисних заходів:

- кабелі електроживлення й лінії зв'язку, котрі спрямовано до інформаційних систем, має бути проведено за можливістю під землею чи захищено у належний спосіб за допомогою інших засобів;

- слід користуватись екранами чи прокладати ці лінії у такий спосіб, аби вони не проходили через загальнодоступні місця.

Для винятково уразливих чи критично важливих систем можливе є уживання додаткових заходів, таких, як:

- шифрування даних;

- встановлення броньованих екранів і використання приміщень, котрі замикаються;

- використання інших маршрутів чи середовищ передавання даних.

Має здійснюватись належне *технічне обслуговування устаткування*, задля забезпечування його повсякчасної доступності й цілісності. Пропоновані такі рекомендації:

- технічне обслуговування устаткування має здійснюватися через проміжки часу, рекомендовані постачальником, і відповідно до інструкцій;

- ремонт і обслуговування устаткування має виконувати лише експлуатаційний персонал, котрий має відповідні повноваження;

- слід реєструвати всі несправності й збої.

Використання *устаткування інформаційних систем*, які підтримують

виробничі процеси, *за межами підприємства* має бути санкціоноване керівництвом; рівень захисту такого устаткування має бути таким самим, як і для устаткування, розташованого на території підприємства. Пропоновані такі рекомендації:

- співробітникам забороняється використовувати персональні комп'ютери для продовження роботи вдома, якщо не встановлено процедуру перевіряння на наявність вірусів;
- під час поїздок забороняється залишати устаткування та носії інформації в загальнодоступних місцях без догляду. Портативні комп'ютери слід провозити як ручний багаж;
- під час поїздок портативні комп'ютери є уразливі стосовно викрадань, втрати й несанкціонованого доступу. Для таких комп'ютерів слід забезпечувати належний захист доступу, аби запобігти НСД до інформації, яка в них зберігається;
- слід завжди дотримуватись інструкцій виробника, стосовних захисту устаткування, наприклад захисту устаткування від впливу потужних електромагнітних полів.

Ризики порушування безпеки, наприклад ушкодження, викрадання, перехоплення, можуть значно варіюватись від місця до місця.

Дані підприємства може бути скомпрометовано внаслідок недбалої *утилізації устаткування*. Перед утилізацією устаткування всі його компоненти, включаючи носії інформації, наприклад, тверді диски, слід перевіряти, аби гарантувати, що конфіденційні дані й ліцензоване програмне забезпечення було вилучено. Ушкоджені запам'ятовувальні пристрої, які містять надто важливі дані, слід оцінювати на ризик витікання даних та визначати, що з ними чинити: знищувати, ремонтувати чи позбутися них.

9.4 Адміністрування комп'ютерних систем і обчислювальних мереж

Рівень деталізації процедур, необхідних для адміністрування й забезпечування функціонування комп'ютерних систем та обчислювальних мереж, істотно змінюється залежно від розміру підприємства й типу устаткування, а також від характеру й уразливості виробничих застосувань.

З метою забезпечування коректної й надійної роботи комп'ютерних систем та обчислювальних мереж слід визначати обов'язки й процедури з адміністрування й забезпечування функціонування всіх комп'ютерів та мереж. Це має бути підкріплене відповідними робочими інструкціями й процедурами реагування на події. Для зменшення ризику недбалого чи несанкціонованого використання систем слід застосовувати принцип поділу обов'язків.

Має бути підготовлено *документовані операційні процедури* для всіх функціонуючих комп'ютерних систем для забезпечування їхньої коректної й надійної роботи. Документовані процедури готують також для:

- робіт, пов'язаних з розробляннням, супроводженням і тестуванням систем;

- робіт з обслуговування систем, пов’язаних з адмініструванням комп’ютерів та мереж, у тому числі процедур запускання й зупину комп’ютерів, резервного копіювання даних, технічного обслуговування устаткування, управління комп’ютерними залами й забезпечування їхнього захисту.

Процедури мають містити докладні коректні інструкції з виконання кожного завдання, у тому числі, з необхідності, такі пункти:

- коректне оперування з файлами даних;

- вимоги щодо планування виконання завдань, включаючи взаємозв’язок з іншими системами, а також час початку й закінчення виконання завдань;

- інструкції з опрацювання помилок та інших виняткових ситуацій, які можуть виникнути під час виконання завдань, у тому числі обмеження на використання системних утиліт;

- порядок звертання за допомогою до експлуатаційного персоналу у разі виникнення проблем, пов’язаних з експлуатацією комп’ютерних систем;

- спеціальні інструкції з оперування вихідними даними, такими, як використання спеціального паперу для друкувальних пристроїв, чи адміністрування конфіденційних вихідних даних, включаючи процедури надійного вилучання вихідної інформації від збійних завдань;

- процедури пере запускання й відновлювання працездатності систем, які використовують в разі відмови останніх.

Операційні процедури розглядаються як формальні документи, змінення до яких слід вносити лише після їхнього затвердження керівництвом, наділеним відповідними повноваженнями.

Серед завдань адміністрування найбільш складним є *мережне адміністрування*. Метою мережного адміністрування є забезпечування захисту інформації, які циркулює в мережах, й підтримуючої інфраструктури. Можливе також вживання спеціальних заходів для захисту конфіденційних даних, які передаються мережами загального користування. Мережні адміністратори мають визначати належні засоби контролю для забезпечування захисту даних, які циркулюють у мережах, і приєднаних до них систем від несанкціонованого доступу. Зокрема, слід враховувати таке:

- обов’язки із забезпечування роботи мереж та комп’ютерів має бути за потреби поділено;

- слід визначати обов’язки та процедури з управління віддаленим устаткуванням, у тому числі устаткуванням на робочих місцях користувачів;

- для забезпечування конфіденційності та цілісності даних, переданих мережами загального користування, і для захисту приєднаних до них систем потрібен вибір спеціальних засобів контролю;

- слід координувати роботи з адміністрування комп’ютерів та мереж як для оптимізації сервісу для виробничих застосувань, так і для забезпечування погодженого здійснення захисних заходів для всіх інформаційних послуг.

Процедури реагування на події. Для забезпечування вчасного, ефективного й зорганізованого реагування на події, які приховують загрози безпеці, слід визначати відповідні управлінські обов’язки й процедури.

Пропоновані такі рекомендації з вибору процедур реагування на події:

а) процедури мають містити в собі всі можливі типи інцидентів у системі безпеки, в тому числі:

- відмова систем і втрата послуг;
- помилки, які виникають від неповноти чи неточності виробничих даних;
- випадки порушування конфіденційності;

б) окрім звичайного плану дій в екстремальних ситуаціях, призначеного для того, аби щонайшвидше відновити працездатність систем та послуг, процедури мають містити в собі:

- аналізування і виявлення причини інциденту;
- планування й здійснення заходів для запобігання повторенню інциденту;
- ведення контрольного журналу реєстрування подій і збирання аналогічної інформації;
- взаємодію з користувачами й іншими особами, які постраждали від інциденту чи беруть участь у процесі відновлення систем;

в) ведення контрольного журналу реєстрування подій і збирання аналогічної інформації, необхідні задля:

- аналізування внутрішніх проблем;
- використання як засвідчення можливого порушування умов договору чи технічних нормативів;
- ведення переговорів з постачальниками програмних засобів та послуг;
- використання як доказу в разі судових розглядань, що підпадають під законодавство про несанкціоноване використання комп'ютерних систем та захисту даних;

г) здійснення ретельного і формального контролю за заходами з відновлення систем після порушування режиму безпеки, відмовлянь і збоїв. Процедури мають забезпечувати таке:

- надавання дозволу на доступ до робочих систем і даних лише персоналові, що має відповідні повноваження;
- докладне документування всіх заходів, вживаних у надзвичайних ситуаціях;
- доведення заходів, вживаних у надзвичайних ситуаціях, до відома керівництва та їхнє аналізування;
- відновлювання цілісності виробничих систем і засобів управління безпекою з мінімальною затримкою.

Поділ обов'язків чи зон відповідальності дозволяє звести ризик недбалого чи несанкціонованого використання систем до мінімуму і зменшити ймовірність несанкціонованого модифікування чи використання даних та послуг. Зокрема рекомендується, щоби виконання наведених нижче функцій не було доручено одним і тим самим співробітникам:

- використання виробничих систем;
- уведення даних;
- забезпечування функціонування комп'ютерів;
- мережне адміністрування;

- системне адміністрування;
- розробляння і супроводження систем;
- управління процесом внесення змінень;
- адміністрування засобів захисту;
- контроль (аудит) засобів захисту.

Поділ програмних засобів розробляння і робочих програм. Роботи, пов'язані з розробляннням і тестуванням систем, можуть призвести до ненавмисного внесення змінень у програми й дані чи несанкціонованого доступу до робочого програмного забезпечення й виробничих даних. Доцільно було б здійснювати поділ програмних засобів розробляння і робочих програм. Пропоновані такі засоби контролю:

- програмні засоби розробляння й робочі програми мають за можливістю запускатись на різних процесорах чи в різних директоріях/сегментах мережі;
- роботи з розробляння і тестування систем слід рознести настільки, наскільки це можливо;
- компілятори, редактори й інші системні утиліти не повинні зберігатися разом з робочими системами, якщо в цьому немає потреби;
- задля зменшення ризику плутанини, слід використовувати різні процедури входження до робочих та тестованих систем. Потрібне використання різних паролів для входження до цих систем, а система меню має виводити на екран відповідні ідентифікаційні повідомлення.

Залучення підрядника з боку до адміністрування комп'ютерних мереж може призвести до додаткового ризику порушування режиму безпеки, наприклад, до можливості компрометації, ушкодження чи втрати даних в організації підрядника. Слід завчасно виявити такий ризик і включити до договору належні захисні заходи для його зменшення, погоджені з підрядником.

Практичні правила є хорошою відправною базою для задавання, узгодження й перевіряння дотримання стандартів безпеки. Слід розглянути такі питання:

- необхідність ідентифікації особливо уразливих чи критично важливих застосувань, винесення яких за межі підприємства є небажане;
- необхідність одержання санкції на використання виробничих застосувань від їхніх власників;
- наслідки для планів забезпечування безперебійної роботи підприємства;
- стандарти безпеки, які підлягають визначенню, і процес перевіряння щодо їхнього дотримання;
- обов'язки та процедури з повідомлення про інциденти в системі безпеки й реагування на них.

Планування роботи систем. Для забезпечування доступності ресурсів і належної навантажувальної здатності систем, потрібні є завчасне планування й підготовка.

Аби зменшити ризик перевантаження систем, забезпечувати належну продуктивність комп'ютерів та обсяг запам'ятовувальних пристроїв, слід оцінити навантажувальну здатність на підставі прогнозу. Аби уникнути відмов

систем унаслідок їхньої недостатньої навантажувальної здатності, слід постійно стежити за їхнім *навантаженням*. Експлуатаційні вимоги щодо нових систем слід визначати, задокументувати й перевіряти до їхнього приймання. Вимоги щодо переходу до аварійного режиму для послуг, які підтримують численні застосування, має бути погоджено і регулярно переглядатися.

Адміністратори систем мають постійно стежити за використанням ключових системних ресурсів, включаючи процесори, головну оперативну пам'ять, файлові запам'ятовувальні пристрої, принтери й інші пристрої, а також комунікаційні системи. Адміністратори комп'ютерів та мереж мають використовувати цю інформацію для виявляння потенційно вузьких місць, які можуть являти загрозу системі безпеки чи послугам користувачів, і планування належних заходів для виправляння ситуації.

Слід задати критерії *приймання нових систем* і провести відповідні випробування до їхнього приймання. Адміністратори комп'ютерів мають чітко визначати, погоджувати, задокументувати і перевіряти вимоги й критерії приймання нових комп'ютерних систем. Пропоноване розглянути таке:

- вимоги щодо продуктивності й навантажувальної здатності комп'ютерів;
- підготовку процедур відновлювання й пере запускання систем після збоїв, а також планів дій в екстремальних ситуаціях;
- підготовку й тестування повсякденних операційних процедур відповідно до заданих стандартів;
- перевіряння того, що встановлення нової системи не матиме згубних наслідків для функціонуючих систем, надто в періоди пікового навантаження на процесори, наприклад, наприкінці місяця;
- підготовку персоналу до використовування нових систем.

Для потвердження цілковитої відповідності всім критеріям приймання систем, слід провести відповідні випробування.

Планування переходу на аварійний режим. Аварійне резервне устаткування надає можливість тимчасового продовження опрацювання даних у разі ушкодження чи відмовляння головного устаткування. Адміністратори комп'ютерів і мереж мають підготувати відповідний план переходу на аварійний режим для кожного інформаційного сервісу.

Вимоги щодо переходу до аварійного режиму для окремих систем має бути задано власниками виробничих застосувань виходячи з процесу планування безперебійної роботи підприємства. Постачальники послуг мають погодити вимоги щодо переходу на аварійний режим для колективно використовуваних послуг і скласти відповідний план переходу на нього для кожного з них.

Аварійне резервне устаткування й процедури переходу на аварійний режим слід регулярно тестувати.

Недостатній *контроль за процесом внесення змінень до робочих інформаційних систем* є поширеною причиною їхніх відмов і порушування режиму безпеки. Слід визначати формальні управлінські процедури й обов'язки для забезпечування задовільного контролю за внесенням усіх змінень в

устаткування, програми й процедури. Зокрема, слід розглянути такі пункти:

- виявлення й реєстрування істотних змінень
- оцінювання можливих наслідків від таких змінень;
- процедура затверджування пропонованих змінень;
- доведення деталей пропонованих змінень до відома всіх причетних осіб;
- процедури й обов'язки з ліквідації невдалих змінень та відновлення систем після їхнього внесення.

Для забезпечування цілісності даних та програм важливі є заходи щодо *запобігання й виявлення* випадків упровадження *шкідливого програмного забезпечення.* Існує ціла низка шкідливих методів, які дозволяють використовувати уразливість комп'ютерних програм стосовно їхнього несанкціонованого модифікування. Це так звані комп'ютерні "віруси", мережні "черви", "троянські коні", логічні "бомби". Адміністратори інформаційних систем мають бути завжди напоготові щодо небезпеки проникнення шкідливого програмного забезпечення до систем й за потреби вживати спеціальних заходів із запобігання чи виявлення його впровадження. Детально ці питання розглянуто у розділі 7.

Оператори комп'ютерів мають вести *журнал реєстрування подій,* де зафіксовувати усі виконувані завдання. Цей журнал має за потреби включати:

- час запускання й зупинення систем;
- потвердження коректного оперування з файлами даних і вихідною інформацією від комп'ютерів.

Журнали реєстрування подій мають регулярно звірятися з операційними процедурами.

Слід вести *реєстрування збоїв,* сповіщати про збої в роботі систем і відразу розпочинати відповідні коригувальні заходи. Зафіксовані користувачами збої, стосовні проблем з комп'ютерними й комунікаційними системами, слід заносити до журналу реєстрування. Мають існувати чіткі правила опрацювання зареєстрованих збоїв, включаючи такі:

- аналізування журналу реєстрування збоїв для забезпечування їхнього усунення;
- аналізування коригувальних заходів, мета яких полягає в перевірянні того, чи не скомпрометовано засоби управління безпекою й чи є заходи санкціонованими.

Для визначення умов, які можуть несприятливо позначитися на роботі комп'ютерного устаткування і для вживання коригувальних заходів, необхідне є невпинне *спостерігання за навколишнім середовищем*, у тому числі за вологістю, температурою та якістю джерел електроживлення. Такі процедури слід реалізовувати відповідно до рекомендацій постачальників.

Процедури робочого, архівного та резервного копіювання. Заходи з *обслуговування систем* потрібні для підтримування цілісності й доступності сервісу. Слід визначати повсякденні процедури для знімання резервних копій з даних, реєстрування подій та збоїв, а також для спостерігання за середовищем, у якому функціонує устаткування. Треба контролювати комп'ютерні носії даних і забезпечувати їхній фізичний захист, аби запобігти ушкодженням

інформаційних ресурсів та перебоям в роботі підприємства.

Для забезпечування можливості відновлювання всіх критично важливих виробничих даних і програм після виходу з ладу комп'ютера чи відмовляння носія інформації, слід мати належні засоби *резервного копіювання даних.* Резервні копії з критично важливих виробничих даних і програм мають зніматися регулярно. Процедури резервного копіювання мають задовольняти вимогам планів забезпечування безперебійної роботи підприємства. Пропоновані такі рекомендації:

1 мінімальну дубльовану інформацію разом з точними і повними записами про резервні копії зберігають у віддаленому місці на достатній відстані для того, аби уникнути наслідків від аварії на головному робочому місці. Слід створити принаймні три покоління резервних копій даних для важливих виробничих застосувань;

2 резервні копії має бути у належний спосіб захищено фізично від впливу навколишнього середовища у відповідності зі стандартами, прийнятими на головному робочому місці. Засоби захисту носіїв інформації, чинні на головному робочому місці, поширюють на місце зберігання резервних копій;

3 резервні дані слід регулярно тестувати, аби бути упевнений, що на них можна буде покластися у разі аварії.

Власники даних мають задати період схоронності критично важливих виробничих даних, а також вимоги щодо сталого зберігання архівних копій.

Слід визначати належні операційні процедури для захисту комп'ютерних носіїв інформації, магнітних стрічок, дисків, касет, даних та системної документації від ушкодження, викрадання й несанкціонованого доступу.

Для управління знімними комп'ютерними носіями інформації, такими як магнітні стрічки, диски, касети й роздруківки, треба мати відповідні процедури. Пропоновані такі засоби контролю в робочому середовищі:

- застосовування системи зберігання даних, у якій забороняється використовувати описові позначки, аби за позначками не можна було визначати, які саме дані зберігаються на запам'ятовувальному пристрої;

- стирання попереднього вмісту повторно використовуваних носіїв інформації, котрі підлягають вилученню, якщо вони більш не є потрібні. Одержання письмової санкції на вилучання носіїв інформації з організації й реєстрування усіх випадків їхнього вилучання в контрольному журналі;

- зберігання всіх носіїв інформації в надійному, захищеному середовищі відповідно до інструкцій виробників.

Усі процедури й рівні повноважень має бути чітко задокументовано.

Щоб захищати конфіденційні дані від несанкціонованого розкривання чи використання, слід визначати *процедури безпечного оперування з даними* та усіма носіями вхідних і вихідних конфіденційних даних, наприклад документів, телексів, магнітних стрічок, дисків, звітів, рахунків тощо. Пропоноване розглянути такі пункти:

- оперування з носіями вхідної й вихідної інформації й їхнє маркування;

- реєстрування одержувачів даних, котрі мають відповідні повноваження;

- забезпечування повноти вхідних даних;

- потвердження одержання переданих даних (за потреби);
- надавання доступу до даних мінімальній кількості осіб;
- чітке маркування всіх копій даних для одержувача, котрий має відповідні повноваження;
- перевіряння списків одержувачів з правом доступу до даних через регулярні проміжки часу.

Системна документація може містити конфіденційну інформацію, наприклад опис прикладних процесів, процедур, структури даних та процесів потвердження повноважень. Для *захисту системної документації* від несанкціонованого доступу застосовують такі засоби контролю:
- системна документація має зберігатись замкненою в надійних шафах;
- список осіб з правом доступу до системної документації має бути максимально обмежено, а дозвіл на її використання має видаватись власником застосування;
- документацію, створювану комп'ютерами, треба зберігати окремо від інших файлів застосувань, і їй слід надати належного рівня захисту доступу.

Конфіденційна інформація може просочитися за межі підприємства і потрапити до осіб, які не мають відповідних прав, унаслідок недбалого вилучання комп'ютерних носіїв даних. Для *вилучання більш не потрібних носіїв даних* слід використовувати чіткі, надійні і перевірені процедури. Носії даних, які містять конфіденційну інформацію, слід надійно знищувати, наприклад спалюючи їх чи подрібнюючи, або очищувати від даних для іншого їх використання усередині підприємства.

Для ідентифікації носіїв даних, котрі можуть мати потребу надійного вилучання, пропоноване використовувати такий контрольний список: вхідна документація, наприклад телекси; копіювальний папір; вихідні звіти; одноразові стрічки для принтерів; магнітні стрічки; знімні диски чи касети; роздруківки програм; протестовані дані; системна документація.

Кожен випадок вилучання носіїв конфіденційної інформації слід, за можливості, реєструвати в контрольному журналі для майбутніх довідок.

За нагромадження інформації, котра підлягає вилучанню, слід враховувати ефект акумуляції. Може статись, що велика кількість нетаємної інформації стає більш конфіденційною, ніж мала кількість таємної інформації.

З метою запобігання втраті, модифікуванню і несанкціонованому використанню даних *обмін даними й програмами* поміж організаціями треба контролювати. Такі обміни слід здійснювати на підставі офіційних угод. Має бути встановлено процедури та стандарти для захисту носіїв інформації під час їхнього транспортування. Слід враховувати наслідки для виробничої діяльності й системи безпеки від використання електронного обміну даними й повідомленнями електронної пошти.

Поміж організаціями має бути укладено *офіційні угоди про обмін даними* й програмами – електронний чи за допомогою кур'єрів, – у тому числі, угоди про зберігання програмного забезпечення. В угодах має бути задано належні умови безпеки, включаючи таке:

- обов’язки з контролю й повідомлення про передавання й одержання даних;
- процедури повідомлення про передавання й одержання даних;
- мінімум технічних стандартів за форматами передавання інформації;
- стандарти з ідентифікації кур’єрів;
- обов’язки та зобов’язання у разі втрати даних;
- права власності на дані й програми, а також обов’язки із захисту даних, дотримання авторських прав на програмне забезпечення тощо;
- технічні стандарти на записування й читання даних та програм;
- спеціальні заходи щодо захисту надто важливих даних, таких, як криптографічні ключі.

Комп’ютерні носії даних можуть бути уразливі стосовно несанкціонованого доступу, використання й ушкодження під час транспортування. *Для захисту носіїв інформації під час транспортування* з однієї організації в іншу, пропоновані такі засоби контролю:
- використання надійних кур’єрів та транспорту. Узгодження переліку кур’єрів, наділених відповідними повноваженнями, з керівництвом і здійснення процедури ідентифікації кур’єрів;
- забезпечування належного захисту вмісту пакетів від можливого фізичного ушкодження під час транспортування відповідно до інструкцій виробників;
- уживання спеціальних заходів (за потреби) для захисту конфіденційної інформації від несанкціонованого розкривання чи модифікування.

Приклади:
- використовування контейнерів закритого типу;
- доставляння за допомогою кур’єрів;
- упаковування, захищене від стороннього втручання, яке дозволяло б виявляти спроби її розкривання;
- як виняток, поділ вантажу на частини й їхнє надсилання різними маршрутами.

Для *захисту електронного обміну даними* (ЕОД) застосовують за потреби спеціальні засоби управління безпекою, оскільки ЕОД з партнерами є уразливий стосовно несанкціонованого перехоплення й модифікування. Окрім того, можливо буде потрібно потвердження щодо передавання чи одержання даних. Слід також подбати про захист приєднаних до мережі комп’ютерних систем від загроз, які випливають з електронного приєднання.

Засоби управління безпекою операцій з ЕОД має бути погоджено з партнерами й постачальниками мережних послуг.

Захист електронної пошти. Електронна пошта все частіше використовується для передавання інформації поміж організаціями, витісняючи традиційні види зв’язку, такі, як телекси і листи. Електронна пошта відрізняється від традиційних видів зв’язку швидкістю, структурою повідомлень, ступенем формальності й уразливістю стосовно перехоплення. Для зменшення ризику, якому піддаються виробничі процеси й система безпеки, пов’язаного із застосовуванням електронної пошти, слід

використовувати належні засоби контролю. Пропоноване розглянути такі пункти:

- уразливість електронних повідомлень стосовно несанкціонованого перехоплення й модифікування;
- уразливість даних, які надсилаються електронною поштою, стосовно помилок, наприклад хибна адресація чи спрямовування повідомлень не за призначенням, а також надійність і доступність сервісу в цілому;
- вплив змінення характеристик комунікаційного середовища на виробничі процеси, наприклад, вплив підвищеної швидкості передавання даних чи змінення системи адресації;
- правові положення, такі, як необхідність перевіряння джерела повідомлень;
- наслідки для системи безпеки від розкривання вмісту каталогів;
- необхідність уживання захисних заходів для контролю віддаленого доступу користувачів до електронної пошти.

Підприємства мають задавати чіткі правила, стосовні статусу й використання електронної пошти.

Захист систем електронного офісу. Системи електронного офісу надають можливість більш швидкого поширення й колективного використання виробничої інформації. Для контролю ризику, якому піддаються виробничі процеси й система безпеки, пов’язані з використанням електронного офісу, потрібні чіткі правила. Пропоноване розглянути такі пункти:

- необхідність вилучання певних категорій конфіденційної виробничої інформації, наприклад, таємної інформації, в разі, якщо система безпеки не забезпечує належного рівня захисту;
- необхідність визначання чітких правил та засобів контролю для адміністрування колективно використовуваної інформації, наприклад, використання корпоративних електронних дошок оголошень;
- необхідність обмежування доступу до персональної інформації стосовно окремих осіб, наприклад персоналу, котрий працює над конфіденційними проектами;
- придатність системи для підтримування виробничих застосувань;
- категорії персоналу й підрядників чи партнерів, яким дозволено використовувати систему й місця, з яких можна одержати доступ до неї;
- необхідність обмеження доступу конкретним категоріям користувачів;
- необхідність зазначення статусу користувачів, наприклад співробітників підприємства чи підрядників, у каталогах до відома інших користувачів;
- правила, стосовні періоду схоронності й резервного копіювання інформації, що зберігається в системі;
- вимоги й процедури переходу до аварійного режиму.

9.5 Управління доступом до систем. Розробляння і супроводження інформаційних систем

Виробничі вимоги щодо управління доступом до систем. Доступ до комп'ютерних систем і даних слід контролювати виходячи з виробничих вимог. Такий контроль має враховувати правила поширення інформації й розмежовування доступу, ухвалених на підприємстві. Виробничі вимоги щодо управління доступом до систем слід визначати і задокументувати. Кожен власник виробничого застосування має чітко сформулювати політику контролю доступу до даних, яка визначатиме права доступу кожного користувача чи групи користувачів. Ця політика має враховувати таке:

- вимоги щодо безпеки окремих виробничих застосувань;
- правила поширення інформації й розмежовування доступу.

Корисно розглядати можливість створення стандартних профілів повноважень доступу користувачів для загальних категорій робіт.

Мета *управління доступом користувачів* полягає у запобіганні несанкціонованому доступові до комп'ютерних систем. Для управління процесом надавання прав доступу до інформаційних систем потрібні формальні процедури. Ці процедури мають містити в собі всі стадії життєвого циклу управління доступом користувачів – від початкового реєстрування нових користувачів до вилучання облікових записів користувачів, котрі більше не мають потреби в доступі до інформаційних послуг. Особливу увагу слід приділити необхідності управління процесом надавання привілейованих прав доступу, які дозволятимуть користувачам оминати засоби системного контролю.

Докладно вимоги та рекомендації до побудови процедур управління доступом приведені у розділі 8.

Розробляння і супроводження інформаційних систем. Для забезпечення змонтованості засобів захисту до інформаційних систем, *вимоги щодо безпеки систем* має бути визначено й погоджено до розробляння інформаційних систем.

Засоби захисту стають значно дешевшими й ефективнішими, якщо їх вмонтовувати до прикладних систем на стадіях задавання вимог та проектування. Усі вимоги щодо безпеки, включаючи необхідність переходу до аварійного режиму для продовження опрацювання інформації, визначають на стадії задавання вимог до проектів. Слід також обґрунтовувати, погоджувати й задокументувати їх у рамках загального плану робіт зі створення інформаційної системи.

Аналізування і задавання вимог щодо безпеки слід провадити на стадії аналізування вимог щодо кожного проекту розробляння систем. При формулюванні виробничих вимог до нових систем чи модернізування існуючих систем слід задавати вимоги й до засобів управління безпекою. Такі вимоги зазвичай зосереджено на автоматичних засобах контролю, вбудованих у системи, однак слід також розглянути необхідність використання допоміжних та ручних засобів управління безпекою. Вимоги до безпеки й засобів

управління нею мають відбивати цінність інформаційних ресурсів для підприємства, а також можливі наслідки від порушування режиму безпеки чи відсутності засобів захисту для виробничих процесів. Підґрунтя аналізу вимог щодо безпеки становлять:

- розглядання необхідності забезпечування конфіденційності, цілісності й доступності інформаційних ресурсів;
- визначення можливостей використання різних засобів контролю для запобігання й виявлення випадків порушування захисту, а також відновлення працездатності систем після виходу з ладу й інцидентів у системі безпеки.

Зокрема при проведенні такого аналізування слід розглядати необхідність:

- управління доступом до інформації й послуг, включаючи вимоги щодо поділу обов'язків та ресурсів;
- реєстрування значущих подій у контрольному журналі для цілей поточного контролю чи спеціальних розслідувань;
- перевіряння і забезпечування цілісності життєво важливих даних на всіх чи обраних стадіях їхнього опрацювання;
- захисту конфіденційних даних від несанкціонованого розкривання, у тому числі використання засобів шифрування даних у спеціальних випадках;
- виконування вимог інструкцій та чинного законодавства, а також договірних вимог;
- знімання резервних копій з критично важливих виробничих даних;
- відновлення систем після їхніх відмовлянь, надто для систем з підвищеними вимогами щодо доступності. Процедури переходу до аварійного режиму слід визначати на стадії задавання вимог;
- захисту систем від внесення несанкціонованих доповнень та змінень;
- надавання можливості безпечного управління системами та їхнє використання співробітниками, які не є фахівцями, але мають належну підготовку;
- забезпечування відповідності систем вимогам аудиторів, наприклад за допомогою використання таких засобів, як убудовані утиліти, програми-утиліти для вибіркового контролю й незалежне програмне забезпечення для повторення критично важливих обчислень.

Засоби управління безпекою, вмонтовані в комп'ютерні системи, може бути скомпрометовано, якщо обслуговуючий персонал і користувачі не будуть обізнані щодо них. Тому слід чітко визначати ці засоби контролю в документації.

Безпека в прикладних системах. Мета безпеки полягає у запобіганні втраті, модифікуванню і несанкціонованому використанню даних користувача в прикладних системах. При проектуванні прикладних систем слід вмонтовувати до них належні засоби управління безпекою, у тому числі засоби реєстрування подій у контрольному журналі. Проектування й експлуатація систем мають відповідати загальноприйнятим промисловим стандартам забезпечування надійного захисту, визначеним у практичних правилах та законодавстві.

Системи, котрі підтримують чи впливають на винятково уразливі, дорогі

чи критично важливі інформаційні ресурси підприємства, можуть потребувати уживання додаткових заходів протидії. Такі заходи слід визначати виходячи з рекомендацій фахівця з безпеки з урахуванням ідентифікованих загроз порушування захисту й можливих наслідків від їхнього здійснення для підприємства.

Задля забезпечення правильного введення даних до прикладних систем, необхідне *перевіряння вірогідності вхідних даних*. Пропоновані такі засоби контролю:

а) перевіряння з метою виявлення таких помилок, як

- величини, що виходять за задані межі;
- помилкові символи в полях даних;
- пропущені чи неповні дані;
- перевищені верхні й нижні границі щодо обсягу даних, які вводяться;
- несанкціоновані чи суперечливі управляючі дані;

б) періодичне аналізування змісту ключових полів чи файлів даних для потвердження їхньої вірогідності й цілісності;

в) оглядання друкованої вхідної документації на предмет внесення несанкціонованих змінень у вхідних даних (слід одержати дозвіл на внесення всіх змінень до вхідних документів);

г) процедури реагування на помилки, пов’язані з перевірянням вірогідності вхідних даних;

д) визначання обов’язків усіх співробітників, які беруть участь у процесі введення даних.

Перевіряння вірогідності внутрішнього опрацювання даних. Дані, які було правильно введено до прикладної системи, може бути ушкоджено внаслідок помилок опрацювання чи навмисних дій. Аби виявити такі випадки ушкодження даних, слід вмонтовувати засоби перевіряння до систем. Необхідні для цього засоби контролю визначаються характером застосовування й наслідками від ушкодження даних для підприємства. Прикладами вмонтованих засобів перевіряння є:

а) контроль сеансу зв’язку і пакетного опрацювання для узгодження файлів даних про платіжний баланс після проведення операцій з ними;

б) контроль платіжного балансу для звіряння початкового сальдо з попереднім кінцевим сальдо:

- контроль за виконанням операцій;
- підведення підсумків з відновлення файлів;
- контроль за виконанням програм;

в) перевіряння вірогідності даних, генерованих системою;

г) перевіряння цілісності даних та програм, які надсилаються поміж центральним та віддаленим комп’ютерами;

д) підведення підсумків з відновлення файлів.

Для конфіденційних даних, які потребують спеціального захисту, слід розглянути можливість *шифрування даних*. Шифрування – це процес перетворення інформації на зашифрований текст для забезпечування її конфіденційності й цілісності під час передавання чи при зберіганні. У цьому

процесі використовуються алгоритм шифрування й інформація про таємні ключі, відома лише зареєстрованим користувачам. Шифрування може потребуватися для захисту конфіденційної інформації, що є уразлива стосовно несанкціонованого доступу, як під час її передавання, так і при зберіганні. Для визначення необхідності шифрування даних і необхідного рівня захищеності слід провести оцінювання ризику. Згідно з чинним законодавством України, криптографічний захист є власністю держави, яка потребує твердого державного контролю над експортуванням, імпортуванням, використанням і передаванням програмних продуктів, котрі підтримують функцію шифрування.

Автентифікація повідомлень — це метод, який використовується для виявлення несанкціонованих змінень, які вносяться до переданих електронних повідомлень, чи їхнього ушкодження. Його можна реалізовувати на апаратному чи програмному рівні за допомогою фізичного пристрою автентифікування повідомлень чи програмного алгоритму. Можливість автентифікування повідомлень слід розглядувати для тих застосувань, для яких життєво важливим є забезпечування цілісності повідомлень. Для визначення необхідності автентифікування повідомлень і вибору найбільш придатного методу її здійснення слід виконати оцінювання ризику порушування режиму безпеки.

Автентифікування повідомлень не призначене для захисту вмісту повідомлень від перехоплення. Для цих цілей придатне зашифровування даних, яке можна також використовувати для автентифікування повідомлень.

Електронний підпис — це спеціальний різновид автентифікування повідомлень, який ґрунтується на методах шифрування з відкритим ключем, який забезпечує автентифікування відправника, а також гарантує цілісність вмісту повідомлення.

Захист файлів прикладних систем. Задля забезпечування надійного здійснення проектів розробляння інформаційних систем та їхньої експлуатації доступ до системних файлів слід контролювати. Підтримування цілісності прикладних систем має бути обов’язком користувача чи групи розробляння, який прикладна система чи програмне забезпечення належать.

Треба здійснювати твердий *контроль за експлуатуванням робочого програмного забезпечення*. Задля зведення ризику ушкодження робочих систем до мінімуму, слід зреалізувати вже згадувані засоби контролю:

- відновлення робочих бібліотек програм має здійснювати лише призначений бібліотекар після одержання санкції на доступ до застосування від керівника персоналу, котрий обслуговує інформаційні системи;
- у робочих системах зберігають лише виконувані програми;
- виконувані програми не слід запускати на робочих системах доти, поки вони не пройдуть тестування й їх не буде прийнято користувачами, а відповідні бібліотеки вихідних текстів програм не буде обновлене;
- слід фіксувати усі випадки відновлення робочих бібліотек програм у контрольному журналі;
- попередні версії програм слід зберігати – це запобіжний захід за надзвичайних ситуацій.

Захист системних тестових даних. Тестування систем та їхнє приймання потребують значних обсягів тестових даних, близьких до реальних даних настільки, наскільки це є можливо. Тестові дані слід захищати й контролювати. Слід уникати використання реальних баз даних, котрі містять персональні дані. Перш ніж використовувати такі дані, їх слід знеособити. Для захисту реальних даних при їхньому використанні для цілей тестування пропоновані такі засоби контролю:

- процедури управління доступом, застосовані для робочих систем, мають також застосовуватися для тестованих прикладних систем;
- слід одержувати окремий дозвіл кожного разу, коли реальні дані копіюються в тестовану прикладну систему;
- реальні дані слід вилучати з тестованої прикладної системи відразу ж після завершення процесу тестування;
- випадки копіювання реальних даних слід зареєструвати в контрольному журналі.

Для забезпечування захисту прикладного програмного забезпечення та даних контролюють *безпеку в середовищі розробляння та робочому середовищі*.

Адміністратори, які відповідають за прикладні системи, мають також відповідати за захист середовища розробляння й робочого середовища. Вони мають аналізувати всі змінення, що їх пропоноване внести до системи, аби гарантувати, що вони не порушать безпеку системи чи робочого середовища.

Задля зведення ризику ушкодження інформаційних систем до мінімуму, слід здійснювати твердий контроль за внесенням змінень до них й розробляти *процедури управління процесом внесення змінень*. Ці процедури мають гарантувати, що безпека та процедури управління нею не буде скомпрометовано, що програмістам, які відповідають за експлуатацію систем, надано доступ лише до компонентів системи, необхідних для їхньої роботи, й що отримано формальний дозвіл на внесення змінень. Такий процес має містити в собі таке:

а) реєстрування погоджених рівнів повноважень, у тому числі:

- служби приймання запитів на внесення змінень групою, яка обслуговує інформаційні системи;
- повноваження користувачів на подавання запитів на внесення змінень;
- рівні повноважень користувачів на приймання докладних пропозицій;
- повноваження користувачів на приймання внесених змінень;

б) приймання змінень, пропонованих лише зареєстрованими користувачами;

в) перевіряння засобів управління безпекою та процедур забезпечування цілісності на предмет їхньої компрометації внесеними зміненнями;

г) виявляння всіх комп’ютерних програм, файлів даних, баз даних та апаратних засобів, котрі потребують внесення виправлянь;

д) затверджування наданих пропозицій до початку роботи;

е) забезпечування приймання пропонованих змінень зареєстрованими користувачами до їхнього внесення;

ж) відновлення системної документації після завершення процесу

внесення кожного змінення, а також архівація чи знищення старої документації;

з) здійснення контролю над версіями всіх оновлених програм;

и) реєстрування всіх запитів на внесення змінень у контрольному журналі.

Технічне аналізування змінень, внесених до операційної системи. Необхідність у внесенні змінень до операційної системи виникає періодично, наприклад інсталяція нової версії, наданої постачальником. У таких випадках слід здійснювати аналізування прикладних систем на предмет можливого порушування режиму безпеки, що виникає від таких змінень. Цей процес має містити в собі таке:

- перевіряння процедур контролю застосувань й забезпечування цілісності на предмет компрометації внаслідок внесення змінень до операційної системи;
- забезпечування включення до щорічного плану експлуатації перевіряння й тестування систем, пов'язані зі зміненнями, внесеними до операційної системи, а також надавання для цього необхідних фінансових коштів;
- забезпечування вчасного повідомлення співробітників щодо змінень в операційній системі для проведення належного аналізу до їхнього внесення.

Обмеження на внесення змінень до пакетів програм. Не рекомендується вносити змінення до пакетів програм. За можливості слід використовувати пакети програм, надавані постачальниками, без їхнього модифікування. У тих випадках, коли виникає потреба у внесенні змінень до пакетів програм, слід розглянути таке:

- ризик компрометації вбудованих засобів контролю та процесів забезпечування цілісності;
- необхідність одержання згоди постачальника;
- можливість одержання необхідних змінень від постачальника в межах стандартного відновлювання програм;
- можливість узяття підприємством відповідальності за подальше супроводження програмного забезпечення внаслідок внесених змінень.

Якщо змінення вважаються вкрай необхідне, то слід зберегти вихідне програмне забезпечення, а змінення внести до чітко визначеної копії. Ці змінення слід цілковито задокументувати у такий спосіб, аби їх можна було вносити до майбутніх оновлених версій програм у разі потреби.

9.6 Планування безперебійної роботи підприємства та аудит безпеки

Для захисту критично важливих виробничих процесів від наслідків великих аварій та катастроф слід мати плани забезпечування безперебійної роботи підприємства. Має існувати процес розробляння й здійснення належних планів для швидкого відновлювання критично важливих виробничих процесів та послуг у разі серйозних перебоїв у роботі підприємства. Такі перебої може бути спричинено, наприклад, природними катастрофами, аваріями, відмовами устаткування, навмисними діями і втратою надаваних послуг.

Процес планування безперебійної роботи підприємства має містити в собі заходи для ідентифікації та зменшення ризиків, ліквідації наслідків від здійснення загроз і швидкого відновлювання основних робіт.

Процес планування безперебійної роботи підприємства. Для розробляння й здійснення планів забезпечування безперебійної роботи підприємства слід передбачати ідентифікації й зменшення ризиків навмисних чи випадкових загроз, яким піддаються життєво важливі послуги. Слід розробляти плани підтримування неперервності виробничої діяльності після відмовляння чи ушкодження життєво важливих послуг чи систем. Процес планування безперебійної роботи підприємства має містити в собі таке:

- ідентифікація критично важливих виробничих процесів і їхнє ранжування за пріоритетами;
- визначення можливого впливу аварій різних типів на виробничу діяльність;
- визначення й узгодження обов'язків та планів дій у надзвичайних ситуаціях;
- документування погоджених процедур та процесів;
- належну підготовку персоналу до виконання погоджених процедур та процесів у надзвичайних ситуаціях;
- тестування планів;
- переглядання й відновлювання планів.

Процес планування має бути в першу чергу зосереджений на підтримці працездатності критично важливих виробничих процесів та послуг, включаючи вимоги щодо укомплектування персоналом й інші вимоги, не пов'язані з опрацюванням інформації, а не лише на процедурах переходу на аварійний режим для комп'ютерних систем.

Задля забезпечення погодженості всіх рівнів планування й визначання пріоритетів для тестування та здійснення, слід мати єдину *систему планування безперебійної роботи підприємства*. У кожнім плані забезпечування безперебійної роботи підприємства слід чітко задавати умови його активації, а також зазначати співробітників, які відповідатимуть за здійснення кожного пункту плану. Нові плани не повинні суперечити встановленим процедурам реагування на надзвичайні ситуації, наприклад планам евакуації, й ухваленим процедурам переходу до аварійного режиму для комп'ютерних та комунікаційних систем.

Узагалі, можуть знадобитися різні рівні планування, оскільки кожен рівень зосереджено на власному завданні, а в його здійсненні можуть брати участь різні групи з відновлювання систем після аварій. Модель системи планування безперебійної роботи підприємства містить у собі такі компоненти:

- процедури реагування на надзвичайні ситуації, які описують заходи, що їх слід вживати одразу після великого інциденту, котрий загрожуватиме небезпекою роботі підприємства та/чи життю персоналу;
- процедури переходу до аварійного режиму, які описують заходи, що їх слід вживати для тимчасового передавання основних робіт та послуг до інших об'єктів;

- процедури поновлення роботи підприємства, які описують заходи, що їх слід вживати для відновлювання нормальної повноцінної виробничої діяльності підприємства на основному місці;

- графік випробувань, де визначається, як і коли буде проведено тестування плану.

Кожен рівень планування і кожен індивідуальний план мають мати конкретних виконавців. Обов'язок зі здійсненню процедур реагування на надзвичайні ситуації, планів ручного переходу до аварійного режиму і планів поновлення нормальної роботи підприємства слід покласти на відповідального за виробничий процес.

Тестування планів забезпечування безперебійної роботи підприємства. Багато планів забезпечування безперебійної роботи організації зазнають невдачі при їхньому тестуванні внаслідок неправильних вихідних припущень, прорахунків чи змінень, внесених в устаткування. Тому ці плани слід регулярно тестувати, аби убезпечити їхню ефективність. Такі тести мають гарантувати, що всі члени групи з відновлювання систем після аварій, постійно пам'ятатимуть про план. Слід скласти графік проведення випробувань плану забезпечування безперебійної роботи організації. Такий графік має указувати, як і коли тестуватиметься кожен елемент плану.

Рекомендовано поетапний підхід до тестування, який ґрунтується на проведенні частих випробувань окремих компонентів плану. Це має забезпечувати дієвість і ефективність плану впродовж року. Окрім того, такий підхід дозволяє уникнути частого проведення вичерпних випробувань повного плану.

Плани забезпечування безперебійної роботи підприємств швидко застарівають унаслідок змінень у виробничих процесах і організації, тому їх слід регулярно *оновлювати*. Прикладами змінень, коли необхідні оновляння планів, є:

- придбавання нового устаткування чи модернізування функціонуючих систем;
- нова технологія виявляння проблем, наприклад виявлення пожеж;
- нова технологія контролю за навколишнім середовищем;
- кадрові чи організаційні змінення;
- змінення підрядників чи постачальників;
- змінення адрес чи телефонних номерів;
- змінення, що вносяться у виробничі процеси;
- змінення, що вносяться до пакетів прикладних програм;
- змінення в робочих процедурах;
- змінення в законодавстві.

Слід призначити відповідальних осіб для ідентифікація та внесення змінень до планів. Необхідність в окремих зміненнях слід переглядати принаймні щомісяця. Цей процес має бути підкріплено коротким щорічним аналізом повного плану. Аби гарантувати, що наслідки від внесених змінень визначено й доведено до відома співробітників, потрібен формальний метод контролю за внесенням змінень.

Слід уникати порушень *правових зобов'язань* та зобов'язань щодо дотримання карного й цивільного права, а також забезпечувати виконання вимог щодо інформаційної безпеки. Усі правові й договірні вимоги, які мають відношення до безпеки, слід визначати в явному вигляді й задокументувати. Слід також визначати й задокументувати конкретні засоби контролю, заходи протидії й обов'язки для виконання цих вимог.

Контроль за копіюванням ПЗ, захищеного законом про авторське право. Слід взяти до уваги обмеження, які накладаються чинним законодавством на використання матеріалів, захищених законом про авторське право.

Правові й договірні вимоги можуть накласти обмеження на копіювання програм. Зокрема слід застосовувати лише програми, розроблені підприємством, чи ліцензійне програмне забезпечення. Програмні продукти зазвичай поставляються відповідно до ліцензійної угоди, яка обмежує їхнє використання певними машинами і може обмежувати процес копіювання створенням лише резервних копій. Слід враховувати таке:

- політика підприємства має забороняти копіювання матеріалу, захищеного законом про авторське право, без згоди його власника;
- користувачам має бути рекомендовано не порушувати цю політику, здійснюючи копіювання програм без письмової санкції їхнього власника;
- копіювання патентованого програмного забезпечення чи програм підприємства для використання на комп'ютерах, які не належать підприємству, для цілей, не пов'язаних з основною виробничою діяльністю, може також призвести до порушування закону про авторське право й політики організації;
- в разі потреби інсталювати програмний продукт на додаткових машинах, слід внести пункт щодо цього до ліцензійної угоди чи придбати додаткові копії;
- слід регулярно перевіряти використання програмного забезпечення й вести належний облік.

Порушування закону про авторське право може призвести до судових розглядань і навіть до порушування кримінальної справи.

Важливу для *підприємства документацію слід захищати* від утрати, знищення й підробляння. Певні документи мають зберігатись в захищеному місці для задоволення правових вимог, а також для підтримування основної виробничої діяльності. За приклади цього слугують документи, які можуть знадобитися як засвідчення того, що підприємство працює відповідно до чинних правових норм, а також для забезпечування належного захисту від можливих цивільних чи карних позовів або для потвердження фінансового стану підприємства стосовно власників акцій, партнерів та аудиторів. Є сенс знищувати документацію, термін зберігання якої сплив, якщо це не позначається негативно на роботі підприємства.

Для виконання цих зобов'язань підприємство має розпочати таке:

- підготувати інструкції щодо зберігання й обігу документації й інформації, а також їхнього знищення;
- скласти план-графік, у якому має бути визначено основні типи документів та терміни їхнього зберігання;

- провадити інвентаризацію всіх джерел основної інформації;

- реалізовувати належні заходи для захисту основної документації від утрати, знищення і підробляння.

Згідно з чинним законодавством України, *персональні дані* про осіб, за якими їх можна ідентифікувати, і які зберігаються чи опрацьовується на комп'ютерах, підлягають захистові. Дотримування законодавства про захист інформації потребує певного структурування керівництва і контроль. Це найчастіше досягається за допомогою призначення співробітника, який відповідає за захист даних, надає рекомендації адміністраторам, користувачам та постачальникам послуг з розподілу обов'язків і використання конкретних процедур. У коло обов'язків власника даних має входити доведення положень про зберігання персональної інформації на комп'ютері до відома співробітника, який відповідає за захист даних, і забезпечування знання й розуміння принципів захисту інформації, визначених чинним законодавством.

Відомо вісім принципів, застосовних до всіх систем, котрі опрацьовують персональну інформацію:

1 слід надавати доступ до інформації, утримуваної в персональних даних, і опрацьовувати персональні дані на законних підставах й відповідно до принципів справедливості;

2 персональні дані слід зберігати лише для певних, законних цілей;

3 Персональні дані, які зберігаються для певних цілей, не слід використовувати чи розкривати у спосіб, несумісний з цими цілями;

4 персональні дані, зберіганні для певних цілей, мають бути адекватними до цих цілей і не бути надлишковими стосовно останніх;

5 персональні дані мають бути точними і, за потреби, свіжими;

6 персональні дані, які зберігаються для певних цілей, не слід зберігати довше, ніж це потрібно для цих цілей;

7 співробітник повинен мати право:

- через розумні проміжки часу й без затримок одержувати інформацію від користувача даних про те, чи зберігає він персональні дані, суб'єктом яких є даний співробітник, а також доступ до таких даних;

- за потребою виправляти чи стирати вищезазначені дані.

8 слід вживати належних заходів щодо захисту персональних даних від несанкціонованого доступу, їхнього змінення, розкривання й знищення, а також від їхньої випадкової втрати чи знищення.

Запобігання незаконному використанню інформаційних ресурсів. Інформаційні ресурси підприємства надаються для виробничих цілей. Їхнє використання має бути санкціоноване керівництвом. Використання цих ресурсів для цілей, не пов'язаних з основною діяльністю підприємства, чи для несанкціонованих цілей без дозволу керівництва і процедур обліку розглядається як протиправне використання інформаційних ресурсів. В разі виявлення таких випадків вони доводяться до відома керівництва для накладення дисциплінарних стягнень. Використання комп'ютера для протиправних цілей вважається карним злочином. Тому є вкрай важливо, аби усі користувачі одержували письмову санкцію на дозвіл доступу. Користувачів

слід попереджати, що вони не мають права доступу, окрім випадків, які формально санкціоновано і задокументовано.

Для забезпечування відповідності систем політиці та стандартам безпеки інформаційних систем підприємства потрібне регулярне *перевіряння безпеки інформаційних систем*. Таке перевіряння слід провадити виходячи з відповідної політики безпеки, а технічні платформи й інформаційні системи слід перевіряти на відповідність чинним стандартам забезпечування безпеки.

Усі підрозділи підприємства мають регулярно перевірюватись, аби забезпечувати *відповідність чинній політиці та стандартам безпеки*. Перевірянню підлягають: інформаційні системи та їхні постачальники; інформація та власники даних; користувачі; керівництво. Власники інформаційних систем мають організовувати регулярні перевіряння власних систем на відповідність чинній політиці безпеки, стандартам та іншим вимогам щодо їхнього захисту.

Аудит безпеки. *Інформаційні ресурси слід регулярно перевіряти на відповідність стандартам забезпечування безпеки.* Технічне перевіряння на таку відповідність містить у собі оглядання робочих систем, аби гарантувати правильне функціонування засобів управління безпекою програмного й апаратного забезпечення. Таке перевіряння має провадитися досвідченим системним інженером, котрий створює технічний звіт для наступного опрацювання фахівцем, вручну чи автоматично за допомогою пакета програм. Такі перевіряння мають провадитися лише компетентними особами чи під їхнім наглядом.

Треба мати засоби контролю для захисту робочих систем і *засоби аудиту* під час їхнього перевіряння. Захист також потрібен для забезпечування цілісності засобів аудиту й запобігання їхньому несанкціонованому використанню. Для зведення ризику виникнення збоїв у виробничих процесах до мінімуму слід ретельно планувати й погоджувати вимоги щодо аудиту й роботи, пов’язаної з перевірянням робочих систем. Пропоноване розглядати таке:

- вимоги щодо аудиту систем має бути погоджено з керівництвом;
- масштаб перевірянь слід погоджувати й контролювати;
- перевіряння має бути обмежено доступом до даних та програм лише в режимі читання;
- доступу інших типів – записування, вилучання – має бути дозволено для окремих копій системних даних, які слід стирати після завершення процесу аудиту;
- треба явно ідентифікувати інформаційні ресурси для проведення перевірянь і зробити їх доступними;
- слід визначати вимоги щодо спеціального чи додаткового опрацювання й погоджувати їх з постачальниками послуг;
- усі випадки доступу слід відстежувати й фіксувати в контрольному журналі для довідок;
- усі процедури, вимоги й обов’язки слід задокументувати.

Захист засобів аудиту систем. Доступ до засобів аудиту систем, тобто

до програм та файлів даних, слід захищати, аби запобігати їхньому можливому несанкціонованому використанню чи компрометації. Такі засоби треба ізолювати від розроблювальних та робочих систем і не слід зберігати в бібліотеках магнітних стрічок і на робочих місцях користувачів, якщо їх не забезпечено належним додатковим захистом.

В штатному розписі підприємства має бути передбачено посаду відповідального, і її має посідати досвідчений фахівець з безпеки. Для невеликих підприємств рекомендовано створювати єдину службу експлуатації, аби забезпечувати погодженість при ухвалюванні рішень з питань безпеки та сприяти максимальному використанню знань і досвіду співробітників.

Контрольні запитання та завдання

1. Наведіть етапи життєвого циклу систем захисту інформації.
2. Дайте означення та мету управління інформаційною безпекою на стадії технічної експлуатації інформаційно-обчислювальної системи.
3. З яких груп практичних правил складається управління інформаційною безпекою?
4. Який зміст має документ щодо політики безпеки підприємства?
5. Для чого і в який спосіб провадять оцінювання ризику?
6. Сформулюйте основні положення з організації захисту.
7. Правила доступу сторонніх організацій – орендарів, інших операторів – до інформаційних ресурсів підприємства.
8. Заходи з класифікації ресурсів та їхнього контролю.
9. Поясніть правила та процедури щодо безпеки фізичного середовища.

Завдання до самостійної роботи

1. Розробити документ щодо типової політики безпеки підприємства зв’язку.
2. Розробити зведення правил безпеки фізичного середовища функціонування інформаційно-обчислювальної системи.
3. Скласти типовий план щодо реагування на інциденти з безпекою підприємства зв’язку та його підрозділу інформаційних технологій.
4. Розробити процедури й порядок створення, контролю та використання резервних та архівних копій програм і даних.
5. Скласти план безперебійної роботи підприємства.

Завдання до практичного заняття

1. Розглянути й проаналізувати основні завдання і функції адміністрування інформаційно-обчислювальних систем у частині забезпечування безпеки інформації:

- обов’язки й процедури з адміністрування й забезпечування функціонування комп’ютерів та мереж;

- які робочі інструкції та операційні процедури має бути задокументовано?

- розглянути рекомендації стандарту з безпеки щодо вибору процедур реагування на події;

- роль поділу обов'язків у зменшенні ризику недбалого чи несанкціонованого використання систем. Які функції не можна суміщати з погляду на безпеку інформації?

- рознесення програмних засобів розробляння й робочих програм та засоби їхнього контролю;

- засоби контролю навантаження систем для підтримування безвідмовної роботи;

- планування переходу до аварійного режиму;

- формальні процедури управління й обов'язки для забезпечування контролю за внесенням усіх змінень в устаткування, програми й процедури;

- заходи щодо виявлення й запобігання проникненню вірусів до систем;

- правила ведення журналів реєстрування подій, де фіксуються усі виконувані завдання, та реєстрування збоїв систем;

- значення та засоби резервного копіювання даних;

- система процедур робочого, архівного та резервного копіювання;

- процедури оперування з даними, котрі забезпечують їхню цілісність, доступність та конфіденційність;

- заходи захисту систем електронного офісу та електронної пошти.

2. Розглянути й проаналізувати заходи безпеки на стадіях розробляння і супроводження інформаційних систем:

- аналізування і завдання вимог щодо безпеки інформаційних систем;

- які засоби управління безпекою слід вмонтовувати до прикладних систем?

- необхідність перевірянь вірогідності вхідних даних; вірогідності внутрішнього опрацювання даних;

- у яких випадках потрібне застосовування шифрування даних, автентифікування повідомлень?

- як здійснюється захист файлів прикладних систем, контроль робочого програмного забезпечення та захист системних тестових даних?

- заходи безпеки в середовищі розробляння та в робочому середовищі;

- вимоги щодо процедур управління внесенням змінень;

- порядок технічного аналізування змінень, внесених до операційної системи;

- які існують обмеження щодо внесення змінень до пакетів програм?

3. Розглянути й проаналізувати систему неперервної роботи підприємства:

- що включає у себе процес планування роботи підприємства?

- компоненти моделі системи планування безперебійної роботи підприємства;

- тестування планів забезпечування безперебійної роботи підприємства;

- за яких змінень слід оновлювати плани забезпечування безперебійної роботи підприємства?
- контроль за копіюванням програмного забезпечення, захищеного законом про авторське право;
- заходи із захисту документації підприємства;
- проаналізувати вісім принципів щодо опрацювання персональної інформації;
- запобігання протиправному використанню інформаційних ресурсів;
- порядок і засоби перевіряння безпеки інформаційних систем;
- мета й засоби аудиту систем.

РОЗДІЛ 10

МЕТОДИЧНІ ОСНОВИ ОЦІНКИ ЕКОНОМІЧНОЇ ДОЦІЛЬНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ

10.1 Методичні основи оцінки економічної доцільності захисту інформації

Розглянемо обґрунтування доцільності та оцінку витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової автоматичної телефонної станції (АТС). Поділимо витрати на інформаційну безпеку за наступними категоріями на прикладі інформаційної безпеки цифрової АТС:

1. Витрати на формування та підтримку системи захисту інформації (витрати на організацію інформаційної безпеки).

2. Витрати на експлуатацію, тобто на технічне обслуговування системи захисту інформації та заходи по попередженню порушень політики безпеки підприємства, на визначення та підтримку досягнутого рівня захищеності ресурсів цифрової АТС.

3. Запобігання збиткам – витрати, яких може зазнати організація в результаті того, що потрібного рівня захищеності не було досягнуто або при порушенні політики безпеки у випадках, пов’язаних з витоком інформації, втратою іміджу компанії, втратою довіри партнерів та споживачів тощо.

4. Загальні витрати, що включають витрати на організацію інформаційної безпеки, витрати на експлуатацію та запобігання збитків.

Класифікація витрат умовна, тому що збирання, класифікація та аналіз витрат на інформаційну безпеку – внутрішня справа підприємств, а детальне розроблення переліку залежать від особливостей конкретної організації. Головне при визначенні витрат на систему безпеки – взаєморозуміння та згода за статтями видатків усередині підприємства. Крім того, категорії витрат мають бути постійними та не мають дублювати один одного.

Неможливо повністю уникнути витрат на безпеку, однак вони можуть бути приведені до прийнятного відділу. Деякі види витрат на безпеку є абсолютно необхідними, а деякі можуть бути суттєво зменшені або виключені, наприклад, ті, які можуть зникнути при відсутності порушень політики безпеки або скоротяться, якщо кількість та руйнівний вплив порушень зменшаться.

При дотриманні політики безпеки та проведенні профілактики порушень можна виключити або суттєво зменшити наступні витрати:

– на відновлення ресурсів інформаційного середовища підприємства;

– на відновлення системи безпеки до відповідності вимогам політики безпеки;

– на відновлення ресурсів інформаційного середовища цифрової АТС;

– на переробку всередині системи безпеки;

– на юридичні суперечки та виплати компенсацій;

– на виявлення причин порушення політики безпеки.

Необхідні витрати – це ті, які необхідні навіть коли рівень загроз безпеці досить низький. Це витрати на підтримання досягнутого рівня захищеності інформаційного середовища цифрової АТС. Обов'язкові витрати можуть включати:

– обслуговування технічних засобів захисту;

– конфіденційне діловодство;

– функціонування та аудит системи безпеки;

– мінімальний рівень повірок та контролю з залученням спеціалізованих організацій;

– навчання персоналу методам інформаційної безпеки.

Сума всіх витрат на підвищення рівня захищеності підприємства від загроз інформаційної безпеки складає загальні витрати на безпеку, яка однак може бути зменшена за рахунок економії, що досягається за рахунок функціонування системи інформаційної безпеки.

Якісний взаємозв'язок між усіма витратами на безпеку, загальними витратами на безпеку та рівнем захищеності інформаційного середовища підприємства зазвичай має вид функції (рис. 10.1).

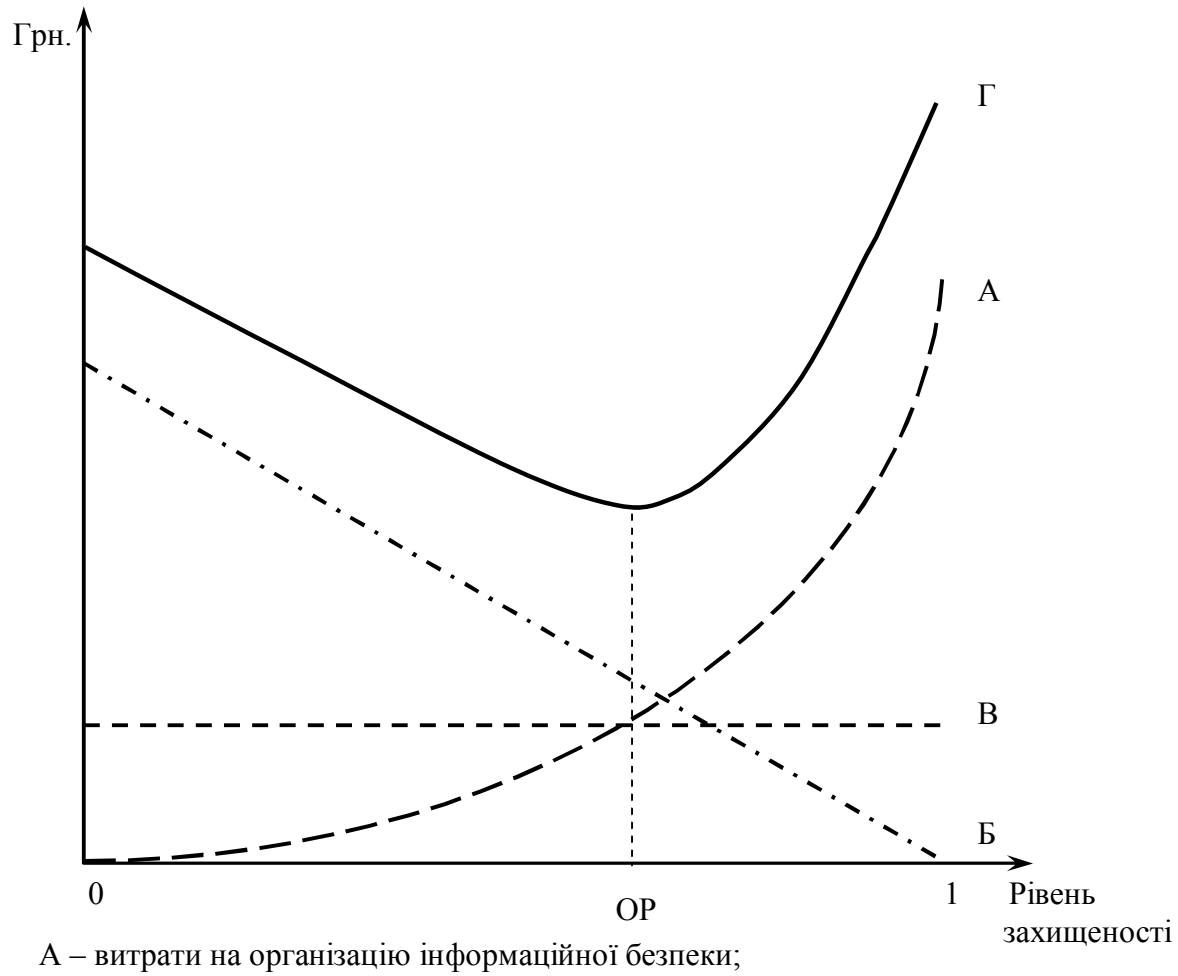
Зі зміною рівня захищеності інформаційного середовища змінюються розміри складових загальних витрат та, відповідно, їхня сума – загальні витрати на безпеку.

На рис. 10.1 показано, що досягнутий рівень захищеності вимірюється за умовною якісною шкалою від 0 до 1, де 0 – повна відсутність захищеності, 1 – абсолютна захищеність, яка на практиці ніколи не може бути досягнута.

Розглядаючи ліву сторону графіка, ми бачимо, що загальні витрати на інформаційну безпеку високі здебільшого тому, що високі витрати на компенсацію (запобігання збиткам) при порушеннях політики безпеки цифрової АТС. Витрати на обслуговування системи безпеки дуже малі.

Припустимо, що частка витрат на інформаційну безпеку збільшується. Це відповідає руху вправо рис. 10.1 за графіком. Якщо ми будемо рухатися вправо за графіком, то досягнутий рівень буде збільшуватися, а інформаційний ризик знижуватися. Це відбувається за рахунок збільшення коштів на організацію інформаційної безпеки. Запобігання збиткам зменшується в результаті попереджувальних заходів. Як показано на графіку, на цьому етапі витрати на компенсацію запобігання збитків падають швидше, ніж зростають витрати на організацію інформаційної безпеки цифрової АТС. Як результат – загальні витрати на безпеку зменшуються. Зміна об'єму витрат на експлуатацію незначна.

Якщо рухатись за графіком вправо за точку економічної рівноваги (тобто, коли рівень захищеності росте), то ситуація починає змінюватись. Добиваючись стійкого зниження витрат на запобігання збиткам від порушення політики безпеки, ми бачимо, що витрати на організацію певного рівня інформаційної безпеки зростають все швидше і швидше. Виходить, що значна кількість коштів має бути витрачена на досягнення досить малого зниження рівня ризику.



А – витрати на організацію інформаційної безпеки;

Б – запобігання збиткам;

В – витрати на експлуатацію системи інформаційної безпеки;

Г – загальні витрати (крива, що характеризує ефективність системи інформаційної безпеки, яка включає витрати на організацію та експлуатацію, а також економію коштів, якої досягають при створенні системи інформаційної безпеки);

ОР – оптимальний рівень захищеності та витрат на інформаційну безпеку (точка економічної рівноваги)

Рисунок 10.1 – Взаємозв'язок між витратами на інформаційну безпеку та досягнутим рівнем захищеності

Рис. 10.1 відбиває тільки загальний випадок, оскільки побудований з урахуванням певних припущень, які не завжди відповідають реальним ситуаціям.

Головне припущення полягає в тому, що точка економічної рівноваги не змінюється в часі. На практиці це припущення часто не виконується. Основні фактори:

– старіння системи інформаційної безпеки;

– розробники засобів захисту не встигають за активністю зловмисників, які знаходять все нові й нові слабкі місця в системах захисту. Крім того, інформатизація підприємства може викликати нові проблеми, вирішення яких потребує додаткових витрат на організацію інформаційної безпеки. Все це

може змістити економічну рівновагу у напряму до лівого краю графіка рис. 10.1.

З проведеного дослідження випливає, що в структурі витрат на інформаційну безпеку, визначну позицію займають витрати на організацію інформаційної безпеки, оскільки їх збільшення веде до зменшення витрат на компенсацію (запобігання збиткам), а витрати на експлуатацію системи безпеки практично не змінюються.

Перейдемо до оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової АТС.

Сфера використання.

1. Методичні основи обґрунтування доцільності витрат на запровадження системи інформаційної безпеки програмно-керованих АТС призначена для визначення ефективності витрат на стадіях їх життєвого циклу – проектування системи інформаційної безпеки, створення, випробування та впровадження

2. Методичні основи містять короткий опис методу розрахунків, порядок розрахунків ефективності витрат на інформаційну безпеку АТС, приклади розрахунків та коментарі до основних положень. Розрахунки ефективності витрат на інформаційну безпеку АТС виконуються за наступною методикою [138].

3. Методичні основи призначені для працівників підрозділів ТЗІ та економістів.

4. Результати визначення ефективності витрат мають використовуватися для вирішення таких завдань:

– вибору варіантів побудови системи інформаційної безпеки АТС та прогнозів ефективності від їхнього здійснення;

– планування та раціональний розподіл ресурсів за етапами життєвого циклу системи інформаційної безпеки АТС;

– визначення фактичної економічної ефективності системи інформаційної безпеки АТС, зокрема її впливу на економіку підприємства.

5. На основі обґрунтування формується техніко-економічне завдання виконавцям на проектування і створення системи інформаційної безпеки АТС. Ключовими його показниками є величина, яка відбиває ефективність застосування, що забезпечена за певний період, та величина відвернутих збитків внаслідок можливої реалізації загроз інформаційній безпеці.

Основні положення.

1. Визнаними в практиці основними показниками, що акумулюють вигоди упровадження системи інформаційної безпеки, є:

– чистий дисконтований доход, який у даному випадку представлений відвернутими втратами від реалізації загроз інформаційній безпеці;

– період окупності інвестицій у реалізацію системи інформаційної безпеки;

– внутрішня норма прибутковості.

Пояснення щодо економічної суті економічних показників та приклади їх визначення наведені у прикладі розрахунків цього підрозділу.

2. Кількісна методика обґрунтування витрат на інформаційну безпеку є методом розрахунку техніко-економічної ефективності впровадження системи інформаційної безпеки в АТС, в якому фінансова вигода забезпечується щорічними збереженнями, які отримані при впровадженні системи інформаційної безпеки

$$A_{\text{щек}}=A_{\text{втр}}\,E - A_{\text{вит}}\,, \qquad (10.1)$$

де $A_{\text{щек}}$ – величина щорічної економії;

$A_{\text{втр}}$ – показник очікуваних втрат;

E – коефіцієнт ефективності системи захисту (його можна назвати коефіцієнтом психологічної ефективності системи захисту), E = 0,85.

$A_{\text{вит}}$ – щорічні витрати на інформаційну безпеку.

3. Визначення показника очікуваних втрат $A_{\text{втр}}$ засноване на знанні Власником цінності своєї інформації та емпіричних відомостях про вторгнення, про втрати від вірусів, про відбиття атак на ресурси тощо. Порушення безпеки може приводити до фінансових втрат, зв'язаних з:

– з простоями та виходом з ладу станційного та мережного обладнання;

– з нанесенням шкоди іміджу та репутації підприємства;

– з оплатою робіт по відновленню роботи системи, програмного забезпечення тощо;

– з витратами по судочинству тощо.

4. Початкові дані для оцінки можуть бути одержані трьома способами:

– збиранням статистичних даних за попередній період про загрози, їхню номенклатуру й частоту, втрати, понесені від загроз – фінансові, моральні, матеріальні, а також використанням результатів обстеження АТС як об'єкта інформаційної діяльності;

– використанням статистичних даних аналогічних українських підприємств, які діють у тому ж правовому полі;

– використанням статистичних даних зарубіжних фірм з урахуванням особливостей українського законодавства, умов підприємницької діяльності та нормативно-правових документів сфери ТЗІ. У прикладі розрахунку використано останній спосіб.

5. Для одержання оцінки очікуваних втрат використовують таблицю оцінки загроз та ризиків, яка дає можливість кількісно оцінити ймовірності подій. В таблиці взаємозв'язуються ймовірності загроз, міра небезпечності загроз і частота подій. Загальні очікувані втрати обчислюються як сума очікуваних втрат з кожної потенційної загрози. Наводиться шаблон табл. 10.1.

Таблиця 10.1 - Розрахунок показника очікуваних втрат

№	Потенційні загрози	Частота виникнення, f	Втрати, грн., L	Втрати, %	$A_{\text{втр}}$, грн.
1	2	3	4	5	6

6. Показник $A_{втр}$ обчислюється за формулою:

$$A_{втр} = f*L, \qquad (10.2)$$

де f – частота виникнення потенційної загрози, рівень якої визначається на основі ймовірності загроз;

L – величина втрат у гривнях, яка визначається на основі небезпечності порушення.

Для тих загроз, на які відсутні статистичні дані про частоту їхнього виникнення, використовують якісні шкали. Частоту виникнення таких загроз визначають використовуючи залежність між частотою й якісною оцінкою ймовірності. Приклад такої залежності показано у табл. 10.2.

Таблиця 10.2 - Приклад перетворювання ймовірності загроз до річної частоти

Рівень імовірності	Опис	Частота
1	2	3
Незначний	Навряд відбудеться	0,05
Дуже низький	Подія відбувається два-три рази на 5 років	0,6
Низький	Подія відбувається менше одного разу на рік або раз на рік	1,0
Середній	Подія відбувається менше одного разу на півріччя або раз на півріччя	2,0
Високий	Подія відбувається менш одного разу на місяць або раз на місяць	12,0
Дуже високий	Подія відбувається декілька разів на місяць	36,0
Екстремальний	Подія відбувається декілька разів на день	365,0

7. Витрати на створення системи інформаційної безпеки поділяють на одноразові і періодичні. Одноразові витрати складаються з витрат на купівлю апаратних засобів, програмного забезпечення, проектування системи.

Періодичні витрати складаються з витрат на технічне обслуговування та супроводження, заробітну платню персоналу, навчання та підвищення кваліфікації спеціалістів, витрат на дослідження загроз порушення політики безпеки.

8. Далі витрати на впровадження системи захисту, розрахунок періоду окупності та економічної ефективності, приведені вартості розраховують класичним методом. Порядок розрахунку наведено нижче.

Порядок розрахунків:

1. Після визначення показника очікуваних втрат приймається рішення про створення системи інформаційної безпеки і проводиться розрахунок її економічної ефективності.

2. Вибираються вхідні дані за статтями витрат на купівлю ліцензії, на проектні роботи, на технічну підтримку. Норматив витрат на технічну підтримку складає 30% від вартості ліцензії. Витрати на впровадження системи захисту інформації розраховуються за наступною формулою:

$$C_{\text{впр}}=C_{\text{л}}+C_{\text{пр}}+\sum_{s} C_i, \qquad (10.3)$$

де: $C_{\text{впр}}$ – витрати на впровадження;
$C_{\text{л}}$ – витрати на купівлю ліцензії;
$C_{\text{пр}}$ – витрати на проектні роботи;
C_i – витрати на технічну підтримку.

Період окупності інвестиційних проектів, пов'язаних з впровадженням інформаційних технологій, не повинен бути більшим ніж три роки, тому період оцінки ефективності даного проекту впровадження дорівнює трьом рокам. Витрати на проектні роботи розподіляються на першому році. Витрати на технічну підтримку розподіляються на подальший період впровадження.

Результати цього і наступних розрахунків зручно і наглядно зводити в таблицю розрахунку показника повернення інвестицій на систему інформаційної безпеки. Приклад такої таблиці та розрахунків оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової АТС наводиться у розділі 10.2., табл. 10.3.

3. Розраховуються на кожен рік накопичені витрати проекту впровадження за формулою:

$$\begin{aligned} C_{\text{нак }1} &= C_{\text{нак поч}}+C_{\text{впр1,}} \\ C_{\text{нак }2} &= C_{\text{нак }1}+C_{\text{впр2,}} \\ C_{\text{нак }3} &= C_{\text{нак }2}+C_{\text{впр3,}} \end{aligned} \qquad (10.4)$$

де $C_{\text{нак}}$ – накопичені витрати проекту впровадження;
$C_{\text{впр}}$ – витрати на впровадження.

4. Розраховується на кожен рік накопичений чистий грошовий потік витрат на впровадження за формулою:

$$NPV_{\text{в}}=\sum_{i=0}^{2}\frac{CF}{(1+r)^i} \qquad (10.5)$$

де $NPV_{\text{в}}$ – накопичений чистий грошовий потік витрат на проект впровадження;
CF – грошовий потік відіграють витрати на впровадження);
r – ставка дисконтування.

Роль грошового потоку грають витрати на впровадження. Ставка дисконтування дорівнює ставці рефінансування Національного Банку України (НБУ), r = 15%.

5. Вибираються з фінансових та технічних звітів підприємства, показники загальної вартості володіння *(TCO – Total Cost of Ownership)*:

$TCO_{\text{п}}$ – поточний показник *TCO*;

$TCO_{ц}$ – цільовий показник *TCO*;

$TCO_{ф}$ – фактичний показник *TCO*.

6. Розраховуються вигоди при оптимізації показника загальної вартості володіння за формулою:

$$В = TCO_{п} – TCO_{ф}, \quad (10.6)$$

де В – накопичений показник вигод при оптимізації показника *TCO*;

$TCO_{п}$ – поточний показник *TCO*;

$TCO_{ф}$ – фактичний показник *TCO*.

7. Розраховуються величини щорічної економії за формулою:

$$A_{щек} = A_{втр} * E - A_{вит}, \quad (10.7)$$

де $A_{щек}$ – величина щорічної економії;

$A_{втр}$ – показник очікуваних втрат;

E – коефіцієнт ефективності системи захисту (його можна назвати коефіцієнтом психологічної ефективності системи захисту);

$A_{вит}$ – щорічні витрати на інформаційну безпеку, $A_{вит} = TCO_{ф}$

8. Розраховується показник вигод при оптимізації показника *TCO* та щорічної економії за формулою:

$$В_{тсо} = В + A_{щек}, \quad (10.8)$$

де $В_{тсо}$ – показник вигод при оптимізації показника *TCO* та щорічних збережень;

В – вигоди при оптимізації показника ТСО;

$A_{щек}$ – величина щорічної економії.

9. Розраховується накопичений показник вигод при оптимізації показника *TCO* та щорічної економії за формулою:

$$\begin{gathered} В_{нак\ 1} = В_{тсо1,} \\ В_{нак\ 2} = В_{нак\ 1} + В_{тсо2,} \\ В_{нак\ 3} = В_{нак\ 2} + В_{тсо3} \end{gathered} \quad (10.9)$$

де $В_{нак}$ – накопичений показник вигод при оптимізації показника *TCO* та щорічної економії;

$В_{тсо}$ – показник вигод при оптимізації показника *TCO* та щорічних збережень.

10. Розраховується грошовий потік за формулою:

$$CF = В_{тсо} - C_{впр}, \quad (10.10)$$

де: *CF* – грошовий потік;

$В_{тсо}$ – показник вигод при оптимізації показника *TCO* та щорічних збережень;

$С_{впр}$ – витрати на впровадження.

11. Розраховується накопичений грошовий потік за формулою:

$$CF_{нак} = В_{нак} - C_{нак}, \quad (10.11)$$

де $CF_{нак}$ – накопичений грошовий потік;

$В_{нак}$ – накопичений показник вигод при оптимізації показника *TCO* та щорічної економії;

$C_{нак}$ – накопичені витрати проекту впровадження.

12. Розраховується накопичений чистий грошовий потік доходів (відвернутих витрат) від проекту впровадження за наступною формулою:

$$NPV_{д} = \sum_{i=0}^{2} \frac{CF}{(1+r)^{i}}, \quad (10.12)$$

де: $NPV_{д}$ – накопичений чистий грошовий потік відвернутих доходів від проекту впровадження;

CF – грошовий потік (вигоди від оптимізації показника ТСО та впровадження корпоративної системи захисту);

r – ставка дисконтування.

Ставка дисконтування у цій формулі приймається за *r* = 25%. Це дасть можливість обчислити далі внутрішню норму прибутковості.

13. Розраховується внутрішня норма прибутковості (*IRR*). Розрахунок проводиться графічним способом. На графіку будується пряма, яка з'єднує точку накопиченого чистого грошового потоку на проект $NPV_{в}$ при ставці дисконтування *r* = 15% з точкою, яка відповідає накопиченому чистому грошовому потоку відвернутих витрат від проекту впровадження – $NPV_{д}$ при ставці дисконтування *r* = 25%. Точка, де пряма перетинає вісь абсцис є внутрішньою нормою прибутковості. Прибутковість тут має значення відвернутих збитків, які могли б бути за відсутності системи інформаційної безпеки.

10.2 Приклад розрахунку оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової автоматичної телефонної станції

Користуючись результатами обстеження об'єкта інформаційної діяльності та матеріалами розробленої моделі загроз складається перелік загроз інформаційної безпеки і заповнюється стовпчик 2 таблиці розрахунку показника очікуваних втрат (табл. 10.3). В наведеному прикладі враховується 11 потенційних загроз інформаційній безпеці відповідно з [79].

Заповняємо табл. 10.3 розрахунку показника очікуваних втрат.

Частота виникнення визначається відповідно до статистичних матеріалів за таблицею перетворювання ймовірності загроз до річної частоти і записується в стовпчик 3.

Таблиця 10.3 – Розрахунок показника очікуваних втрат

№ пп.	Потенціальні загрози	Частота виникнення, f	Втрати, грн., L	Втрати, %	$A_{втр}$, грн.
1	2	3	4	5	6
1	Саботаж	0,6	348,4	1,3	209,04
2	Проникнення у систему	1,0	402	1,5	402
3	Атаки на ПЕОМ управління	36	495,8	1,85	17 848,4
4	Помилки в роботі з базою даних	36	790,6	2,95	28 461,6
5	Телефонне шахрайство	12,0	1425,76	5,32	17 109,12
6	Неавторизований доступ	12,0	951,4	3,55	11 416,8
7	Крадіжка обладнання і програм	0,6	1407	5,250	844,2
8	Фінансове шахрайство	1,0	1988,56	7,42	1 988,56
9	Помилки в роботі мережі сигналізації, синхронізації та керування	1,0	2546	9,5	2 546
10	Крадіжка приватної інформації	1,0	6003,2	22,4	6 003,2
11	Віруси	36,0	10441,28	38,96	375 886,08
12	Всього		26800	100,00	462 715

Втрати розраховуються на основі статистичних даних, які забрані на даному підприємстві або на інших аналогічних підприємствах, і записуються у стовпчик 4. Внесок кожної потенційної загрози обчислюється у відсотковому відношенні і записується у стовпчик 5.

$A_{втр}$ розраховується за формулою (10.2) і записуються у стовпчик 6. У даному випадку маємо відповідно:

$A_{втр1} = 0,6*348,4 = 209,04$ грн.;

$A_{втр2} = 1,0*402 = 402$ грн.;

$A_{втр3} = 36*495,8 = 17848,4$ грн.;

$A_{втр4} = 36*790,6 = 28461,6$ грн.;

$A_{втр5} = 12,0*1425,76 = 17109,12$ грн.;

$A_{втр6} = 12,0*951,4 = 111416,8$ грн.;

$A_{втр7} = 0,6*1407 = 844,2$ грн.;

$A_{втр8} = 1,0*1988,56 = 1988,56$ грн.;

$A_{втр9} = 1,0*2546 = 2546$ грн.;

$A_{втр10} = 1,0*6003,2 = 6003,2$ грн.;

$A_{втр11} = 36,0*10441,28 = 375886,08$ грн.

Підсумовуючи дані колонки 6 табл.10.3 отримуємо показник очікуваних втрат $A_{втрΣ}$=462715 грн.

Вибираємо вхідні дані за статтями витрат, які наводимо в табл. 10.4.

Таблиця 10.4 – Вихідні дані

№ пп.	Статті витрат	Вартість, грн.
1	2	3
1	Витрати на купівлю ліцензії	150 000
2	Витрати на проектні роботи	3 500
3	Технічна підтримка (30% від вартості ліцензії щорічно)	45 000

Розраховуємо $C_{впр}$ – витрати на впровадження системи захисту інформації за формулою (10.3) та розподіляємо їх на три роки. Витрати на проектні роботи розподіляємо на першому році. Витрати на технічну підтримку розподіляємо на подальший період впровадження. Ці і подальші результати обчислень зводимо в таблицю розрахунку оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки (табл. 10.5).

Розраховуємо на кожен рік $C_{нак}$ – накопичені витрати проекту впровадження за формулами (10.4). Маємо послідовно:

$C_{нак\ 1}$ =150 000 + 3500 = 153 500 грн.;

$C_{нак\ 2}$ = 153 500+45 000 = 198 500 грн.;

$C_{нак\ 3}$ = 198 500 + 45000 = 243 500 грн.

Результати заносимо в табл. 10.5.

Розраховуємо *NPV* – накопичений чистий грошовий потік витрат на впровадження за формулою (10.5). За три роки маємо *NPV* = 150 000 * 0,15 = 22500 грн. Цей результат заносимо у другий стовпчик табл.10.5.

Робимо на кожен рік вибірку з фінансових та технічних звітів підприємства, показники загальної вартості володіння *(TCO – Total Cost of Ownership)*:

$TCO_{п}$ – поточного показника ТСО;

$TCO_{ц}$ – цільового показника ТСО;

$TCO_{ф}$ – фактичного показника ТСО.

Результати вибірки заносимо в табл. 10.5.

Розраховуємо на кожен рік та в цілому за три роки *B* – накопичений показник вигоди при оптимізації показника загальної вартості володіння та щорічні збереження за формулою (10.6).

Маємо послідовно:

B_1 = 8794,58 - 8359,99 = 434, 59 грн.;

B_2 = 8794,58 - 7273,52 = 1521,06 грн.;

B_3 = 8794,58 - 6621,64 = 2172,94 грн.;

B_{Σ} = 434,59 + 1521,06 + 2172,94 = 4128,59 грн.

Результати обчислень заносимо в табл. 10.5.

Записуємо у табл. 10.5 величину показника очікуваних втрат $A_{втр}$ та величину коефіцієнта ефективності системи корпоративного захисту (коефіцієнт психологічної ефективності) *E,* $A_{витi} = TCO_{фi}$ Розраховуємо $A_{щек}$ – величини щорічних збережень за формулою (10.7).

Маємо послідовно:

$A_{щек\ 1} = A_{втр} * E - A_{вит\ 1} = 462\ 715 * 0{,}85 - 8359{,}99 = 384\ 947{,}76$ грн.;

$A_{щек\ 2} = A_{втр} * E - A_{вит\ 2} = 462\ 715 * 0{,}85 - 7273{,}52 = 386\ 034{,}23$ грн.;

$A_{щек\ 3} = A_{втр} * E - A_{вит\ 3} = 462\ 715 * 0{,}85 - 6621{,}64 = 386\ 686{,}11$ грн;

$A_{щекΣ} = A_{втр} * E - A_{вит\ Σ} = 1\ 388\ 145 * 0{,}85 - 22255{,}15 = 1\ 157\ 668{,}1$ грн.

Результати обчислень заносимо в табл. 10.5.

Розраховуємо на кожен рік та в цілому показник вигод при оптимізації показника *ТСО* та щорічних збережень $В_{тсо}$ за формулою (10.8). Маємо послідовно:

$В_{тсо1} = В_1 + A_{щек1} = 434{,}59 + 384\ 947{,}76 = 385\ 382{,}35$ грн.;

$В_{тсо2} = В_2 + A_{щек2} = 1521{,}06 + 386034{,}23 = 387\ 555{,}29$ грн.;

$В_{тсо3} = В_3 + A_{щек3} = 2172{,}94 + 386\ 686{,}11 = 388\ 859{,}05$ грн.;

$В_{тсоΣ} = В_{тсо1} + В_{тсо2} + В_{тсо3} = 385\ 382{,}35 + 387\ 555{,}29 + 388\ 859{,}05 = 1\ 161\ 796{,}69$ грн.

Результати обчислень заносимо в табл. 10.5.

Розраховуємо на кожен рік накопичений показник вигод при оптимізації показника *ТСО* та щорічні збереження за формулами (10.9). Маємо послідовно:

$В_{нак\ 1} = 385\ 382{,}35$ грн.;

$В_{нак\ 2} = 385\ 382{,}35 + 387\ 555{,}29 = 772937{,}64$ грн.;

$В_{нак\ 3} = 772937{,}64 + 388\ 859{,}05 = 1\ 161\ 796{,}69$ грн.

Результати обчислень заносимо в табл. Б.3.

Розраховуємо на кожен рік та в цілому грошовий потік *CF* за формулою (10.10). Маємо послідовно:

$CF_1 = B_{тсо1} - C_{впр1} = 385\ 382{,}35 - 3500 = 381\ 882{,}35$ грн.,

$CF_2 = B_{тсо2} - C_{впр2} = 387\ 555{,}29 - 45\ 000 = 342\ 555{,}29$ грн.,

$CF_3 = B_{тсо3} - C_{впр3} = 388\ 859{,}05 - 45\ 000 = 343\ 859{,}05$ грн.,

$CF_Σ = CF_1 + CF_2 + CF_3 = 385\ 382{,}35 + 342\ 555{,}29 + 343\ 859{,}05 = 918\ 296{,}69$ грн.

Результати обчислень заносимо в табл. 10.5.

Розраховуємо на кожен рік накопичений грошовий потік $CF_{нак}$ за формулою (10.11). Маємо послідовно:

$CF_{нак1} = В_{нак1} - C_{нак1} = 385\ 382{,}35 - 153\ 500 = 231\ 882{,}35$ грн.;

$CF_{нак2} = В_{нак2} - С_{нак2} = 772\ 937{,}63 - 198\ 500 = 574\ 437{,}63$ грн.;

$CF_{нак3} = В_{нак3} - С_{нак3} = 1\ 161\ 796{,}69 - 243\ 500 = 918\ 296{,}69$ грн.

Таблиця 10.5 - Розрахунок оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової АТС

№ п.п	Показники	Початкові витрати, грн.	Роки			
			1	2	3	Всього, грн.
1	Витрати на впровадження, $C_{впр}$	150 000	3 500	45 000	45 000	243 500
2	Накопичені витрати проекту впровадження, $C_{нак}$	150 000	153 500	198 500	243 500	-
3	Накопичений чистий грошовий потік *(NPV)*	22 500	-	-	-	-

	витрат на проект впровадження, $NPV_в$					
4	Поточний показник *TCO,* $TCO_п$	-	8 794,58	8 794,58	8 794,58	26 383,74
5	Цільовий показник *TCO,* $TCO_ц$	-	6 621,64	6 621,64	6 621,64	19 864,92
6	Фактичний показник *TCO,* $TCO_ф$	-	8 359,99	7 273,52	6 621,64	22255,15
7	Вигоди при оптимізації показника *TCO,* В	0	434,59	1521,06	2172,94	4128,59
8	Показник очікуваних втрат $A_{втр}$	0	462 715	462 715	462 715	1 388 145
9	Ефективність системи корпоративного захисту, *E*	-	85%	85%	85%	-
10	Величина щорічної економії, $A_{щек}$	0	384 947,76	386 034,23	386 686,11	1 157 668,1
11	Показник вигод при оптимізації показника *TCO* та щорічної економії, $В_{тсо}$	0	385 382, 35	387 555,29	388 859,05	1 161 796,69
12	Накопичений показник вигод при оптимізації показника *TCO* та щорічної економії, $В_{нак}$	0	385 382, 35	772 937,64	1 161 796,6 9	-
13	Грошовий потік, *CF*	- 150 000	381 882,35	342 555,29	343 859,05	918 296,69
14	Накопичений грошовий потік, $CF_{нак}$	- 150 000	231 882,35	574 437,63	918 296,69	-
15	Накопичений чистий грошовий потік *(NPV)* доходів впровадження $NPV_д$	- 37 500	-	-	-	-
16	Внутрішня норма прибутковості, *IRR*	18,5%	-	-	-	-

Розраховуємо *NPV* – накопичений чистий грошовий потік витрат на проект впровадження та доходів від проекту впровадження за формулою (10.12). Ставка дисконтування у цій формулі приймається за $r = 25\%$. Це дасть можливість обчислити далі внутрішню норму прибутковості. Отриманий результат розрахунку *NPV* = - 150 000 * 0,25 = - 37 500 грн. заносимо в табл. 10.5.

Розраховуємо *IRR* – внутрішню норму прибутковості. Розрахунок проводиться графічним способом. На графіку будується пряма, яка з'єднує точку накопиченого чистого грошового потоку витрат на проект ($NPV_в$) при ставці дисконтування $r = 15\%$ з точкою, яка відповідає накопиченому чистому грошовому потоку доходів (відвернутих витрат) від проекту впровадження – $NPV_д$ при ставці дисконтування $r = 25\%$.

Точка, де пряма перетинає вісь абсцис є внутрішньою нормою прибутковості. Прибутковість тут має значення відвернутих збитків, які могли б бути за відсутності системи інформаційної безпеки. З рис. 10.2 випливає, що

Грн. ----------

IRR = 18,5%. При ставці дисконтування 18,5% поточна вартість очікуваних відвернутих збитків буде дорівнюватися поточній вартості необхідних грошових вкладень.

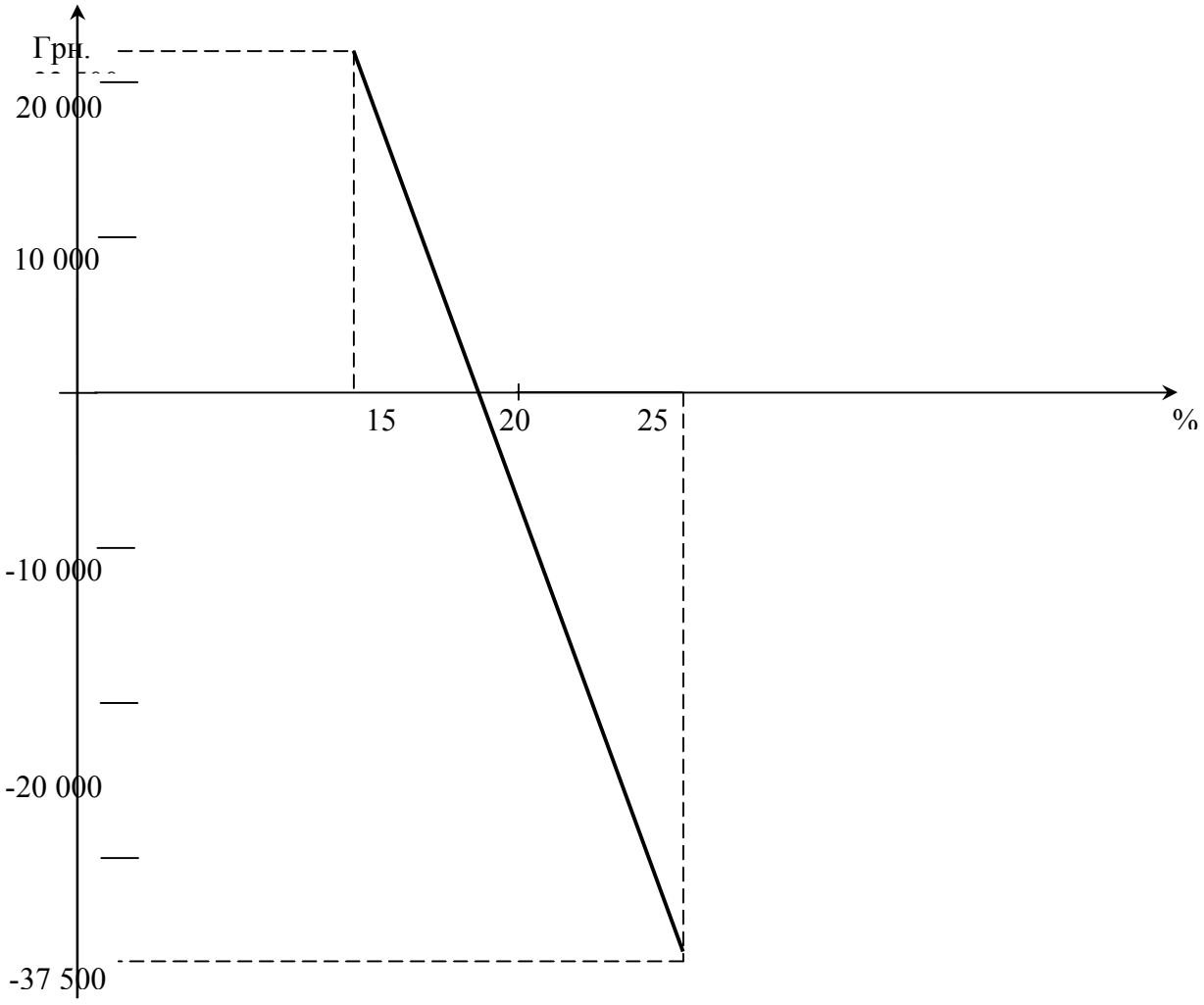


Рисунок 10.2 – Внутрішня норма прибутковості

Коментарі до економічних понять та методики обґрунтування

Суть поняття „дисконтування” пов'язано з тим, що гроші мають нестабільну ціну. Сума їх на сьогодні або в момент їх вкладення у проект має більшу цінність ніж у майбутньому, або навпаки. Різниця між теперішньою і майбутньою цінністю грошей може бути виражена як відсоткова ставка, що характеризує відносні зміни в оцінці грошей за певний період.

На коригування початкових вкладень на цю ставку або доходів, одержаних від них, впливає процес дисконтування грошових потоків. В нашому випадку під „доходами” розуміють відвернуті збитки, які мали б місце за відсутності системи інформаційної безпеки.

Норма дисконту (або мінімальний коефіцієнт окупності) має дорівнювати фактичній ставці відсотка за довгостроковими позичками на ринку капіталу або ставці відсотка (вартості капіталу), що сплачується одержувачем позички.

Норма дисконту повинна бути мінімальною нормою прибутку, нижче якої підприємцю невигідно вкладати кошти в інвестиції.

Чистий дисконтований доход або чиста сучасна вартість – це сучасна вартість майбутніх чистих грошових потоків, дисконтована на рівень граничної вартості капітальних вкладень. Нульове її значення вказує на те, що надходжень від інноваційного проекту достатньо для того, щоб відновити вкладений в інновації капітал (кошти) і забезпечити мінімально необхідний рівень доходності від цього вкладення.

Чистий дисконтований доход визначається як різниця між усіма річними дисконтованими припливами і відтоками реальних грошей, що накопичуються протягом життя проекту, або між дисконтованими на створення і впровадження інновацій витратами та доходами від їхнього використання.

Якщо чиста сучасна вартість інноваційного проекту позитивна, проект заслуговує визначення щодо його реалізації.

Внутрішня норма прибутковості – це норма дисконту, де для неї дисконтована вартість чистих надходжень від проекту дорівнює дисконтованій вартості інвестицій, а різниця між ними дорівнює нулю.

При розрахунках його випробовується кілька норм дисконту до тих пір, поки не буде знайдено той його рівень, за яким чистий дисконтований дохід дорівнюватиме нулю. Пошук її норми прибутковості здійснюється ітеративним методом. Якщо чиста поточна вартість грошових потоків позитивна, слід використовувати з цією метою більш високу ставку дисконтування, щоб зрівняти поточну вартість доходів і вкладень у проект.

Економічні аспекти впровадження системи інформаційної безпеки. Інноваційні інвестиції вкладення економічних ресурсів у систему інформаційної безпеки та їх впровадження з метою створення й одержання чистої вигоди на окремому господарському об'єкті господарювання.

Вигоди від використання системи інформаційної безпеки виявляються у вигляді відвернутих збитків, доходів підприємств, які надають послуги з захисту інформації, соціально-економічних та інших переваг.

Потік реальних грошей, за допомогою якого здійснюється оцінка вигоди від впровадження системи інформаційної безпеки, це відвернення платежів за збитками, або платежу (відтік реальних грошей як наслідок ефективного чи неефективного використання системи).

Якщо протягом певного періоду відвернуті збитки перевищують витрати, можна говорити про позитивні грошові потоки (positive cash flows). Якщо витрати перевищують відвернуті збитки – мають місце чисті витрати (net expenditure) або відтоки грошових коштів (cash outlay). Уся серія грошових потоків, зв'язаних з інноваційним проектом, є потоком грошових коштів (flow stream).

Для виявлення вихідних даних, особливо потенціальної можливої вигоди проекту, необхідна тісна взаємодія підприємств-замовників з розробниками технологій інформаційної безпеки та систематичне проведення моніторингу стану інформаційної безпеки з метою накопичення статистичних даних про загрози, атаки, величину збитків від атак та ефективності системи захисту.

Контрольні запитання та завдання

1. За якими категоріями поділяють витрати на інформаційну безпеку?
2. Пояснить взаємозв'язок між витратами на інформаційну безпеку та досягнутим рівнем захищеності?
3. Що мається на увазі під точкою економічної рівноваги?
4. У чому сутність методичних основ обґрунтування доцільності витрат на запровадження системи інформаційної безпеки?
5. За якою формулою розраховується наступний показник $A_{щек}$?
6. Як розраховується показник $A_{втр}$?
7. За якою формулою розраховується накопичений чистий грошовий потік доходів (відвернутих витрат) від проекту впровадження?
8. Сутність поняття „дисконтування"?

Завдання до самостійної роботи

У відповідності до обраного варіанту розрахувати оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки.

Розрахунок показника очікуваних втрат розраховується студентом самостійно.

Розрахунок показника очікуваних втрат

№ пп.	Потенціальні загрози	Частота виникнення, f	Втрати, грн., L	Втрати, %	$A_{втр}$, грн.
1	2	3	4	5	6
1	Саботаж				
2	Проникнення у систему				
3	Атаки на ПЕОМ управління				
4	Помилки в роботі з базою даних				
5	Телефонне шахрайство				
6	Неавторизований доступ				
7	Крадіжка обладнання і програм				
8	Фінансове шахрайство				
9	Помилки в роботі мережі сигналізації, синхронізації та керування				
10	Крадіжка приватної інформації				
11	Віруси				
12	Всього				

Варіанти завдань

№ пп.	Статті витрат	Вартість, грн. Варіанти									
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
1	Витрати на купівлю ліцензії	100 000	200 000	220 000	250 000	300 000	280 000	180 000	190 000	350 000	320 000
2	Витрати на проектні роботи	5000	4500	6000	4300	4500	4000	3800	4700	5300	4400
3	Технічна підтримка (30% від вартості ліцензії щорічно)										
		11	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
1	Витрати на купівлю ліцензії	160 000	230 000	240 000	260 000	270 000	310 000	330 000	340 000	360 000	170 000
2	Витрати на проектні роботи	3800	5100	5500	6000	4700	5700	5900	4200	4600	3900
3	Технічна підтримка (30% від вартості ліцензії щорічно)										

		21	**22**	**23**	**24**	**25**					
1	Витрати на купівлю ліцензії	210 000	230 000	240 000	250 000	290 000					
2	Витрати на проектні роботи	5100	4500	6300	6100	4300					
3	Технічна підтримка (30% від вартості ліцензії щорічно)										

РОЗДІЛ 11

РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

11.1 Меоди оцінки ризиків інформаційної безпеки

Телекомунікаційні мережі стали невід'ємною частиною інформаційно-комунікаційних технологій (ІКТ), які перетворюються у фундамент економіки, його бюджетно утворюючий та системно утворюючий рушій. У той же час, як будь-яке явище прогресу, розвиток ІКТ несе за собою нові проблеми, нові ризики, нові побічні негативні явища, зокрема проблему інформаційної безпеки. Незважаючи на своє вирішальне значення для розвитку інформаційного суспільства, ІКТ виявилися слабо захищеними від зловживань, зовнішніх вторгнень, стали ареною діяльності кіберзлочинців і розквіту кібертероризму. При своєму масовому розповсюдженні і простоті використання ІКТ потерпають від внутрішніх інцидентів, зв'язаних з порушеннями персоналом регламенту використання інформаційних ресурсів. Про слабкість систем інформаційної безпеки ІКТ сьогодні свідчить статистика, наприклад, центру оперативного реагування CERT, який відслідковує всі інциденти, зв'язані з несанкціонованим вторгненням у інформаційні ресурси США (рис. 11.1.а. Кількість зареєстрованих інцидентів такого роду стало стрімко зростати починаючи з 1998 року [30]. Нові дані свідчать, що темпи зростання кількості інцидентів з інформаційною безпекою продовжують зростати. В той же час, заходи протидії не встигають за ростом числа інцидентів. Як видно з рис. 11.1.б, кількість виявлених вразливостей у системах захисту вже не зростає, стабілізувавшись на рівні 40000 за рік. Поки що у класичному протистоянні злочинності і суспільства в галузі ІКТ виграють злочинці.

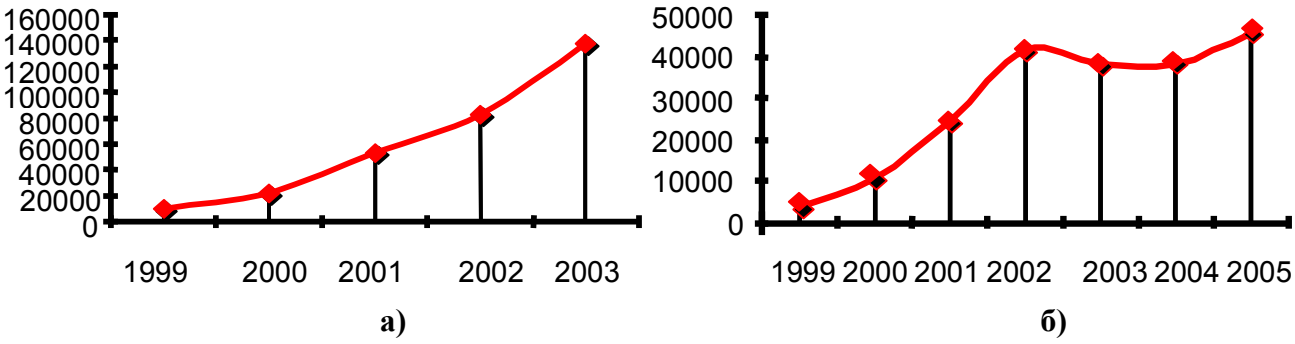


Рисунок 11.1 - Кількість зареєстрованих інцидентів зв'язаних з несанкціонованим вторгненням у інформаційні ресурси США

Україну цей процес теж буде торкатись по мірі виконання програми інформатизації і впровадження ІКТ в усі сфери життєдіяльності суспільства і держави. Ще є деякий малий проміжок часу для прийняття дієвих заходів і передбачення недоліків впровадження ІКТ.

Той факт, що кількість злочинів зростає у рази за рік, свідчить про необхідність вдосконалення існуючої системи інформаційної безпеки. Одним з дієвих способів вдосконалення систем інформаційної безпеки є страхування ризиків. Застосування його в галузі безпеки інфотелекомунікацій має свої особливості. Рішенню цієї проблеми і присвячено даний розділ навчального посібника.

Процес створення інформаційної безпеки починається з обстеження об'єкту ІКТ, де, як правило, вже склалась певна система обробки інформації, баз даних, аналізу знань, прийняття рішень. Метою етапу обстеження є отримання структури інформаційних ресурсів, класифікація, категоріювання й оцінка цінності інформації та ресурсів, які підлягають захисту, а також модель загроз інформаційним ресурсам.

Крім того, визначаються ризики інформаційної безпеки.

Під ризиком інформаційної безпеки розуміють потенційну можливість того, що загрози будуть використовувати вразливості інформаційних ресурсів і, таким чином спричиняти шкоду підприємству.

Ризик оцінюється як функція ймовірності таких подій та міри величини наслідків таких подій. В ряді випадків не існує прямих шкал для виміру певних властивостей, таких як цінність захищаємої інформації або інформаційного ресурсу.

Тоді можуть застосовуватись похідні шкали, такі як вартість відновлення ресурсу, тривалість відновлення ресурсу тощо. Часто застосовують шкали для отримання експертної оцінки, наприклад, які мають три значення:

- малоцінний інформаційний ресурс, який може бути відновлений швидко і дешево;

- ресурс середньої цінності, який може бути відновлений за час не більший за критичний, а вартість його відновлення висока;

- цінний ресурс, від якого залежать критично важливі задачі, у випадку втрати якого час на відновлення перевищує критичний або вартість відновлення якого надзвичайно висока.

При оцінці ризиків необхідно враховувати суб'єктивну точку зору власника інформаційних ресурсів, організаційні та психологічні аспекти. У простих випадках використовують оцінку ризиків по двом факторам, яка виражається формулою [136]:

$$R = P_З * B_{ВТ}, \qquad (11.1)$$

де R – величина ризику;

$P_З$ – ймовірність загрози;

$B_{ВТ}$ – величина втрат за реалізації ризику.

Тобто ризик – це оцінка математичного очікування втрат.

Можливо застосування методики оцінки ризику за трьома факторами – загрозам, вразливостям і вартості втрат.

Загрозою називають сукупність умов та факторів, які можуть стати причиною порушення цілісності, доступності, конфіденційності інформації.

Вразливість – це слабкість у системі захисту, яка робить можливою реалізації загрози.

У цій методиці ризик визначається так:

$$R = P_З * P_{ВР} * B_{ВТ}, \qquad (11.2)$$

де $P_{ВР}$ – ймовірність вразливості від даної загрози.

Цей вираз можна розглядати як математичну формулу, якщо використовуються кількісні шкали, або як формулювання загального принципу, якщо хоча б одна з шкал є якісною.

Інформаційно-комунікаційним технологіям притаманні різні вразливості, слабкі місця. Зловмисники, кінець кінцем, ці вразливості виявляють і негайно використовують для проникнення. Можна виділити такі види вразливостей і слабких місць:

- природжені, зумовлені властивостями самої технології;
- привнесенні внаслідок помилок у програмно-апаратному забезпеченні, або низької якості виконання, або апаратної чи логічної (якісної) недостатності (наприклад, завищеною ймовірністю перенавантаження);
- навмисне закладені;
- випадкові.

Привнесені, випадкові і навмисне закладені вразливості виявляються при обстеженні або експертизі системи інформаційної безпеки (СІБ). Велика складність сучасних систем принципово залишає значну кількість невиявлених помилок у програмному забезпеченні і навіть у проектних рішеннях. Тому ці вразливості продовжують виявлятись під час експлуатації систем.

Що стосується природжених вразливостей, то для боротьби з ними проводиться теоретична і практична робота. Створюються захищені комп'ютери і комп'ютерні системи, цифрові вузли комутації поставляються з вбудованими штатними системами захисту інформації, інженерні засоби захисту створюються ще під час будівництва споруд, інтенсивно просувається міжнародна стандартизація інформаційної безпеки нових систем телекомунікацій тощо.

11.2 Удосконалення системи інформаційної безпеки телекомунікаційних мереж за допомогою страхування ризиків

Отримання об'єктивних оцінок ризиків актуальне для страхових агентств, які займаються страхуванням інформаційних ризиків. На практиці, страхові агентства використовують якісні оцінки. Прості методики, без довготривалого і дорогого обстеження, дозволяють віднести інформаційно-телекомунікаційну систему до тієї чи іншої групи ризику на основі інтерв'ю з посадовими особами. В таких методиках фіксуються і аналізуються побічні фактори.

При страхуванні ризиків інформаційної безпеки телекомунікаційних мереж необхідно оцінювати ті ризики, які залишаються після впровадження системи захисту. Це змушує оцінювати параметри і властивості впроваджених заходів захисту.

На етапі проектування розробляється глобальний проект СІБ, що відповідає вимогам технічного завдання. Під час будівництва створюється СІБ і актуалізується політика безпеки, яка розповсюджується на елементи ІКТ, засоби і заходи захисту, персонал і керівництво. Відповідальним етапом є тестування створюваної СІБ. Тестування проводиться не на реальній інформації, а на тестових інформаційних ресурсах. Після здачі СІБ в експлуатацію проводиться державна експертиза на відповідність вимогам чинних в Україні нормативно-правових документів системи технічного і криптографічного захисту. Якщо в процесі проектування та створення СІБ були допущені помилки, або виникли нові загрози, то може виникнути потреба у повторенні попередніх етапів.

При позитивній експертизі на об'єкті ІКТ дозволяється обробка реальної інформації і наступає період експлуатації СІБ, який описується локальною частиною алгоритму побудови СІБ. Цю частину алгоритму можна назвати алгоритмом використання СІБ, який є циклічним і має вигляд як на рис. 11.2.

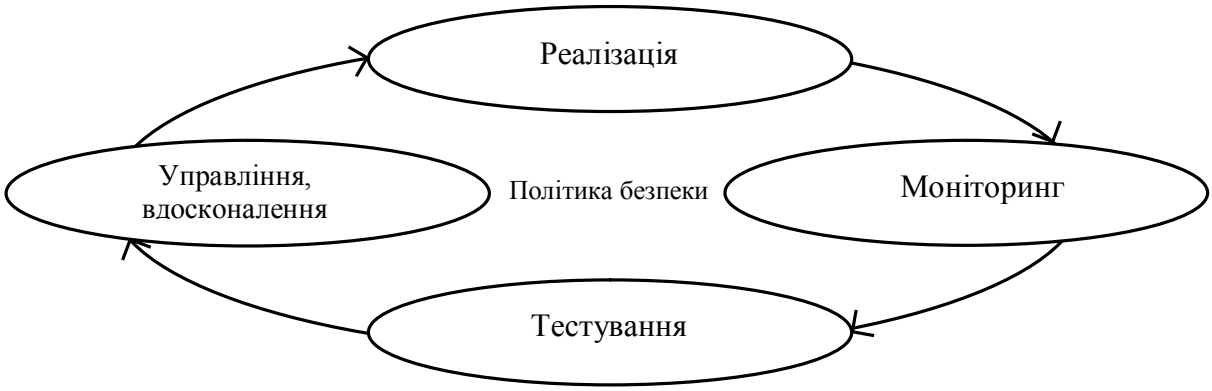


Рисунок 11.2 – Алгоритм використання системи інформаційної безпеки

На етапі експлуатації СІБ політикою безпеки передбачається проведення моніторингу інформаційної безпеки, управління інформаційною безпекою, аудиту та інших заходів, які забезпечують контроль стану і рівня захищеності інформаційних ресурсів та виявлення нових загроз. При зменшенні рівня захищеності або виявленні нових загроз, що виникли під час експлуатації, а також при змінах та при вдосконаленні самої ІКТ має бути прийняте рішення на доробку чи вдосконалення СІБ.

Сучасні інформаційні системи безперервно розвиваються. Складну систему доводиться поділяти або на ієрархічні рівні і/або на більш прості системи і створювати СІБ для кожної системи окремо. При цьому необхідно враховувати *основне теоретичне положення інформаційної безпеки складної системи*, а саме безперервності захисту у часі (за етапами життєвого циклу), просторі (за елементами мережі) і множині загроз (та вразливостей і слабких місць). Відомо, що рівень захищеності системи визначається найменш захищеною ланкою і не може бути вищим рівня захищеності цієї ланки.

Така ж ситуація виникає у порівняно нескладних ситуаціях взаємодії декількох суб'єктів економічних відносин, за яких використовуються ІКТ. Електронна бізнес-співпраця може бути представлена схемою на рис. 11.3

[140], яка наглядно показує сутність бізнес-процесів і полегшує аналіз бізнес-інформації. Кожен з партнерів бізнес-співпраці у часі розробки і у часі виконання процесу володіє і обробляє певний обсяг інформації, частина якої стає спільною, і використовує певні інформаційні ресурси. Кожен з партнерів повинен забезпечити необхідний (чи базовий, по домовленості) рівень інформаційної безпеки і бажано контрольований незалежним органом (наприклад державою). Цей рівень має бути забезпечений однаковим, як для власних, так і для спільних ресурсів. Будь-який власний ресурс може стати спільним і навпаки. З іншого боку, СІБ може не розрізняти інформаційні ресурси за властивістю їх власності. Втрати можуть понести всі партнери, хоча несанкціонований витік інформації допущений лише в одному місці. Хоча в даному випадку витік інформації може допустити нечесний партнер-зловмисник.

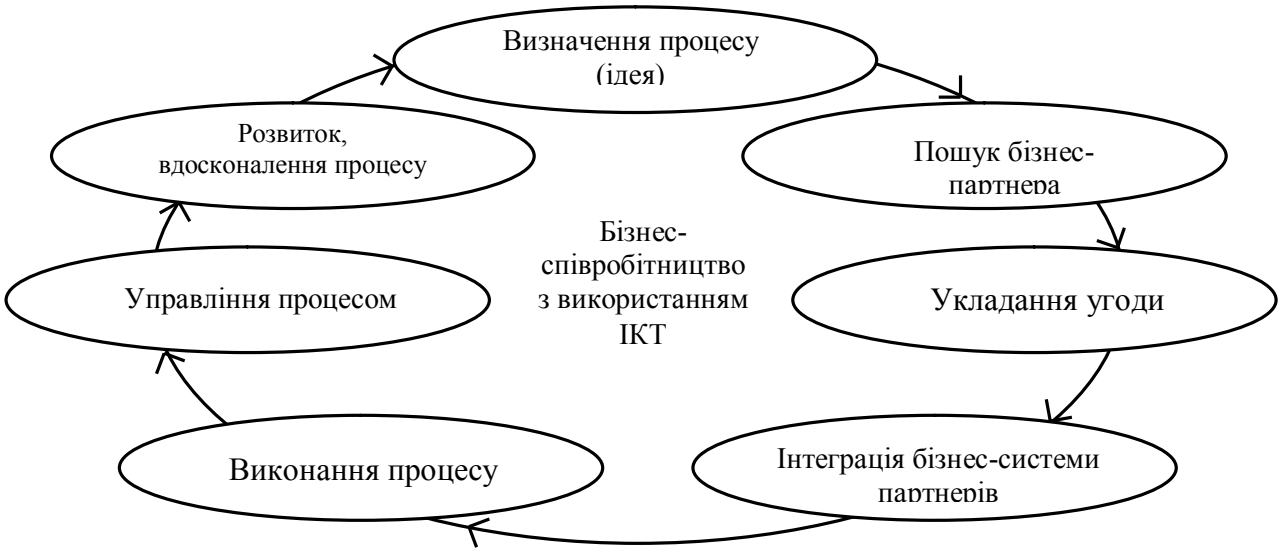


Рисунок 11.3 – Електронна бізнес-співпраця

Щоб стабілізувати рівень злочинності в ІКТ, доцільно забезпечити всіма суб'єктами взаємовідносин однаковий рівень інформаційної безпеки, не нижчий деякого базового. Встановлювати рівень інформаційної безпеки значно вищим, ніж базовий, при взаємодії з іншими учасниками, недоцільно, бо результуюча захищеність все одно не буде вище базового рівня. В умовах руху країни до інформаційного суспільства, забезпечення базового рівня інформаційної безпеки всіх без винятку суб'єктів інформаційних відносин та безпеки інформаційних ресурсів стає загально державною задачею, від вирішення якої залежить безпечність, ефективність і надійність ІКТ. Всі суб'єкти взаємовідносин в державі повинні нести певні витрати на забезпечення інформаційної безпеки.

Вибір допустимого рівня залишкового ризику зв'язаний з витратами на реалізацію системи інформаційної безпеки. Витрати на інформаційну безпеку повинні знаходитись у розумних межах і не перевищувати 5-15% коштів, які

витрачаються на підтримання роботи інформаційно-телекомунікаційної системи.

Чим вищий буде базовий рівень інформаційної безпеки на всіх об'єктах інформаційної діяльності, тим на меншому рівні стабілізується кількість злочинів. Повністю ліквідувати злочинність не можливо. З психологічних досліджень відомо, що 10 – 15% людей не скоять злочину ні при яких обставинах. Але є і 10% людей які будуть намагатись скоїти злочин, навіть усвідомлюючи невідворотність покарання. Ці люди будуть наполегливо шукати і будуть штучно створювати вразливості ІКТ, щоб їх використати в своїх злочинних цілях. СІБ, як і правоохоронні органи, повинні планомірно і надійно залатати всі „дірки", вразливості і слабкі місця в інформаційній безпеці ІКТ.

Ефективність створеної СІБ залежить, в значній мірі, від якості проведення обстеження об'єкту ІКТ, формування вимог до СІБ і, особливо від оцінки цінності інформації та інших інформаційних ресурсів, які підлягають захисту. Визначення цінності інформаційних ресурсів є найважливішим але й найбільш неоднозначним, нечітким, суб'єктивним, а тому є слабким місцем класичного підходу до інформаційної безпеки. Такий недолік зв'язаний з недосконалістю нинішніх уявлень про цінність інформації. Саме поняття інформації ще не осмислено остаточно ні у філософському, ні у науково - прикладному планах. Достатньо обґрунтованих критеріїв цінності інформації поки що не знайдено. Теоретичні критерії Хартлі, Шенона, Харкевича, Колмогорова тощо відносяться до випадків статистичної цінності інформації і в практиці обробки реальної інформації їх застосовувати важко. Одним із методів визначення цінності інформації є розрахунки величини збитку внаслідок реалізації загроз, або розрахунки початкових ризиків інформаційної безпеки. Ці та інші практичні методи характеризуються такими особливостями, які можна вважати недоліками:

- засобами обробки інформації є інша інформація (програми) і підходи до оцінки різних видів інформації можуть бути різними;
- одні види інформації можна оцінити кількісно, іншу лише якісно, застосовуючи якісні шкали та експертні методи оцінки.
- кожен вид інформації може оцінюватись багатосторонньо. За одними критеріями цінність інформації може бути більшою, а за іншими – меншою.

Для усунення вказаних недоліків пропонується новий підхід до інформаційної безпеки. Суть підходу полягає в тому, що для складних систем, із великою кількістю потоків інформації різних категорій, спочатку визначається доля витрат на інформаційну безпеку. Величина цієї долі витрат залежить від необхідного рівня захищеності і визначається на базі теорії і за аналогією з розподілом витрат у практично реалізованих СІБ. На сьогодні в середньому витрати на інформаційну безпеку становлять 10 – 15% від загальних витрат. При цьому, чим більший обсяг капіталу чи обороту, тим більша доля витрат на інформаційну безпеку. Відомо, що конфіденційність інформації має тенденцію до підвищення при збільшенні обсягів цієї інформації (даних). Виділивши необхідну долю витрат на інформаційну безпеку всієї ІКТ, проводять розподіл їх за окремими об'єктами ІКТ, враховуючи їх критичність з

точки зору захисту інформації. Далі на кожному з об’єктів застосовують процедури з метою ефективної побудови СІБ при заданих ресурсах.

В результаті побудови СІБ буде реалізований певний (імовірно достатній) рівень захищеності інформаційних ресурсів і буде деякий залишковий ризик. Обмежені кошти не дають можливості досягти абсолютного захисту. Та це неможливо і теоретично. СІБ знижує початковий ризик інформаційної безпеки до певного залишкового ризику. Для підвищення ефективності такого рішення застосовується страхування залишкового ризику.

Ясно, що *стратегії страхування залишкового ризику* мають бути різними у перехідний період і у період стабілізації ситуації з інформаційною безпекою. У перехідний період страхова система повинна враховувати умови різкого зростання кіберзлочинності і обирати відповідну стратегію. Предмет страхування в цих умовах є динамічний, постійно змінюваний. Подолання росту кіберзлочинності, стабілізація числа кіберзлочинів на певному рівні дасть змогу застосовувати типові схеми страхування ризиків.

На нашу думку, новий підхід не заперечує і не відміняє класичний, а застосовуються у випадках складних ІКТ та наявності багатьох взаємодіючих об’єктів. Новий підхід застосовується для визначення витрат на інформаційну безпеку комплексно для всієї складної ІКТ, яка використовується взаємодіючими об’єктами. Після розподілу витрат за об’єктами застосовується класичний підхід, дещо скоригований, для створення СІБ на кожному з взаємодіючих об’єктів.

Підбиваючи підсумки, можна зробити наступні висновки:

- необхідно забезпечити базовий (можливо однаковий) рівень безпеки всіх суб’єктів і об’єктів взаємодії, які використовують ІКТ;
- не захист інформації – тобто неприйняття заходів забезпечення базового рівня інформаційної безпеки – слід розглядати як злочин проти суспільства;
- класична процедура має застосовуватись, як і раніше, для створення СІБ на кожному об’єкті окремо з метою досягнення максимальної ефективності виділених коштів.

Страхування інформаційних ризиків телекомунікаційних мереж може бути ефективним при наявності розвинутої системи інформаційної безпеки усіх без винятку її частин. Стратегії застосування страхування інформаційних ризиків залежать від такого негативного явища, як темпи росту числа кіберзлочинів і перспектив його стабілізації.

Контрольні запитання та завдання

1. Як залежить від часу кількість зареєстрованих та попереджених інцидентів, зв'язаних з несанкціонованим вторгненням у інформаційні ресурси?
2. Що мається на увазі під „вразливістю" та які види вразливостей існують?
3. Поясніть алгоритм використання системи інформаційної безпеки. З яких етапів складається цей алгоритм?
4. Поясніть схему електронної бізнес-співпраці та сутність бізнес-процесів і аналізу бізнес-інформації.
5. Що є механізмами забезпечення інформаційної безпеки? Поясніть суть кожного з механізмів інформаційної безпеки.
6. Наведіть основне теоретичне положення інформаційної безпеки складної системи.
7. Що розуміють під ризиком інформаційної безпеки?
8. За якою формулою оцінюються ризики втрати конфіденційної інформації?
9. Яку роль відіграє страхування залишкового ризику інформаційної безпеки?
10. Які можуть бути стратегії страхування залишкового ризику?

Від яких факторів залежить ефективність системи інформаційної безпеки?

Завдання до самостійної роботи

1. Проаналізуйте можливості і запропонуйте заходи для зменшення числа скоєних кіберзлочинів чи хоча б стабілізації їх числа на прийнятному рівні.
2. На Вашу думку, ефективно чи ні проводити страхування інформаційних ризиків телекомунікаційних мереж? Обґрунтуйте вашу відповідь.

РОЗДІЛ 12

ОРГАНІЗАЦІЯ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

12.1 Організація служби інформаційної безпеки підприємства

Значення інформації на сучасному етапі розвитку людства безумовно важливе. Інформація сьогодні уже розглядається не тільки, як спосіб одержання різних відомостей, але й як продукт продажу. Тому проблема її збереження постала дуже гостро. А особливо це стосується інформації з обмеженим доступом, яка може бути віднесена до комерційної та державної таємниці.

Проблема захисту інформації та несанкціонованого доступу до неї прийняла антагоністичний характер в постановці, відомій із теорії гри. Стосовно проблеми захисту інформації це означає, що для її рішення необхідна не просто розробка окремих механізмів захисту, а організація цілого комплексу заходів захисту в широкому розумінні цього питання, таких як використання спеціальних засобів, механізмів і заходів з метою попередження втрати інформації.

Аналіз стану справ в області захисту інформації показує, що у розвинутих країнах склалася достатньо сформована концепція та інфраструктура захисту, основу якої складають:

- дуже розвинутий арсенал технічних засобів захисту, які створюються на промисловій основі;
- значна кількість фірм, які спеціалізуються на вирішенні питань захисту інформації;
- досить чітка система концептуальних поглядів на цю проблему;
- наявність значного практичного досвіду.

Але безумовно, як засвідчує зарубіжна преса, загрози для інформації не тільки не зменшуються, але й мають досить стійку тенденцію до зростання.

Основні концептуальні положення комплексної системи безпеки інформації організації. Досвід показує, що для боротьби з цією тенденцією необхідна чітка та цілеспрямована організація процесу захисту. Для цього необхідно активно залучати професійних спеціалістів, керівництво організацій, співробітників і користувачів. Ці факти визначають підвищену значимість організаційної суті питання.

Забезпечення інформаційної безпеки не може бути одноразовим актом. Це безперервний процес, який зводиться до обґрунтування та реалізації найбільш раціональних методів, способів і шляхів удосконалення та розвитку системи захисту, безперервному контролі, виявленні її слабких місць та можливих каналів витоку інформації.

Інформаційна безпека може бути забезпечена тільки при комплексному використанні усього арсеналу засобів захисту у всіх структурних елементах виробничої системи і на усіх етапах обробки інформації. Найбільший ефект досягається тоді, коли усі засоби, методи та заходи об’єднуються в єдиний

комплекс - комплексну систему інформаційної безпеки організації (КСІБ). При цьому функціонування системи захисту повинно контролюватись, поновлюватись та доповнюватись в залежності від зміни зовнішніх і внутрішніх умов.

Ніяка КСІБ не може забезпечити необхідного рівня забезпечення інформаційної безпеки без належної підготовки користувачів і виконання ними усіх встановлених правил, направлених на захист інформації.

КСІБ можна *визначити* як організовану сукупність спеціальних органів, засобів, методів і заходів, які забезпечують захист інформації на підприємстві.

З позиції системного підходу до захисту інформації установлюються такі вимоги, захист інформації повинен бути:

- неперервним,
- плановим,
- централізованим,
- цілеспрямованим,
- активним,
- надійним,
- універсальним,
- комплексним.

Основні вимоги до КСІБ:

- чіткість визначених повноважень і прав користувачів щодо доступу на певні види інформації;
- надання користувачу мінімальних повноважень, необхідних йому для виконання дорученої роботи;
- зведення до мінімуму кількості загальних для декількох користувачів засобів захисту;
- облік випадків і спроб несанкціонованого доступу до конфіденційної інформації ;
- забезпечення оцінки ступеня конфіденційності інформації;
- забезпечення контролю цілісності засобів захисту.

Надійність функціонування КСІБ також не можлива без постійного контролю за роботою її складових елементів.

Контроль КСІБ має за мету:

- своєчасно виявити та закрити потенційні канали витоку інформації;
- встановити відповідність змісту запланованих і проведених заходів по забезпеченню інформаційної безпеки системи вимогам розроблених інструкцій, пам’яток і інших документів;
- визначити правильність організації робіт із забезпечення інформаційної безпеки і ступінь їх виконання;
- визначити ступінь підготовки органів безпеки до виконання поставлених перед ними завдань, персоналу підприємства – з питань розробки, зберігання, обліку та роботи з документами, які вміщують конфіденційну інформацію, та офісним обладнанням;

- узагальнити досвід організації та проведення заходів з питань забезпечення інформаційної безпеки для використання його в процесі удосконалення системи безпеки;

- перевірити організацію і результати роботи з удосконалення системи санкціонованого доступу на підприємство, організацію допуску персоналу до конфіденційної інформації;

- перевірити участь керівників структурних підрозділів підприємства в організації та забезпеченні виконання заходів із забезпечення інформаційної безпеки.

КСІБ, як і будь-яка інша система, повинна мати певні *види забезпечення*, спираючись на які вона буде спроможна виконати свою цільову функцію.

З врахуванням цього КСІБ повинна мати:

- правове забезпечення (нормативні документи);

- організаційне забезпечення (наявність спеціальних служб: захисту документів; служби режиму, допуску та охорони; служби захисту інформації з допомогою технічних засобів тощо);

- апаратне забезпечення (технічні засоби захисту інформації);

- інформаційне забезпечення (інформацію для забезпечення роботи служби безпеки);

- програмне забезпечення (програми захисту та оцінки наявності каналів витоку інформації);

- математичне забезпечення (математичні заходи розрахунку загроз від технічних засобів розвідки, зон та норм необхідного захисту);

- лінгвістичне забезпечення (спеціальні мовні засоби спілкування спеціалістів та користувачів в сфері захисту інформації);

- нормативно-методичне забезпечення (методики, які забезпечують діяльність користувачів в умовах жорстких вимог захисту інформації).

КСІБ може бути охарактеризована рядом показників, які визначають її організаційну і функціональну структуру. До таких характеристик можна віднести спрямованість захисту, спосіб попередження несанкціонованого доступу до інформації, масштабованість системи, часові характеристики впливу за ступенем активності.

Найбільш важливою характеристикою КСІБ є направленість захисту. Розглядаються також такі напрямки захисту як правовий, організаційний і інженерно-технічний захист. Останній реалізується фізичними, апаратними та програмними засобами та математичними методами захисту.

Вирішальна роль людського фактору в системі збереження державної та комерційної таємниці. Незалежно від того, на скільки добре розроблена та впроваджена КСІБ, вона в решті-решт ґрунтується на людській діяльності, в якій можливі помилки або свідомі дії, направлені на знищення інформації, або передачу її зацікавленим організаціям.

Неможна, також, не відзначити, що сьогодні, як і завжди між державами світу йде постійна боротьба за сфери своїх інтересів. І методи цієї боротьби різноманітні, починаючи від дипломатичної діяльності і закінчуючи збройними конфліктами.

Велику актуальність сьогодні мають методи „психологічної війни”.

Відомо, що завданнями психологічної війни є вплив на особу, як носія інформації та як основну ланку в системах управління різноманітного призначення.

Таким чином, особа сьогодні може розглядатися як основний об’єкт атаки нетрадиційними методами ведення війни. Тому на сучасному етапі розвитку методів і засобів захисту інформації, одним із головних напрямків необхідно виділити процес виявлення і оперативної ліквідації загроз для інформації, які можуть виникати в процесі діяльності персоналу установ і організацій.

Ніяка технічна система безпеки не забезпечить надійний захист інформації, якщо хтось із персоналу установи буде свідомо здійснювати її несанкціоноване копіювання, або навмисне пошкодження.

Відомо багато методів впливу на особу з метою одержання від неї потрібної інформації, які завжди активно використовуються зацікавленими сторонами. Методи впливу:

- підкуп;
- шантаж;
- загрози;
- одержання потрібної інформації при веденні звичайної розмови;
- обмін інформацією;
- переконання;
- використання психологічних методів;
- впровадження співробітником організації "своєї людини".

Усі ці факти свідчать, що для створення та надійного функціонування усіх елементів КСБІ, забезпечення кадрової безпеки організації (банку, підприємства) повинен бути створений спеціальний структурний підрозділ - служба безпеки.

Варіант організації штатної структури служби безпеки організації. Для організацій України, що проводять роботу з інформацією, яка становить державну таємницю, статус служб безпеки, їх підпорядкованість, основні обов’язки та права співробітників визначені Постановою КМУ № 609 від 4 серпня 1995 року.

Враховуючи досвід діючих режимно-секретних органів (РСО) в установах України, а також зарубіжний і вітчизняний досвід по створенню і організації діяльності служб безпеки для недержавних установ, пропонується приблизний варіант її організаційно-штатної структури.

Служба безпеки організації повинна підпорядковуватись безпосередньо керівнику установи, а керівник служби повинен бути заступником керівника організації.

До складу служби безпеки можуть входити структурні підрозділи по збору інформації та контролю за її використанням, підрозділи технічного захисту інформації та підрозділи охорони. Запропонована організаційна структура служби безпеки наведена на рис. 12.1.

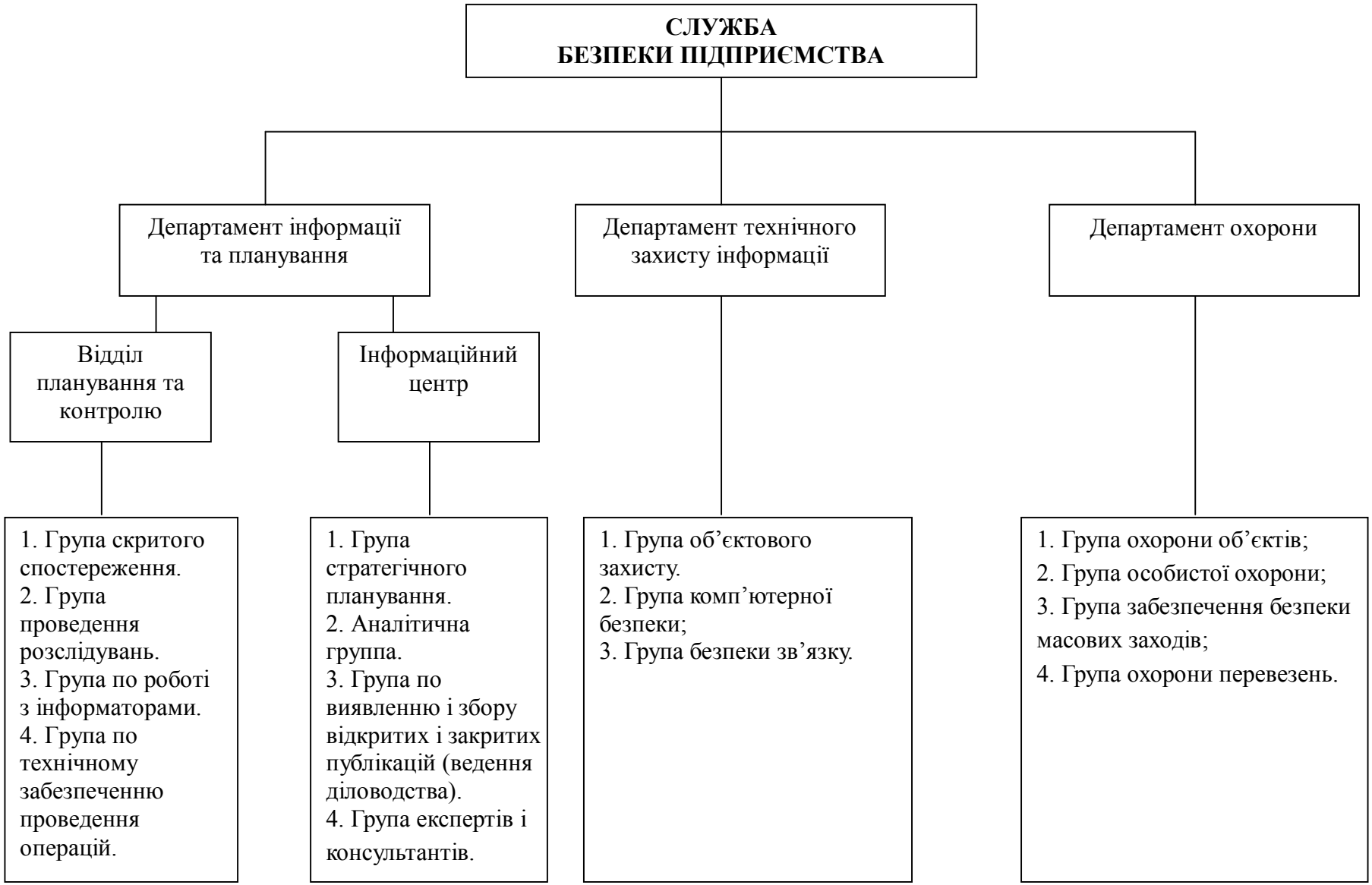


Рисунок 12.1 - Організаційна структура служби безпеки підприємства

У склад підрозділів служби безпеки входять: департамент інформації та планування, департамент технічного захисту інформації, департамент охорони.

Департамент інформації та планування:

Відділ планування та контролю:

Склад:

Група прихованого спостереження;

Група проведення розслідувань;

Група по роботі з інформаторами;

Група по технічному забезпеченню проведення операцій.

Основні завдання департаменту інформації та планування:

- планування роботи із забезпечення безпеки інформації на підприємстві;
- ведення прихованого спостереження за організаціями та особами;
- проведення розслідувань фактів витоку інформації, або втрат документів;
- проведення навчання персоналу організації з питань безпеки інформації;
- проведення роботи з персоналом інших організацій-конкурентів з метою їх вербування, або переходу на роботу до своєї організації;
- проведення заходів із забезпечення безпеки інформації при використанні персональних комп'ютерів, а також при їх роботі в мережі;
- технічне забезпечення проведення різних заходів безпеки.

Інформаційний центр:

Склад:

Група стратегічного планування;

Аналітична група;

Група по виявленню і збору відкритих і закритих публікацій (ведення діловодства);

Група експертів і консультантів.

Основні завдання інформаційного центру:

- проводить оцінку зовнішніх загроз для організації та розробляє комплекс заходів по їх попередженню;
- проводить збір та аналізує інформацію в середині організації;
- проводить збір літератури та нормативних документів;
- ведення діловодства;
- проводить оцінку матеріалів.

Департамент технічного захисту інформації:

Склад:

Група об'єктового захисту;

Група комп'ютерної безпеки;

Група безпеки зв'язку.

Основні завдання департаменту технічного захисту інформації:

- проводить встановлення та забезпечує функціонування технічних засобів охорони будівель та приміщень організації;

- проводить заходи по забезпеченню безпеки інформації при використанні персональних комп'ютерів, а також при їх роботі в мережі;

- проводить заходи по забезпеченню безпеки інформації при використанні засобів зв'язку (телефон, факс тощо).

Департамент охорони:

Склад:

Група охорони об'єктів;

Група особистої охорони;

Група забезпечення безпеки масових заходів;

Група охорони перевезень.

Основні завдання департаменту охорони:

- проводить заходи з фізичної охорони та оборони будівлі та приміщень організації;

- забезпечує особисту охорону керівництво та персоналу організації;

- забезпечує охорону персоналу та майна організації при проведенні виставок, презентацій та інших масових заходів;

- забезпечує охорону перевезень майна та інших цінностей організації.

Із спеціальних питань РСО також необхідно підпорядкувати відділ кадрів установи по підбору та розстановці працівників.

Структура, чисельність і склад служби безпеки організації визначається реальними фінансовими можливостями, масштабами діяльності, ступенем конфіденційності інформації. В залежності від таких факторів склад служби безпеки може бути від двох - трьох чоловік, які працюють за сумісництвом, до повномасштабної служби з розвинутою структурою.

В умовах, коли основним об'єктом злочинних дій став капітал банків і комерційних підприємств, на перший план в діяльності їх особистих служб безпеки виходить інформаційно-аналітичне забезпечення, економічна розвідка та контррозвідка, а також організація оперативних заходів.

Сучасні вимоги до підготовки спеціалістів служби безпеки. Враховуючи сучасні вимоги до роботи співробітників служб безпеки (РСО) система підготовки, перепідготовки та підвищення їх кваліфікації повинна передбачати оволодіння знаннями додатково в областях:

- Інформаційно - аналітичної роботи.
- Методів розвідки та контррозвідки.
- Оперативної роботи.
- Соціальної психології та психології особистості.
- Основ банківської справи та бухгалтерського обліку.
- Основ менеджменту та маркетингу.
- Цивільного та кримінального права.

Спеціаліст служби безпеки організації сьогодні повинен вміти (рис. 12.2).

Наведені вимоги потрібно враховувати при організації підготовки, перепідготовки та підвищення кваліфікації спеціалістів системи інформаційної безпеки.

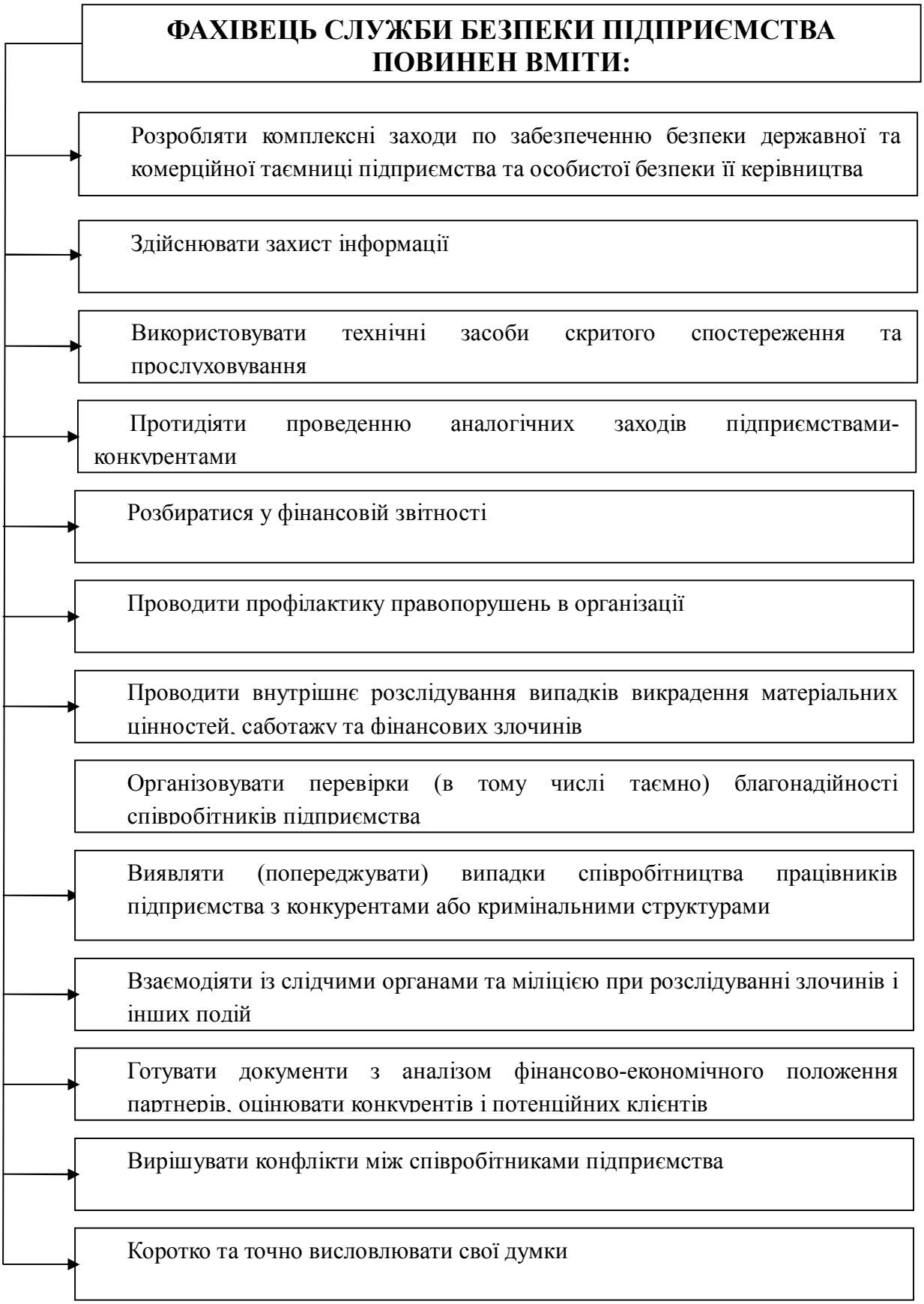


Рисунок 12.2 – Вимоги до фахівця служби безпеки

Перейдемо до ролі менеджменту персоналу у сфері інформаційної безпеки.

12.2 Менеджмент персоналу у сфері інформаційної безпеки

Проблема захисту мереж телекомунікацій та інформації, що циркулює в них, вимагає значної уваги в зв'язку з тим, що в інформаційному суспільстві, до якого прагне Україна, захист інформаційного середовища стає таким же важливим для кожного громадянина, суспільства і держави, як і захист навколишнього середовища, підприємства, власного майна.

В Україні до інформаційних ресурсів прийнято відносити технічну інфраструктуру й інформацію, що в ній обробляється, циркулює і зберігається. Недостатня увага приділяється колосальному пласту питань, який впливає на забезпечення безпеки інформаційних систем: діяльності персоналу, адміністративній та юридичній підтримці. Проблема захисту ускладнюється тим, що загрози, від яких доводитися захищати мережі та інформацію, дуже різноманітні і мають навіть різне походження: природне, техногенне, антропогенне. Однак для загроз природного, техногенного та ненавмисного антропогенного походження прогноз частково можливий, а наслідки рідко корелюються із діями або інформацією користувачів, тому рідко бувають катастрофічними. Принципи захисту від таких загроз відомі, і, як правило, їх можна реалізувати під час розробки, впровадження та експлуатації мереж телекомунікацій [167]. Ця проблема вирішувалась у багатьох суміжних областях безпеки, управління та прийняття рішень [23, 173, 207], але відносно антропогенних загроз, тобто проблеми управління персоналом системи інформаційної безпеки враховувалась мало і ця задача остаточно не вирішена. Слід відзначити, що багато питань інформаційної безпеки вже вирішуються системою технічної експлуатації, системою управління електрозв'язком, системою управління якістю та менеджменту телекомунікацій. Але це стосується в основному протидії техногенним загрозам інформаційним ресурсам. Антропогенні загрози враховуються мало. Водночас, необхідність управління персоналом тісно зв'язана із захистом комерційної таємниці фірми, тому що персонал є одним з основних носіїв інформації, і як вважають фахівці, ймовірність витоку інформації через підкуп, переманювання співробітників складає 43%, а через вивідування – 24%.

Найнепередбачуваніші загрози виникають внаслідок навмисної, особливо зловмисної антропогенної діяльності, саме захист від таких загроз найбільш складний і потребує особливої уваги при розгляді стратегії розвитку мереж телекомунікацій [167].

Питання менеджменту фахівців із захисту інформації вперше було поставлено у другій половині 60-х років. Тоді воно розглядалося тільки в площині кадрового забезпечення захисту державних секретів, оскільки комерційної таємниці ще не існувало, а захист несекретної інформації не був настільки актуальним, як сьогодні. Разом з тим поряд з продовженням існування державної таємниці з'явилась і комерційна таємниця. В міру

зростання кількості підприємств недержавного сектора збільшується й обсяг інформації, що складає комерційну таємницю. Від надійності захисту цієї інформації залежить ефективність функціонування комерційних підприємств, їх безпека і конкурентоспроможність [12].

Уразливість будь-якої системи, як правило, оцінюється найбільш слабкою ланкою. Накопичений досвід недвозначно показав, що сама слабка ланка системи інформаційної безпеки підприємства – це власні співробітники. Необачність або просто необережність, неуважність одного співробітника може звести нанівець навіть найдійовіші контрзаходи технологічного характеру. Саме тому до міжнародних і національних стандартів з інформаційної безпеки включаються цілі розділи, присвячені роботі з персоналом підприємства [42].

З початку року в Україні було розкрито понад 40 тис. економічних злочинів, які призвели до втрат у розмірі близько 1 млрд. грн. Цілісність комерційної таємниці фірми на 80% залежить від правильного підбирання, розміщення, грамотно поставленої роботи з кадрами, стабільності кадрового складу. Вирішенню цієї проблеми і присвячений даний підрозділ.

Метою вирішення цієї задачі є розробка організаційних рекомендацій управління персоналом щодо становлення системи інформаційної безпеки.

У ринковій економіці виживання є важливою задачею будь-якого підприємства. Діяльність з управління персоналом є важливою гарантією того, що підприємство буде жити і процвітати. Адже самі люди обмежують або збільшують силу і слабкість підприємства. Людина з її потребами, мотиваціями і конкретними інтересами є зараз мірою прогресу і, коли фірма дійсно піклується про людей, це обов'язково відбивається на її діяльності.

Організаційні рекомендації щодо управління персоналом системи інформаційної безпеки. Існує багато різних засобів несанкціонованого доступу до інформації. Але слід одразу ж зазначити, що ніякий окремо взятий засіб захисту не спроможний гарантувати адекватну безпеку. Надійний захист можливий лише за умови створення механізмів комплексного забезпечення безпеки. Виділяють три основні складові такого комплексу: нормативно-правові, технічні, організаційні засоби.

Більш детально зупинимося на організаційних засобах. Людина не тільки є вмістилищем інформації, вона обробляє, аналізує її, та робить необхідні висновки і діє відповідно до них. Інформацію, що їй відома, вона може легко відтворювати, копіювати і поширювати, а також одержавши лише частину інформації стати власником значно більшого її обсягу [13]. Співробітники підприємства можуть виступати, як об’єктом, так і суб’єктом загроз, спрямованих на порушення економічної стабільності підприємства. Організаційні заходи захисту мереж та інформації передбачають охорону мережі телекомунікацій, особливо її системи управління, ретельний підбір та контроль діяльності персоналу, причетного до створення, впровадження й експлуатації мережі, установлення режиму обмеженого доступу до окремих видів інформації, ретельну розробку комплектів інструкцій з технічного обслуговування і захисту мережного обладнання та інформації, регулярне інформування фахівців і керівників про чинне законодавство в сфері безпеки

телекомунікацій та інформатики, застосування дисциплінарної, адміністративної та кримінальної відповідальності при виявленні порушення безпеки мереж телекомунікацій [167].

Організаційні рекомендації управління персоналом щодо становлення системи інформаційної безпеки на підприємстві можуть бути сформовані таким чином:

1. На підприємстві повинна існувати детальна адміністративна політика по відношенню до персоналу. Ця політика повинна детально регламентувати і мінімізувати права доступу співробітників до інформації, метою політики доступу є вимоги до регламенту використання доступної інформації.

2. Адміністративна політика повинна підкріплюватися не менш детальним моніторингом дій користувачів з довіреною їм інформацією. Таким моніторингом повинні бути охоплені всі без винятку користувачі, хто має легальні права доступу до інформації, налагодження апаратури, бази даних, операційних систем.

3. Виявлена розбіжність адміністративної політики і моніторингу може означати наявність „конфлікту інтересів" підприємства та її персоналу.

4. Необхідно дотримуватись принципу „прозорості": персонал повинен ясно пояснювати усі свої дії з інформацією, які виявлені системою моніторингу.

5. Повинен існувати перелік корпоративних морально-етичних вимог, який чітко регламентує правила поведінки співробітника, що дозволяє виявити „конфлікт інтересів" і дає можливість керівництву застосувати, у разі потреби, адміністративні заходи впливу.

6. З персоналом повинна проводитися багатопланова робота, метою якої є вироблення у людей етики корпоративної поведінки та відносин до ресурсів підприємства.

Інформаційна безпека підприємства прямо зв'язана з економічною поведінкою її персоналу. В основі економічної поведінки лежать ціннісні орієнтири людей (гроші, статус, роль, ідеали). На економічну поведінку впливають різні фактори: технічний рівень виробництва, організація, нормування, оплата та умови праці, задоволення від праці, морально-психологічний клімат у колективі, освітній і культурний рівень працівника, характер суспільно-політичної активності в суспільстві та робочій групі [90].

Особливості проблеми захисту телекомунікаційних мереж та інформації пред'являють певні специфічні вимоги до персоналу, насамперед, до процесу їх діяльності з інформаційної безпеки. При підбиранні кандидатів, яким потрібно буде працювати з секретною інформацією, необхідно враховувати їх ділові, професійні, моральні якості та психологічні особливості [12].

Сформулюємо організаційно-психологічні заходи щодо забезпечення інформаційної безпеки підприємства:

1. Перевірка персоналу і регламент роботи з персоналом. Перевірка співробітників, прийнятих на постійну роботу, повинна проводитися під час подачі заяви про прийом на роботу, і повинна включати наступні етапи:

– наявність позитивних характеристик (рекомендацій) однієї, що характеризує ділову якість, а іншої – особисті якості;

– перевірку повноти і точності резюме (автобіографії) претендента на вакансію;

– підтвердження заявленого рівня освіти і професійної кваліфікації;

– незалежну ідентифікацію особистості (паспорт або йому подібний документ).

У тих випадках, коли посадові обов'язки, як при первинному виході на роботу, так і в результаті просування по службі, передбачають доступ до засобів оброблення інформації, особливо до засобів оброблення інформації з обмеженим доступом, комерційної та такої, що належить державі, – підприємство повинно також перевірити стан надійності та довіри співробітника. Співробітники, які займають відповідальні посади, повинні проходити таку перевірку регулярно [42].

2. Слід заохочувати пильність на робочих місцях, і передбачати шляхи, за допомогою яких співробітники могли б повідомляти про підозрілу діяльність.

3. Формування у співробітників почуття відповідальності за виконувану роботу і самостійності, як виконавця.

4. Співробітники повинні знати, що всі їхні дії контролюються.

Умови наймання повинні визначати обов’язки і відповідальність співробітника за інформаційну безпеку. За необхідності, така відповідальність повинна зберігатися протягом певного часу після звільнення співробітника. Повинні бути також зазначені дії, що починаються в тому випадку, якщо співробітник нехтує вимогами до інформаційної безпеки [42].

5. Впровадження діючої системи матеріальної і моральної мотивації кожному члену колективу.

6. Забезпечення участі всього персоналу, звичайно за умови, коли це є можливим, у прийнятті принципових, стратегічних рішень.

7. Дотримання політики інформаційної безпеки значною мірою є елементом корпоративної культури. Тому цими відносинами необхідно управляти.

8. Необхідне навчання і регулярна перепідготовка кадрів, як у напрямку основної діяльності, так і з питань інформаційних технологій, діловодства і безпеки.

Усі співробітники підприємства, а за необхідності, і користувачі зі сторонніх підприємств, повинні пройти навчання за регламентом і процедурами, які використовуються на підприємстві і регулярно отримувати інформацію щодо змін в них.

Така програма підготовки стосується вимог до забезпечення безпеки, питань юридичної відповідальності і засобів керування діловими процесами, а також включає навчання з правильного використання засобів оброблення інформації (наприклад, процедури входу в систему, використанню програмного забезпечення), – перш ніж буде наданий доступ до інформації та засобів її оброблення [42].

9. Розміщення кадрів відповідно до здібностей, кваліфікації, освіти, вислуги років, стану здоров’я та інших факторів, які впливають на кар’єру і на посаду персоналу.

Персонал системи інформаційної безпеки потребує особистих засобів управління. У зв'язку з тим, діяльність служби персоналу, пропонуємо поділити на чотири основних напрями:

Підбір надійних і висококваліфікованих працівників. Найчастіше пошук нових співробітників входить у коло обов'язків служби персоналу, хоча нерідко підбір здійснюється безпосередньо керівниками тих ділових підрозділів, де відкрилася вакансія. Професійні знання і навички претендента оцінюють кваліфіковані фахівці саме того підрозділу, в якому новачок буде працювати. На жаль, при цьому часто забувають переконатися в надійності людини.

При підбиранні кандидатів, яким потрібно буде працювати із секретною інформацією, необхідно враховувати їхні ділові, професійні, моральні якості та психологічні особливості. Тут важливо скласти уявлення не тільки про окремі якості і риси кандидата, а також про особистість у цілому, її світоглядних установках, інтелекті, переконаннях, ціннісних орієнтирах, здібностях до даного виду діяльності, рисах характеру [167].

Перевірка персоналу в кожному підприємстві проходить по-своєму. Великі підприємства можуть собі дозволити послуги відповідних державних структур, у той час як невеликі підприємства покладаються на досвід та інтуїцію свого керівництва і служби персоналу. Вважаємо що, ефективність перевірок знаходиться на низькому рівні і потребує удосконалення.

Захист конфіденційної інформації і персональних даних співробітників та захист інформації, що знаходиться в головах співробітників і має цінність для організації, в якій вони працюють. До захисту конфіденційної відноситься інформація, яка є цінністю підприємства: статутні документи фірми; зведені звіти за фінансової діяльності фірми; кредитні договори з банками; договори купівлі і продажу; відомості про перспективні ринки збуту і вигідних партнерів; інформація, якщо за її розголошування передбачено санкції; дані про конкурентів, їх слабкі і сильні сторони; умови фінансової діяльності; технологічні секрети; заходи, що робляться конкурентами; виявлення уразливих ланок серед співробітників; виявлення осіб, перспективних для вербування; зв'язки і можливості керівництва; виявлення кола постійних відвідувачів.

Керівники більшості наших підприємств приділяють недостатню увагу знанням і навичкам співробітників, хоча саме вони є одним із ключових інформаційних ресурсів підприємства, за час відсутності якого інші ресурси можуть стати марними. Як свідчить світовий та вітчизняний досвід, тяжкі наслідки для підприємства може спричинити перехід до конкурентів ключових співробітників, їх відсутність на робочих місцях через хворобу або з інших причин. Вважаємо що, ймовірність втрати знань, які зберігаються в головах співробітників, є серйозною загрозою інформаційної безпеки підприємства. Для зменшення рівня цієї загрози треба знижувати зацікавленість співробітників у зміні місця роботи, для чого пропонуємо:

1. Стежити за середніми рівнями заробітної плати на ринку праці, і не допускати помітного відставання рівня зарплати від середнього рівня.

2. Не забувати про моральне заохочення співробітників, про створення сприятливого клімату в колективі. Уважне і людяне відношення до співробітників не вимагає великих витрат, але найчастіше дає набагато більший ефект, ніж матеріальне заохочення.

3. Розвивати корпоративну культуру, яка включає лояльність до свого підприємства.

4. Впроваджувати програми переміщення працівників усередині підприємства тому, що талановиті працівники є джерелом конкурентної переваги підприємства.

5. Уникати ситуацій, коли співробітник стає незамінним, вчасно готувати кадровий резерв. Якщо обстановка на підприємстві сприятлива і співробітники упевнені у своєму майбутньому, в подальшому просуванні, - тоді вони, як правило, охоче передають свій досвід більш молодим колегам.

6. Детально і ретельно описувати ділові процеси та операції на всіх ділянках, оформляючи ці описи у вигляді внутрішніх нормативних документів – інструкцій. Доцільно забезпечити правильне виконання дій навіть персоналом, незнайомим з даною ділянкою роботи. Слід також прописати правила передачі повноважень і функцій відсутніх співробітників.

7. Надавати співробітникам тільки ту інформацію, яка їм необхідна для виконання службових обов'язків. Отже, по можливості, уникати ситуацій, коли співробітники мають доступ до всієї інформації з визначеного критично-важливого питання. Корисно відслідковувати, з якою особливо ціннісною інформацією співробітники були ознайомлені (так, як це робиться в секретному діловодстві).

Процес звільнення. Виходячи з аналізу діяльності служби персоналу звільнення, на нашу думку є одним з трудомістких процесів, який потребує особливої уваги при розгляді питань управління персоналом системи інформаційної безпеки. Звільнення людини, яка працює з конфіденційною інформацією, являє загрозу інформаційній безпеці підприємства. Насамперед, потрібно з'ясувати причину звільнення (за власним бажанням чи його викрито в промисловому шпигунстві, або перехід до конкурентів), спробувати визначити справжню причину його рішення, проаналізувати і вирішити чи потрібно його утримувати, чи звільнити.

Процес звільнення повинен містити відповідні етапи: написання співробітником заяви з повним розкриттям причини його рішення; організація передачі справ; здача співробітником усіх документів, ключів, пропусків; проведення інструктажу робітника, який звільняється, про зобов'язання та відповідальність за збереження таємниці конфіденційної інформації; виявлення обсягів відомої йому конфіденційної інформації (при шпигунстві – зміна всіх ключів, паролів, шифрів на конфіденційну інформацію та посилення контролю); документальне оформлення звільнення; виявлення майбутнього місця роботи.

На нашу думку треба розглядати плинність кадрів в організації. Якщо плинність вище 5%, то слід не тільки подумати про закріплення співробітників, але і звернути особливу увагу на взаємозамінність співробітників. Залишення

посади кращого співробітника завжди викликає додаткову напругу, і багато чого залежить від того, як підприємство підготовлено до цієї ситуації. Якщо робота організована так, що в підрозділах працівники можуть підмінити один одного, якщо ведеться регулярне навчання персоналу і створюється кадровий резерв, тоді залишення посади будь-якого співробітника (незалежно від причин) не призведе до збільшення наслідків.

Корисно визначити найбільш відповідальні ділові процеси на підприємстві, і простежити за тим, щоб не було фахівців – „монополістів", без яких неможливо обійтись.

На жаль, на невеликих підприємствах окрему ділянку роботи звичайно веде тільки одна людина, і є ризик втратити не тільки самого співробітника, його знання та навички (при звільненні, хворобі тощо), але і втратити контроль над цією ділянкою діяльності, тому що ніхто не зможе продовжити цю роботу.

Інша сторона проблеми полягає в тому, що в „монополістів" з'являється можливість шантажувати керівництво. Також важливо організувати навчання молодих співробітників на робочих місцях своїми старшими колегами, що можливо тільки за наявності мотивації в досвідчених працівників, коли „вчителі" знають, яку вигоду це їм принесе (підвищення по службі, передачу частини технічної роботи новому співробітникові, премію за наставництво).

Якщо за професійними якостями працівник відповідає своєму робочому місцю і робота на підприємстві задовольняє його потреби, такий працівник буде віддавати своєму підприємству максимум своїх сил, знань і здібностей. Він буде заробляти для підприємства набагато більше, ніж підприємство витратить на нього й організацію його роботи.

Але врахувати особливості й індивідуальність кожного працівника підприємства – дуже складна задача. Саме для рішення подібного роду питань виник кадровий консалтінг.

Кадровий консалтінг – це система організаційно-психологічних заходів щодо діагностики і, за необхідністю, корекції організаційної структури і/або культури підприємства з метою поліпшення виробничих показників, оптимізації соціально-психологічного клімату, посилення мотивації персоналу. Щоб підприємство працювало чітко і злагоджено, щоб фахівці віддавали роботі максимум сил і здібностей, де треба чітко виконували вказівки, а де – виявляли творчий підхід до справи, і залишалися вірні своєму підприємстві, потрібно, щоб підприємство задовольняло їх потреби.

Відповідно, щоб підприємство було зацікавлене в задоволенні потреб працівника, необхідно, щоб і він задовольняв потреби підприємства. Ці позиції розглянуті в табл. 12.1.

Виявляємо, що забезпечення інформаційної безпеки – багатогранна проблема, і робота з людьми є однією з найбільш складних ділянок. Як і раніше справедливе стародавнє гасло „Кадри вирішують все!", оскільки без надійних, високопрофесійних, відданих своїй організації кадрів, без згуртованого колективу забезпечити захист інформації неможливо.

Діяльність служби персоналу повинна розглядатися як одна з ключових складових системи інформаційної безпеки підприємства.

Таблиця 2.4 - Кадровий консалтінг

Потреби підприємства по відношенню до працівника	Потреби працівника по відношенню до підприємства
Працівник повинен заробляти для підприємства грошей більше, ніж витрачається на його заробітну плату	Підприємство повинно забезпечити збалансоване сполучення матеріальних та моральних складових мотивації працівника
Працівник повинен робити точно те, що йому запропоновано посадовою інструкцією	Підприємство повинно забезпечити працівникові визначений ступінь психологічного комфорту (це дуже багатофакторна вимога)
Працівник повинен бути адекватно ініціативний, у потрібний час використовувати творчий підхід до реалізації своїх функцій	Працівник прагне до мінімізації витрат своєї праці
Працівник повинен вміти в нестандартній ситуації прийняти і реалізувати оптимальне рішення	

Далі переходимо до проблем аудиту інформаційної безпеки.

Контрольні запитання та завдання

1. Наведіть основні концептуальні положення комплексної системи безпеки інформації організації. Які вимоги включає системний підхід до захисту інформації?
2. Дайте визначення поняття Комплексної системи інформаційної безпеки (КСІБ).
3. Які існують методи впливу на особу для одержання потрібної інформації?
4. Які є основні вимоги до КСІБ?
5. Які види забезпечення повинна мати КСІБ, спираючись на які вона буде спроможна виконати свою цільову функцію?
6. Поясніть організаційну структуру служби безпеки підприємства. Які підрозділи входять до організаційної структури служби безпеки підприємства?
7. Назвіть основні завдання департаменту інформації та планування.
8. Назвіть основні завдання департаменту технічного захисту інформації.
9. Сучасні вимоги до підготовки спеціалістів служби безпеки.
10. Яка мета управління персоналом щодо становлення системи безпеки?
11. Вимоги до фахівця служби безпеки.
12. Які особисті засоби управління потребує персонал системи інформаційної безпеки? Назвіть основні напрями діяльності служби персоналу щодо забезпечення інформаційної безпеки підприємства.
12. Дайте визначення поняття „кадровий консалтінг”?

Завдання до самостійної роботи

1. Проаналізуйте варіант організації штатної структури служби безпеки конретного телекомунікаційного підприємства.
2. Проведіть аналіз організаційних рекомендацій щодо управління персоналом системи інформаційної безпеки.

РОЗДІЛ 13

АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

13.1 Загальні принципи аудиту інформаційної безпеки

При управлінні інформаційною безпекою, поряд з процесами оцінки ризиків інформаційної безпеки, організації й експлуатації захисних заходів, навчання персоналу інформаційній безпеці та іншими важливими процесами, визначальними є процеси контролю та перевірки інформаційної безпеки.

Серед процесів контролю та перевірки інформаційної безпеки особливе місце займає *аудит* (від лат. *audit – слухати*) інформаційної безпеки об'єкту інформаційної діяльності. Аудит є незалежною експертизою окремих областей функціонування організації. Його основним призначенням є формування, як правило, незалежної оцінки інформаційної безпеки. Своєчасність, точність і повнота оцінок інформаційної безпеки, отриманих у результаті аудиту, дають можливість виявити вразливості системи, визначити коригуючі заходи, що направлені на вдосконалення процесів забезпечення інформаційної безпеки.

Результатом аудиту є висновок про те, наскільки успішно функціонує об'єкт і наскільки він відповідає вимогам, які йому пред'являються. Цей висновок формується на основі вивчення якості виконання персоналом цього об'єкту функцій, які зафіксовані у технологічних регламентах, посадових інструкціях, створених за чинними стандартами та іншими нормативно-правовими документами.

Вихідними документами аудиту є оціночні звіти з конкретними й твердими рекомендаціями щодо приведення внутрішніх процесів, регламентів, інструкцій до відповідності чинним стандартам та нормативно-правовим документам.

Аудит проводиться на об'єкті інформаційної діяльності (ОІД), який є складною системою, що включає технічну й інфокомунікаційну інфраструктуру з її документацією та персонал, який використовує цю інфраструктуру для досягнення цілей ОІД. Оцінка роботи персоналу, а також систем з електронними обчислювальними машинами (ЕОМ), з'єднаними у системи та мережі, можлива лише методами аудиту.

Оцінка якості процесу роботи технічних та інфокомунікаційних систем можлива ще й методами випробувань. Проводяться натурні випробування, а коли це неможливо в реальних умовах, то проводять моделювання. За результатами випробувань моделі роблять висновки щодо реальної поведінки ОІД, його якості або надійності. Результати випробувань вказуються у акті випробувань, де фіксується, що ОІД відповідає заданим вимогам. ОІД має експлуатаційну документацію, де вказані умови та способи експлуатації, за яких властивості об'єкта не втрачаються.

Відповідно цим особливостям є два способи визначення об'єкту аудиту. У першому випадку ОІД розглядається як програмно-технічна система з

необхідною технічною та експлуатаційною документацією. Обслуговуючий персонал розглядається окремо. Цей підхід отримав розповсюдження у Росії.

У другому випадку ОІД – це складна система, яка включає технічну інфраструктуру з документацією та персонал, який використовує цю інфраструктуру для досягнення цілей функціонування об'єкта. Персонал працює у відповідності з правилами, інструкціями, написаними спеціально для нього. В Україні такий підхід реалізовано у нормативно-правових документах сфери захисту інформації у інформаційно-телекомунікаційних та автоматизованих системах.

Для оцінки рівня інформаційної безпеки ОІД у цілому успішно застосовується ISO 17799 «Аудит інформаційної безпеки», який походить від британського стандарту BS 7799. Статистика по інцидентам з інформаційною безпекою показує, що співвідношення вкладу у рівень інформаційної безпеки різних складових підпорядковується універсальному закону нерівності – Закону Парето у відношенні 20/80. При цьому 20% вкладу в інформаційну безпеку припадає на технічні системи, а 80% – на людей, які експлуатують ці системи [93].Закон Парето означає, що висновки щодо стану інформаційної безпеки мають враховувати не тільки показники якості технічних заходів захисту, а й оцінки якості їх експлуатації та рівні організації всіх процесів ОІД.

Як і при будь-яких оцінках, важливе значення має величина і точність оцінок. Оцінки випробувань роботи технічних засобів складаються із вимірювання відповідних фізичних величин (інтенсивності акустичних сигналів, напруженості електромагнітного поля, сили електричного струму тощо) і порівняння *кількісних* результатів вимірювання з нормами. Для вимірювання застосовують відповідні вимірювальні прилади, які мають регулярно проходити метрологічну повірку. Точність вимірювання фізичних величин залежить від класу точності вимірювальної апаратури.

Оцінки якості роботи персоналу та головних інформаційних процесів у комп'ютерних системах та мережах мають іншу природу. Вимірювання фізичних величин тут неможливо. Дії людей не характеризуються якимось набором фізичних параметрів. Критерії оцінки рівня захищеності у залежності від дій людей або комп'ютерних процесів можна оцінити *якісно* за допомогою якісних шкал. Ці шкали можуть мати:

дві градації – «так – ні» чи «відповідає – не відповідає»;

три градації – «низький-середній-високий» рівень;

п'ять градацій – «дуже низький-низький-середній-високий-дуже високий» рівень тощо.

Оцінку рівня захищеності за цими шкалами виконують експерти, що керуються точно визначеними методиками оцінки і процедурами обробки результатів оцінки, які гарантують достовірність оцінок.

Що стосується точності оцінок, то замість класу точності застосовують критерії гарантії оцінок. Суть цих гарантій полягає у отриманні впевненості у тому, що оцінки виконані правильно і її результатам можна вірити. Гарантії досягаються відповідною кваліфікацією експертів та виконанням низки вимог до дій на всіх етапах життєвого циклу ОІД від етапів технічного завдання на

його створення та проектування, до етапів експлуатації та утилізації при виводі об’єкта з експлуатації.

Аудитом називається систематичний, незалежний та документований процес отримання свідоцтв аудиту та об’єктивного їх оцінювання з метою встановлення степені виконання узгоджених критеріїв аудиту.

Свідоцтвом аудиту називають записи, звіти, викладання фактів та інша інформація, що має відношення до критеріїв аудиту та може бути перевіреною.

Критеріями аудиту можуть бути: політика інформаційної безпеки; процеси інформаційної безпеки або менеджменту об’єкта; відповідні процедури та вимоги. Аудит ОІД забезпечує інформацію, на основі якого організація може покращити характеристики своєї діяльності. Результати аудиту є одним з методів підтримки політики керівництва і контролю.

Результативність, надійність та об’єктивність висновків за результатами аудиту забезпечуються чітким дотриманням *принципів проведення* аудиту, до яких відносяться:

- етичність поведінки як основи професійності. Відповідальність, непідкупність, уміння зберігати таємницю та обачність є суттєвими ознаками професіоналізму;

- безпристрасність, тобто зобов’язання представляти правдиві і точні звіти. Діяльність з аудиту точно і правдиво відображаються у записах, звітах аудиту та висновках за результатами аудиту. Невирішені проблеми та розбіжності між аудиторською групою та організацією, що перевіряється, відображаються у звітах чи актах;

- професійна обачність, тобто старанність та уміння приймати правильні рішення при проведенні аудиту. Професійна обачність аудиторів відповідає важливості завдань, які виконуються, та довірчості з боку замовника й зацікавлених сторін;

- незалежність, що є основою безпристрасності й об’єктивності висновків з результатів аудиту. Аудитори незалежні у своїй діяльності та вільні від упередженості та конфліктів інтересів. Аудитори зберігають об’єктивну оцінку на протязі всього процесу аудиту і гарантують, що у основі оцінок та висновків лежать лише свідоцтва аудиту;

- підхід, заснований на свідоцтвах, як основа для досягнення надійних та відтворюваних висновків аудиту. Свідоцтва аудиту є вибіркою із існуючої інформації, що здійснюється у обмеженому інтервалі часу. Використання вибірок передбачає довіру до висновків з результатів аудиту.

Важливими є низка факторів для успішності оцінок процесів:

- мотивація керівництва та персоналу об’єкта у оцінках;

- забезпечення конфіденційності під час і після оцінки;

- довіра.

Мотивація керівництва і персоналу мають суттєвий вплив на результативність оцінки. Необхідно спонукати учасників оцінки до відкритості та конструктивності. Оцінка процесів зосереджується на процесах, а не на функціонуванні його учасників. Мета оцінки полягає у тому, щоб зробити процеси більш ефективним у досягненні цілей, а не в тому що б покласти

відповідальність на окремих осіб. Персонал об'єкта, як основний учасник оцінки процесів, є основним джерелом знань та досвіду щодо процесів. Керівництво і персонал об'єкту мають нагоду виявити потенційно слабкі місця. Відкрите обговорення попередніх висновків під час оцінки сприяє тому, щоб вихідні дані оцінки були значущими для оцінки.

Конфіденційність джерел інформації та зібраної під час оцінки документації необхідна для безпеки цієї інформації, а також інформації, що є власністю організації. Під час опитувань та обговорювань необхідно усунути загрози конфіденційності та забезпечити адекватні засоби контролю за обертанням та обробкою цієї інформації.

Організатори оцінки, керівництво й персонал об'єкту оцінки мають вірити, що оцінка принесе об'єктивний та показовий результат. Усі сторони мають бути впевненими у кваліфікації та неупередженості фахівців, та що вони правильно розуміють об'єкт і його функціонування для проведення оцінки.

Олександр Астахов наводить зразок «Етичного кодексу аудитора інформаційних систем» [5]:

Сприяти приведенню інформаційних систем у відповідність з прийнятими стандартами та інструкціями;

Здійснювати свою діяльність відповідно до стандартів в області аудиту інформаційних систем, прийнятими в сфері інформаційної безпеки;

Діяти на користь працедавців, акціонерів, клієнтів і суспільства в старанній, лояльній і чесній манері;

Свідомо не брати участі в незаконній, або несумлінній діяльності;

Дотримувати конфіденційність інформації, одержаної при виконанні своїх посадових обов'язків;

Не використовувати конфіденційну інформацію для отримання особистої вигоди і не передавати її третім особам без дозволу її власника;

Виконувати свої посадові обов'язки, залишаючись незалежним і об'єктивним;

Уникати діяльності, яка ставить під загрозу незалежність аудитора;

Підтримувати на належному рівні свою компетентність в областях знань, пов'язаних з проведенням аудиту інформаційних систем, беручи участь у професійних заходах;

Проявляти старанність при отриманні і документуванні фактографічних матеріалів, на яких базуються висновки і рекомендації аудитора;

Інформувати всі зацікавлені сторони про результати проведення аудиту;

Сприяти підвищенню обізнаності керівництва організацій, клієнтів і суспільства в питаннях, пов'язаних з проведенням аудиту інформаційних систем;

Відповідати високим етичним стандартам в професійній і особистій діяльності;

Удосконалювати свої особові якості.

Види аудиту класифікуються за її методами, цілями, і частотою проведення.

За методами проведення аудит поділяється на внутрішній та зовнішній.

Зовнішній аудит - цей, як правило, разовий захід, що проводиться за ініціативою керівництва організації або акціонерів, а також споживачів чи інших осіб від їх імені. Зовнішній аудит проводиться сторонньою організацією, яка має відповідної кваліфікації фахівців, засоби і методики проведення аудиту та ліцензії на цей вид діяльності, отримані в установленому порядку. Замовником може бути дана або інша зацікавлена організація. Висновки із результатів аудиту використовуються для покращення якості процесів організації. Рекомендується проводити зовнішній аудит регулярно.

Внутрішній аудит проводиться силами самої організації для самооцінки стану інформаційної безпеки організації, пошуку слабких місць, покращенню якості процесів організації або оцінки степені відповідності системи забезпечення безпеки встановленим вимогам. Внутрішній аудит є безперервною діяльністю, яка здійснюється на підставі «Положення про внутрішній аудит» і відповідно до плану, підготовка якого здійснюється підрозділом внутрішнього аудиту і затверджується керівництвом організації. Аудит безпеки інформаційних систем є однією із складових аудиту інформаційних технологій.

За метою проведення аудит поділяється на аудит для підтвердження відповідності вимогам національної системи нормативно-правових документів інформаційної безпеки та на аудит підтвердження відповідності міжнародним стандартам ISO 17799 та ISO\IEC 15408. Останній використовується як критерій аудиту інформаційних технологій.

За частотою проведення аудит поділяється на епізодичний, що систематично проводиться за заявками через певні інтервали часу, та безперервний, що вбудований технологічно у систему та реалізується автоматичними та на пів автоматичними засобами.

Усвідомлення необхідності аудиту інформаційної безпеки (ІБ) формується в результаті аналізу проблем ІБ безпеки та визначення потреб організації у оцінці відповідності політик, процесів, процедур забезпечення ІБ організації встановленим критеріям ІБ.

13.2 Цілі та метод проведення зовнішнього аудиту

Цілями проведення аудиту безпеки є:

- аналіз ризиків, пов’язаних з можливістю здійснення загроз інформаційної безпеки відносно ресурсів ОІД;
- оцінка поточного рівня захищеності ОІД;
- локалізація вузьких місць в системі захисту ОІД;
- оцінка відповідності ОІД чинним стандартам в області інформаційної безпеки;
- вироблення рекомендацій з упровадження нових і підвищення ефективності існуючих механізмів інформаційної безпеки ОІД.

Розглянемо етапи робіт з проведення аудиту інформаційної безпеки об’єктів інформаційної діяльності. *Аудит починається з процедури ініціації*.

Аудит проводиться за ініціативою керівництва організації, яке в даному питанні є основною зацікавленою стороною. Підтримка керівництва організації є необхідною умовою для проведення аудиту.

Аудит є комплексом заходів, в яких крім самого аудитора, необхідно задіяти представників більшості структурних підрозділів організації. Дії всіх учасників цього процесу повинні бути скоординовані. Тому на етапі ініціації процедури аудиту повинні бути вирішені наступні організаційні питання:

- права і обов'язки аудитора повинні бути чітко визначені і документально закріплені в його посадових інструкціях, а також в положенні про зовнішній аудит;
- аудитором має бути підготовлено і погоджено з керівництвом план проведення аудиту;
- у положенні про аудит повинен бути закріплено, зокрема, що зобов'язання співробітників організації сприяти аудитору і надавати всю необхідну для проведення аудиту інформацію.

На етапі ініціації процедури аудиту повинні бути визначені границі проведення обстеження. Одні інформаційні підсистеми об'єкту не є достатньо критичними і їх можна виключити з обстеження. Інші підсистеми можуть виявитися недоступними для аудиту з міркувань конфіденційності.

Границі проведення обстеження визначаються таким чином, що вказуються:

- перелік обстежуваних фізичних, програмних і інформаційних ресурсів;
- майданчики і приміщення, що підлягають обстеженню;
- основні види загроз інформаційної безпеки, що враховуються при проведенні аудиту;
- організаційні (законодавчі, адміністративні і процедурні), фізичні, програмно-технічні і інші аспекти забезпечення інформаційної безпеки, які необхідно врахувати в ході проведення обстеження, їх пріоритети та в якому обсязі вони повинні бути враховані.

План і границі проведення аудиту обговорюється на робочих зборах, в яких беруть участь аудитори, керівництво організації і керівники структурних підрозділів.

Етап *збору інформації аудиту* є найскладнішим і найтривалішим. Проводиться вивчення необхідної документації на об'єкт інформаційної діяльності, основу та додаткові інформаційні та технічні системи і здійснюється тісна взаємодія аудитора з багатьма посадовими особами організації.

Компетентні висновки щодо положення справ в ОІД з інформаційною безпекою можуть бути зроблені аудитором тільки за умови наявності всіх необхідних початкових даних для аналізу.

Отримання інформації про організацію, функціонування і поточний стан ОІД здійснюється аудитором в ході спеціально організованих інтерв'ю з відповідальними особами організації, шляхом вивчення технічної і організаційно-розпорядливої документації, а також дослідження ОІД з використанням спеціалізованого програмного інструментарію.

Забезпечення інформаційної безпеки ОІД - це комплексний процес, що вимагає чіткої організації і дисципліни. Він повинен починатися з визначення ролей і розподілу відповідальності серед посадовців, що мають відношення до інформаційної безпеки. Тому аудиторське обстеження починається з отримання інформації про організаційну структуру користувачів ОІД і обслуговуючих підрозділів. У зв'язку з цим аудитору потрібна наступна документація:

- схема організаційної структури користувачів;
- схема організаційної структури обслуговуючих підрозділів.

У ході інтерв'ю аудитор ставить опитуваним наступні запитання:

- хто є власником інформації?
- хто є користувачем (споживачем) інформації?
- хто є провайдером послуг?

Призначення і принципи функціонування ОІД багато в чому визначають існуючі ризики і вимоги інформаційної безпеки, що пред'являються до системи. Тому на наступному етапі аудитора цікавить інформація щодо призначення і функціонування ОІД. Аудитор ставить опитуваним приблизно такі запитання:

- які послуги і яким чином вони надаються кінцевим користувачам?
- які основні види застосувань функціонують в ОІД?
- кількість і види користувачів, що використовують ці застосування?

Аудитору потрібна також така документація:

- функціональні схеми;
- опис автоматизованих функцій;
- опис основних технічних рішень;
- інша проектна і робоча документація на інформаційну систему

Далі, аудитору потрібна детальніша інформація щодо структури ОІД. Це дозволить з'ясувати, яким чином здійснюється розподіл механізмів інформаційної безпеки за структурними елементами і рівнями функціонування ОІД. Типові питання, які обговорюються у зв'язку з цим під час інтерв'ю, включають:

- з яких компонентів (підсистем) складається ОІД?
- функції окремих компонент?
- де проходять границі системи та контрольованої зони?
- які є точки входу?
- як ОІД взаємодіє з іншими системами?
- які канали зв'язку використовуються для взаємодії з іншими ОІД?
- які канали зв'язку використовуються для взаємодії між компонентами системи?
- за якими протоколами здійснюється взаємодія?
- які програмно-технічні платформи використано при побудові системи?

Аудитор на цьому етапі використовує також документацію:

- структурна схема ОІД;
- схема інформаційних потоків;
- опис структури комплексу технічних засобів інформаційної системи;
- опис структури програмного забезпечення;

- опис структури інформаційного забезпечення;
- розміщення компонентів інформаційної системи.

Підготовка значної частини документації на ОІД, звичайно, здійснюється вже в процесі проведення аудиту. Коли всі необхідні дані щодо ОІД, включаючи документацію, підготовлені, можна переходити до їх аналізу.

Аналіз даних аудиту

Аудитори можуть використовувати один трьох методів аналізу даних, що, визначаються вибраними підходами до проведення аудиту.

Перший підхід, найскладніший, базується на аналізі ризиків. Опираючись на методи аналізу ризиків, аудитор визначає для обстежуваної ОІД індивідуальний набір вимог інформаційної безпеки, що найбільшою мірою враховує особливості даної ОІД, середовища її функціонування та існуючі в даних середовищах загрози інформаційної безпеки. Даний підхід є самим трудомістким і вимагає найвищої кваліфікації аудитора.

Другий практичний підхід, опирається на використанні стандартів інформаційної безпеки. Стандарти визначають базовий набір вимог інформаційної безпеки та функціональні профілі захисту для широкого класу ОІД, який формується в результаті узагальнення світової практики. Стандарти можуть визначати різні набори вимог інформаційної безпеки (функціональні профілі захисту), залежно від рівня захищеності ОІД, який потрібно забезпечити, її приналежності (комерційна організація, або державна установа), а також призначення (фінанси, промисловість, зв'язок тощо). Від аудитора в даному випадку вимагається правильно визначити набір вимог стандарту (обрати функціональний профіль захисту), відповідність яким вимагається забезпечити для даної ОІД.

Необхідна також методика, що дозволяє оцінити цю відповідність. Через свою простоту (стандартний набір вимог, тобто функціональний профіль захисту, для проведення аудиту вже наперед визначений стандартом) і надійність (стандарт - є стандарт і його вимоги ніхто не спробує оспорити), описаний підхід найбільш поширений. Він дозволяє при мінімальних витратах ресурсів робити обґрунтовані висновки про стан ОІД.

Третій підхід, найефективніший, припускає комбінування перших двох. Базовий набір вимог інформаційної безпеки, що пред'являються до ОІД, визначається стандартом. Додаткові вимоги, які в максимальній мірі враховують особливості функціонування даної ОІД, формуються на основі аналізу ризиків. Цей підхід є набагато простішим першого, оскільки основна частина вимог інформаційної безпеки вже визначена стандартом, і, в той же час, він позбавлений недоліку другого підходу, який полягає в тому, що вимоги стандарту можуть не враховувати специфіки обстежуваної ОІД.

Найскладнішим і найбільш відповідальним у процесі аудиту є аналіз ризиків.

Аналіз ризиків – це те, з чого повинна починатися побудова будь-якої системи інформаційної безпеки. Він включає заходи щодо обстеження інформаційної безпеки ОІД з метою визначення того, які ресурси і від яких загроз треба захищати, а також в якій мірі ті або інші ресурси потребують

захисту. Визначення набору адекватних контрзаходів здійснюється в ході управління ризиками. Ризик визначається ймовірністю спричинення збитку (втрат) і величиною збитку, що наноситься ресурсам ОІД, у разі здійснення загрози інформаційної безпеки.

Аналіз ризиків полягає в тому, щоб виявити існуючі ризики і оцінити їх величину (дати їм якісну, або кількісну оцінку). Процес аналізу ризиків можна розділити на декілька послідовних етапів:

- ідентифікація ключових ресурсів ОІД;
- визначення важливості тих або інших ресурсів для організації;
- ідентифікація існуючих загроз інформаційної безпеки і уразливості, які роблять можливим здійснення загроз;
- розрахунок ризиків, пов'язаних із здійсненням загроз інформаційної безпеки.

Ресурси ОІД можна розділити на такі категорії:

- інформаційні ресурси;
- програмне забезпечення;
- технічні засоби (сервери, робочі станції, активне мережне устаткування тощо);
- людські ресурси

У кожній категорії ресурси діляться на класи і підкласи. Необхідно ідентифікувати лише ті ресурси, які визначають функціональність ОІД і істотні з погляду забезпечення інформаційної безпеки.

Важливість (або вартість) ресурсу визначається величиною збитку, що наноситься у разі порушення конфіденційності, цілісності або доступності цього ресурсу. Звичайно розглядаються наступні види збитку:

- дані були розкриті, змінені, видалені або стали недоступні;
- апаратура була пошкоджена або зруйнована;
- порушена цілісність програмного забезпечення.

Збиток може бути завданий організації в результаті успішного здійснення наступних видів загроз інформаційної безпеки:

- локальні і віддалені атаки на ресурси ОІД;
- стихійні лиха;
- помилки, або навмисні дії персоналу ОІД;
- збої в роботі ОІД, викликані помилками в програмному забезпеченні або несправностями апаратури.

Під уразливістю розуміють такі властивості ОІД, що роблять можливим успішне здійснення загроз інформаційної безпеки.

Величина ризику R визначається за формулою:

$$R = \frac{C_P}{K_{BP}} P_З , \qquad (13.1)$$

де $C_р$ – вартість ресурсу,

$P_з$ – ймовірність здійснення загрози,

$K_{вр}$ – величина не уразливості.

Задача управління ризиками полягає у виборі обґрунтованого набору контрзаходів, що дозволяють понизити рівні ризиків до прийнятної величини.

Вартість реалізації контрзаходів повинна бути менше величини можливого збитку. Різниця між вартістю реалізації контрзаходів і величиною можливого збитку повинна бути обернено пропорційна ймовірності спричинення збитку.

Наступним етапом процесу аудиту є використання методів аналізу ризиків.

Якщо для проведення аудиту інформаційної безпеки обрано підхід, який базується на аналізі ризиків, то на етапі аналізу даних аудиту звичайно виконуються такі групи задач:

- аналіз ресурсів ОІД, включаючи інформаційні ресурси, програмні і технічні засоби, а також людські ресурси;
- аналіз груп задач, що вирішуються системою, і бізнес процесів;
- побудова моделі ресурсів ОІД, що визначає взаємозв'язки між інформаційними, програмними, технічними і людськими ресурсами, їх взаємне розташування і способи взаємодії;
- оцінка критичності інформаційних ресурсів, а також програмних і технічних засобів;
- визначення критичності ресурсів з урахуванням їх взаємо залежностей;
- визначення найімовірніших загроз інформаційної безпеки відносно ресурсів ОІД і уразливості, які роблять можливим здійснення цих загроз;
- оцінка ймовірності здійснення загроз, величини не вразливості та збитку, що наноситься організації у разі успішного здійснення загроз;
- визначення величини ризиків для кожної трійки: загроза - група ресурсів - уразливість.

Для вирішення цих задач можуть використовуватися різні формальні і неформальні, кількісні і якісні, ручні і автоматизовані методики аналізу ризиків. Суть підходу від цього не міняється.

Оцінка ризиків може даватися як з використанням різних якісних, так і кількісних шкал. Головне, щоб існуючі ризики було правильно ідентифіковано й категорійовано відповідно до ступеня їх критичності для організації. На основі такого аналізу може бути розроблена система першочергових заходів щодо зменшення величини ризиків до прийнятного рівня.

Далі проводиться оцінка відповідності вимогам стандартів.

У разі проведення аудиту інформаційної безпеки на відповідність вимогам стандарту, аудитор, покладаючись на свій досвід, оцінює застосовність вимог стандарту до обстежуваної ОІД та її відповідність цим вимогам. Дані про відповідність різних областей функціонування ОІД вимогам стандарту, звичайно, представляються в табличній формі. З таблиці видно, які вимоги інформаційної безпеки в системі не реалізовані. Виходячи з цього, робляться висновки про відповідність обстежуваної ОІД вимогам стандарту і даються рекомендації з реалізації в системі механізмів інформаційної безпеки, що дозволяють забезпечити таку відповідність.

Вироблення рекомендацій.

Рекомендації, видавані аудитором за наслідками аналізу стану ОІД, визначаються підходом, що використовується, особливостями обстежуваної

ОІД, станом справ з інформаційною безпекою і ступенем деталізації, що використовується при проведенні аудиту.

Рекомендації аудитора повинні бути конкретними і застосовними до даної ОІД, економічно обґрунтованими, аргументованими (підкріпленими результатами аналізу) і відсортованими за ступенем важливості. При цьому заходи щодо забезпечення захисту організаційного рівня практично завжди мають пріоритет над конкретними програмно-технічними методами захисту.

Підготовка звітних документів

Аудиторський звіт є основним результатом проведення аудиту. Його якість характеризує якість роботи аудитора. Структура звіту може істотно розрізнятися залежно від характеру і цілей аудиту, що проводиться. Певні розділи повинні бути обов'язково присутніми в аудиторському звіті. Він повинен, містити опис цілей проведення аудиту, характеристику обстежуваної ОІД, вказівку границь проведення аудиту і методів, що використовуються, результати аналізу даних аудиту, висновки, що узагальнюють ці результати і містять оцінку рівня захищеності ОІД або відповідність його вимогам стандартів, та, рекомендації аудитора щодо усунення недоліків й вдосконалення системи захисту.

13.3 Оцінка інформаційної безпеки

Найбільш складною процедурою аудиту інформаційної безпеки є оцінка інформаційної безпеки. В ідеальному випадку кожна організація, кожен її співробітник має примати заходи до захисту інформації у залежності від її цінності, наявних загроз та її вразливості. У реальному світі люди не завжди надають потрібної уваги захисту інформації, а частина людей за ради вигоди чи інших цілей використовують погано організовану систему безпеки для доступу до інформації не будучи до цього уповноваженими.

Законодавством розглядаються три види кримінальних злочинів у комп'ютерній сфері:

- неправомірний доступ до комп'ютерів, зокрема, незаконне копіювання програм;
- неправомірний доступ з метою скоїти або сприяти здійсненню подальших правопорушень, таких як крадіжка чи шахрайство;
- неправомірна зміна програмного забезпечення, зокрема, неправомірне й навмисне знищення програмного забезпечення, баз даних чи зараження вірусами.

Для успішного судового переслідування зловмисників організації повинні мати достатні докази того, що доступу до інформаційних систем було не санкціоновано. За законом людина має чітко усвідомлювати, що не була уповноважена до доступу у систему. Для цього необхідно чітко визначитись щодо політики прийнятного використання інформаційних систем, зокрема розробити політику інформаційної безпеки, вести у системах журнали реєстрації подій в системі або аудиторські лог-файли та проводити регулярні перевірки журналів реєстрації подій в системі. Необхідно приймати розумні і

належні фізичні, технічні та організаційні заходи безпеки, які направлені на забезпечення цілісності й конфіденційності інформації. Також необхідно проводити систематичні, деталізовані й точні оцінки ризиків. Не захищені системи не можуть розглядатись як джерела достовірної інформації. Чинне законодавство містить вимогу щодо проведення оцінки ризиків та створення на цій базі оцінки системи заходів інформаційної безпеки.

У сфері аудиту інформаційної безпеки є невирішені проблеми, які вимагають як практичних дій, так і наукових досліджень. До цих проблем відносяться такі питання:

- який рівень безпеки необхідний конкретній організації;
- як організація може довести наявність необхідного рівня безпеки та належного контролю цього рівня.

Далі розглянемо низку практичних та наукових результатів у цій сфері, що отримані на сьогоднішній день. Почнемо з моделі оцінки процесів забезпечення інформаційної безпеки.

Основу оцінки складають перелік оцінюваних процесів та сукупність показників, за якими проводиться збір даних та визначення степені досягнення атрибутів процесів встановлених критеріїв аудиту інформаційної безпеки. Атрибути процесів вимірюються, отримані кількісні показники об'єднуються в узагальнені групові показники, у свою чергу узагальнені групові показники об'єднуються у комплексний показник інформаційної безпеки, за допомогою якого оцінюється безпека.

Метод вимірювання є логічною послідовністю операцій, яка виконується для вимірювання атрибутів відносно певної шкали. Операціями можуть бути підрахунки подій або часу їх виникнення чи тривалості.

Визначають два види вимірювання атрибутів:

- суб'єктивний, це кількісне визначення, яке включає міркування людини;
- об'єктивний, за якого виконується кількісне визначення засноване на обчисленнях.

Величина виміряного атрибуту переводиться у значення за шкалою вимірювань. Вид шкали залежить від характеру взаємовідносин між значеннями на шкалі. Можуть застосовуватись наступні шкали:

- номінальна шкала, значення вимірювання є категоріями;
- порядкова шкала, значення категорій ранжуються. Наприклад, загрози розподіляються за рівнем їх небезпечності;
- інтервальна шкала, значення вимірювання мають однакові відстані, які відповідають однаковим величинам атрибуту. Нульове значення відсутнє;
- шкала відношень, де значення вимірювання мають однакові відстані, які відповідають однаковим величинам атрибуту, нульове значення відповідає нульовому значенню атрибуту.

Показник функціонування W процесу є міра відповідності реального результату, тому, який потрібен. Функція відповідності, яка показує степінь досягнення мети процесу, має відповідати вимогам: змістовності, інтерпретованості та вимірюваності.

Змістовність означає, що при оцінці показника враховуються всі суттєві характеристики, властивості й атрибути процесу. Інтерпретованість необхідна, щоб розуміти результати оцінювання. Вимірюваність означає, що для показника існує метод вимірювання, який забезпечує достовірні дані і достовірний спосіб оцінювання.

Якщо процес оцінюється за деяким числом його атрибутів або ціль процесу досягається вирішення декількох задач, то вводиться узагальнений векторний показник функціонування, що об'єднує часткові показники

$$W_O = \langle W_1, W_2, ..., W_m \rangle, \qquad (13.2)$$

де m – число часткових показників функціонування W_i.

Додатковими вимогами до векторного показника функціонування є: мінімальне число часткових показників та повнота охоплення характеристик, властивостей та атрибутів процесу.

Часткові показники можуть мати різні розмірності. При формуванні узагальненого векторного показника необхідно нормувати часткові показники, щоб можна було їх спів ставляти. Значення часткового показника представляють у процентах або долях.

Вимірювання інформаційної безпеки може базуватись на недосконалій чи нечіткій інформації, отриманої в результаті опитування персоналу організації. Тому необхідне визначення точності чи значимості інформації при представлення фактичного значення показника. Точність показників залежить від обраного методу вимірювання, джерела даних і достовірності даних.

Об'єднання часткових показників – це алгоритм або обчислення, яке об'єднує часткові показники за певним правилом. Правило засноване на розумінні чи припущенні щодо очікуваного зв'язку між показниками. Таким правилом може бути присвоєння частковим показникам коефіцієнта значимості. Значимість часткових показників визначається степенем впливу атрибуту процесу на результат процесу. Тоді узагальнений показник обчислюється наступним чином

$$W_O = \sum \alpha_i W_i, \qquad (13.3)$$

де α_i – коефіцієнти значимості часткових показників W_i;

$$\sum_{i=1}^{m} \alpha_i = 1;$$

m – число часткових показників функціонування W_i в узагальненому показнику W_o.

Об'єднання часткових показників може бути виконано на основі теорії корисності, коли користуються системою надавання переваг одним частковим показникам перед іншими. Процес, який оцінюється узагальненим показником, може мати оцінку, що дорівнює частковому показнику, що має перевагу.

Формування комплексного показника теж представляє собою алгоритм чи обчислення, які об'єднують узагальнені показники за певним правилом. Це правило теж може бути засноване на системі переваг. У результаті об'єднання узагальнених показників отримують комплексний показник, який відображає інформаційну безпеку організації або системи.

При виборі часткових, узагальнених та комплексних показників враховують такі критерії:

- відповідність цілям процесів та цілям перевірки;
- можливість здійснення збору даних;
- доступність кадрових ресурсів для збору та управління даними;
- простота збору даних;
- степінь втручання у діяльність персоналу;
- доступність відповідних інструментальних засобів;
- забезпечення конфіденційності;
- потенційний опір постачальників даних;
- простота інтерпретації показників споживачам та спеціалістам оцінки;
- особливості організацій та систем, які перевіряються;
- вартість використаних показників: вартість збору даних, автоматизація обчислень, аналізу даних, інтерпретації результатів аналізу, повідомлення результатів проведеної оцінки.

Інтерпретація результатів оцінки представляє собою пояснення, яке зв'язує кількісну оцінку показників з потребами вимірювань мовою споживача результатів вимірювання. Так інтерпретація може відображати порушення властивостей інформаційної безпеки, можливі негативні наслідки для діяльності організації або функціонування системи за результатами оцінки.

Отримала розповсюдження інша модель оцінювання інформаційної безпеки, яка заснована на моделі зрілості процесів забезпечення безпеки. Наприклад, для процесу «Аналіз і оцінка ризику інформаційної безпеки» системи менеджменту інформаційної безпеки організації, яку визначає стандарт ISO/IEC 27001 описується модель зрілості з п'яти рівнів. Розглянемо опис нульового, першого, третього та п'ятого рівнів.

Нульовий рівень означає повну відсутність певного процесу аналізу та оцінки ризиків інформаційної безпеки. Керівництво організації не усвідомлює наслідки для бізнесу реалізації загроз інформаційної безпеки, інциденти з інформаційною безпекою не попереджаються, не розглядаються і не аналізуються.

Перший рівень означає, що в організації існує і документально визначена сфера дії менеджменту інформаційної безпеки, складено перелік інформаційних ресурсів та ймовірності реалізації загроз, розраховані можливі втрати від реалізації загроз. Але процес аналізу і оцінки ризиків не стандартизовано.

Третій рівень передбачає, що в організації існує політика організації, яка визначає періодичність та область оцінки ризиків інформаційної безпеки, процес оцінки ризиків документовано й стандартизовано, суть процесу доводиться до зацікавленого персоналу. Складено план з оцінки ризиків. Але методи збору інформації щодо інцидентів, загроз та вразливостей віддані на розсуд персоналу і не координуються.

П'ятий рівень – найвищої зрілості. Оцінка ризиків доведена до рівня кращих практик. Обрана стратегія оцінки ризиків безперервно удосконалюється. Залучаються сторонні сертифіковані спеціалісти для консультацій з питань ризиків, оптимізації системи збору інформації для оцінки

та аналізу ризиків. Використовуються наради типу «мозкового штурму» для виявлення та аналізу ідентифікованих ризиків. Система заходів захисту скоординована з пріоритетами ризиків та залежністю «ефективність заходів захисту – вартість». Комплексно використовується встановлена форма звітності щодо ефективності заходів захисту.

Процедури збору, аналізу, зберігання, супроводження та передачі даних щодо загроз, вразливостей та інцидентів інформаційної безпеки автоматизовано та формалізовано. Встановлена відповідальність за порушення процедур інформування щодо інцидентів інформаційної безпеки. Керівники та рядовий персонал навчаються практикам інформаційної безпеки з перевіркою їх знань.

Оцінка ризику представляє собою добре структурований, формалізований процес, що постійно вдосконалюється і добре управляється.

Для оцінки рівня зрілості конкретного процесу в організації пропонується метод «від початкового до максимального».Оцінка виконується за такими параметрами:

- область дії системи менеджменту інформаційної безпеки;
- опис реалізації процесу;
- гарантії для бізнесу;
- інформація щодо середовища;
- ідентифікація задіяних ресурсів;
- вплив процесу на досягнення цілей бізнесу;
- загрози, вразливості.

Для аналізу мають бути представлені документальні свідоцтва щодо:

- виконання аналізу ризиків на підставі ідентифікації інформаційних ресурсів, їх вразливостей та загроз;
- виконання оцінки можливих втрат із-за реалізації загроз інформаційної безпеки;
- вибір варіанту обробки та мінімізації кожного з ризиків;
- зниження кількості потенційних інцидентів та збільшення кількості виявлених інцидентів

Така оцінка може бути здійснена як продовження оцінки на відповідність показникам інформаційної безпеки.

Після завершення аудиту замовник чи керівництво перевіреної організації мають оцінити результати проведення аудиту. Використання результатів аудиту можливо для прийняття рішень з планування й реалізації коригуючих та превентивних заходів у відношенні процесів системи забезпечення інформаційної безпеки організації чи програми аудиту.

13.4 Безперервний внутрішній аудит інформаційної безпеки телекомунікаційних мереж

В телекомунікаційних мережах безперервний аудит інформаційної безпеки впроваджується згідно міжнародних Рекомендацій X.800 та X.816 [218, 220].

Розглянемо аудит інформаційної безпеки найбільш критичної ланки телекомунікаційних систем, а саме інформаційної безпеки систем технологічного управління (СТУ), зупинка яких викликає переривання процесу управління, дозволяє також враховувати дії суб'єктів, контролювати правильність використання ресурсів, виявляти спроби пошкодити систему.

Безперервний аудит безпеки – це незалежний перегляд та дослідження системних даних, протоколів і подій для перевірки адекватності управління системою, для забезпечення відповідності між встановленою політикою та діючими процедурами, для виявлення виломів безпеки і для цілеспрямованого вдосконалення політики та процесу функціонування системи.

Механізми аудиту безпеки хоч і не здатні безпосередньо запобігати порушенням безпеки, але виконують важливі функції запису та аналізу подій, що трапляються в системі, сприяють правильній реакції на ситуації порушення безпеки системи шляхом зміни робочих процедур. При виникненні неприпустимої загрози безпеці, коли параметри системи перевищують встановлені межі, в системі генерується сигнал тривоги.

Ієрархічна модель реалізації послуг аудиту. Серед множини процедур аудиту можна виділити робочі фази, кожна з яких характеризується своєю тривалістю:

t_1 - визначення події, що стосується безпеки системи;

t_2 - прийняття рішення щодо запису події або генерацію тривожної сигналізації;

t_3 - опрацювання прийнятого рішення, тобто створення повідомлень аудиту безпеки або тривожної сигналізації;

t_4 - аналіз та оцінка, згідно з визначених критеріїв, події, що стосується безпеки системи, а також визначення реакції на подію, тобто послідовності дій;

t_5 - накопичення (збирання) розподілених в системі записів в журнали реєстрації аудиту (*security audit trail*);

t_6 - формування звіту із записів журналів реєстрації аудиту;

t_7 - архівація, тобто переміщення записів в журналах реєстрації аудиту.

Усі наведені вище фази не розділені за часом, тобто можуть перекриватись, тривати одночасно.

На рис. 13.1 наведено ієрархічну модель послуг аудиту та тривожної сигналізації в СТУ, що будується у відповідності з рекомендацією *ITU-T X*.816.

На найнижчому рівні *S*1 відбувається, згідно з визначених критеріїв, визначення подій, що стосуються безпеки СТУ, та реакції на події. При прийнятті рішення вхідними параметрами дискримінатора події є тип події, що стосується безпеки, час доби та деякі особливі характеристики об'єкта-чинника події. Вихідною реакцією дискримінатора є повідомлення про дію у відповідь на подію, генерування тривожної сигналізації та повідомлення аудиту безпеки.

На рівні *S*1 відсутні можливості ведення стеження та аналізу подій, тому тривожні повідомлення направляються до *S*2, а повідомлення аудиту безпеки – до *S*3 для подальшого включення до журналів реєстрації аудиту. Журнал реєстрації аудиту містить дані, що збираються та потенційно використовуються для полегшення аудиту безпеки.

На рівні *S*3 відбувається поновлення (*update*) журналів реєстрації аудиту, забезпечується для рівня *S*6 доступ до журналів реєстрації та до їх архівів з можливістю сортувати та вибирати потрібні записи журналів згідно з визначених критеріїв з подальшим занесенням цих записів до звіту безпеки. При формуванні звітів з безпеки інформації ці критерії враховуються при обробленні інформації, що міститься в одному чи більше журналах реєстрації аудиту. Рішення приймається на основі таких параметрів: тип аудит-запису; тип події, що стосується безпеки; тривалість події, що розглядається; тип об'єкту, інформація, котра потрібна для прийняття рішення. Кінцеве рішення видається у вигляді списку вибраних записів.

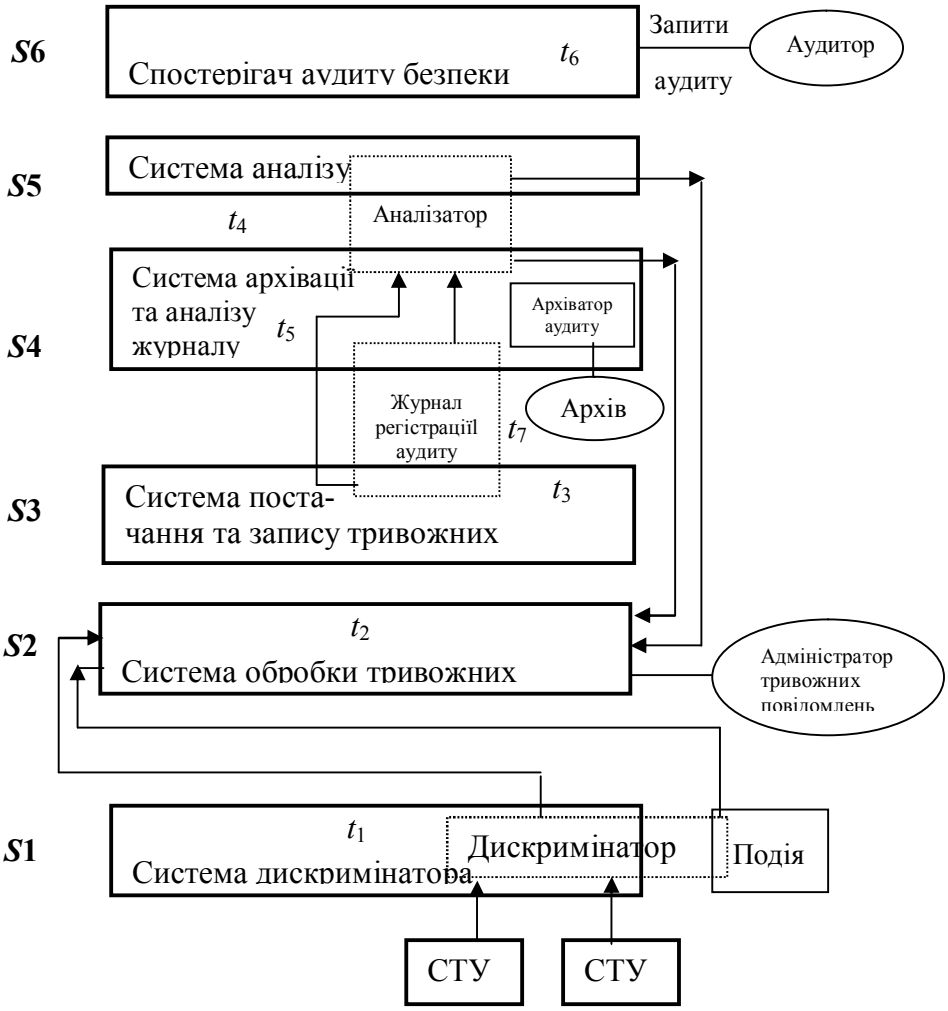


Рис.13.1. Модель реалізації послуг аудиту та тривожної сигналізації в СТУ.

На рівні *S*4 відбувається архівація записів журналу реєстрації та пошук потрібних записів в архівах.

Програмне забезпечення (ПЗ) рівня *S*5 здійснює аналіз записів журналів реєстрації, а також архівних записів, згідно з визначених критеріїв, а також пересилає сигнали тривоги до *S*2 при перевищенні певних граничних значень

параметрів системи або визначених умов роботи системи, що можуть трактуватись як ненормальні.

Критерії в даному разі визначають, яким чином аналізатор аудиту буде обробляти записи журналів реєстрації. В загальному випадку аналіз записів журналу реєстрації аудиту відбувається шляхом оцінки частоти появи подій та типу подій до того, як буде визначено реакцію системи на подію. Прийняття рішення базується на таких параметрах: тип події, частота появи події, тривалість події. Після ретельного аналізу події визначається, яка дія потрібна у відповідь.

Участь операторів у процесі аудиту передбачається на двох рівнях. Аудит-адміністратор здійснює загальне управління аудитом, а оперативне управління покладається на адміністратора тривожних повідомлень.

Динаміка реалізації послуг аудиту. Складемо граф, що ілюструє послідовність виконання рівнями моделі своїх функцій при порушенні безпеки СТУ як реакція на дії зловмисника, що стосуються безпеки системи (рис. 13.2).

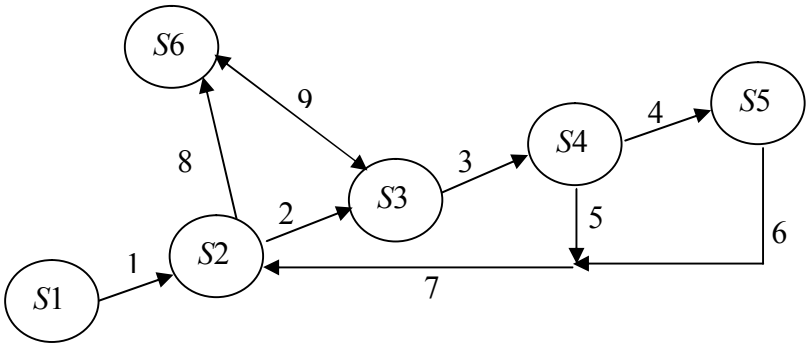


Рис. 13.2. Послідовність дій рівнів моделі реалізації послуг аудиту та тривожної сигналізації в СТУ

Система дискримінатора рівня *S*1 визначає подію, що трапилась в системі або іншій СТУ і, якщо ця подія стосується безпеки, інформує про це систему обробки тривожних повідомлень на рівні *S*2. Система постачання та запису тривожних повідомлень рівня *S*3 взаємодіє з вищими рівнями *S*4 та *S*5, де відбувається архівація та аналіз сформованих повідомлень аудиту безпеки. Рівень *S*6 взаємодіє з рівнем *S*3 при створенні звітів безпеки.

Результати роботи на рівнях *S*4 та *S*5 передаються до системи обробки тривожних повідомлень, яка сповіщає про результати аналізу адміністратора тривожних повідомлень та відповідає на запити аудитора (рівень *S*6). За результатами обробки та аналізу інформації виноситься певне рішення щодо реакції системи.

Для проведення дієвої політики аудиту безпеки важливою є здатність неперервної перевірки адекватності засобів контролю параметрів системи та гнучкого реагування на результати перевірок. Цей процес базується на ретельному аналізі записів та нових повідомлень журналу реєстрації аудиту, що можуть надходити як від самих аудит-повідомлень, так і від інших журналів реєстрації аудиту.

При аналізі подій, що трапились у системі, використовуються механізми фільтрації повідомлень за певними критеріями, наприклад, в залежності від часу доби, за типом самої події чи об'єкту-чинника події тощо. З точки зору управління ці фільтри можуть бути визначені як керовані об'єкти з певними специфічними параметрами, властивостями та поведінкою.

Наприклад, в необслуговуваній кінцевій системі аудит безпеки може мати такі інстальовані функції: диспетчер аудиту (*audit dispatcher*), запис аудиту (*audit recorder*), провайдер аудиту (*audit provider*), аналізатор аудиту (*audit analyser*). Можуть бути згруповані такі важливі для аудитора безпеки функції як перегляд журналу регістрації та аналізатор аудиту.

Остаточне рішення щодо запису певної події до журналу реєстрації аудиту, або включення тривожної сигналізації, приймає аудит-адміністратор, процес або особа, до обов'язків котрого, насамперед, входить вибір серед усіх подій в системі таких, що стосуються безпеки. Цей процес відбувається в рамках політики аудиту безпеки, яка визначає комплексні загальні правила збирання, запису та аналізу важливих для системи подій.

Передбачається наявність засобів контролю критичних параметрів середовища телекомунікаційного об'єкту (зменшення пропускної спроможності каналів, падіння якості передавання, зміни температури, відчинення дверей, вікон чи люків тощо) або комбінації таких засобів. Робочі станції в СТУ мають умонтовані програмно-апаратні засоби для автентифікації користувача, керування доступом, захисту системної пам'яті та пам'яті, що містить програмне забезпечення системи забезпечення безпеки СТУ. Але вони залишаються уразливими до атак, вірусів, несанкціонованого доступу та пов'язаними із ними погрозами.

У реальних СТУ для забезпечення служб аудиту, реєстрації та спостереження діють механізми реєстрації інформації щодо сеансів користувачів, фіксації будь-яких змін прав користувачів для керування доступом, реєстрації використання критично важливих файлів та їх модифікації, реєстрації використання інструментів керування трафіком, що циркулює в СТУ, а також використання засобів аудиту.

Базові кількісні характеристики. Послідовність подій, що характерна для несанкціонованого доступу (НСД) у загальному вигляді може бути описана такими кроками:

Впорядкування інциденту полягає у зменшенні потенційно небезпечних наслідків події, що стосується безпеки СТУ, з використанням засобів впорядкування інциденту і ресурсів для попередження операторів.

Резервування має гарантувати коректне закінчення сеансу роботи сервера або робочої станції з подальшим відновленням нормальних робочих параметрів.

Відновлення має забезпечити правильне та швидке відновлення нормальної роботи СТУ після перерви в її роботі за мінімальний можливий проміжок часу з врахуванням пріоритету важливості для функціонування.

Конкретні загрози визначають організаційні заходи щодо забезпечення безпеки СТУ.

У СТУ передбачається як розміщення функцій безпеки в межах певного компонента системи, так і розподіл їх між компонентами системи. Особливості побудови системи впливають на спосіб інсталяції функцій безпеки. В реальних системах досить поширеним є спосіб дублювання функцій шляхом розміщення їх в різних кінцевих системах та групування функцій.

Розглянемо дії порушника безпеки СТУ та реакцію системи на його дії. Вважається, що порушник знає функціональні особливості СТУ, має високий рівень знань в області програмування й обчислювальної техніки, проектуванні й експлуатації автоматизованих інформаційних систем, досвід роботи з технічними засобами, знає структуру, функції і механізми дії засобів захисту, їхні сильні і слабкі сторони. Припустимо, що має місце спроба порушника отримати доступ до баз даних, архівів або зони керування засобами забезпечення безпеки СТУ. При цьому атака може бути безумовною, або відбуватись після настання очікуваної події на атакованому об'єкті, або по запиту від атакованого об'єкта.

1. Віддалене підключення порушника до лінії, що з'єднує комп'ютерну мережу, на якій базується СТУ та всі інші зовнішні мережі;
2. Спроба порушника підібрати або зламати пароль входу до комп'ютерної мережі СТУ (всього N спроб). Тут і далі фіксування всіх подій відбувається на рівні $S1$;
3. Фіксування спроби порушника підібрати або зламати пароль входу до комп'ютерної мережі СТУ;
4. Спроба порушника підібрати або зламати пароль входу до певного сервера або робочої станції комп'ютерної мережі СТУ;
5. Фіксування спроби порушника підібрати або зламати пароль входу до певного сервера або робочої станції комп'ютерної мережі СТУ;
6. Несанкціоновані дії, що стосуються безпеки СТУ;
7. Фіксування несанкціонованих дій, що стосуються безпеки СТУ, технічними та програмними засобами системи. Всі події в системі записуються, спрацьовує тривожна сигналізації (працюють рівні $S2$, $S3$). Відбувається аналіз та оцінка дій порушника на рівні $S4$. Після аналізу та класифікації події, що пов'язана з безпекою, реакцією СТУ на дії порушника можуть бути дії з впорядкування інциденту, резервування та дії, спрямовані на відновлення працездатності системи.
8. Вихід з об'єкту;
9. Фіксування виходу з об'єкту;

Кроки 3, 5, 7, 9 (фіксування подій) залежать від відповідних попередніх кроків. Дійсно, якщо подія не відбулась, вона не може бути зафіксованою. Розглянемо кроки 1, 2, 4, 6, 8, які навпаки, є незалежними випадковими величинами $X_1, X_2, \ldots, X_n$, (n = 5). Припускаємо, що їх тривалості однаково розподілені за показниковим законом з параметром λ. Розподіл частості випадкових величин Y_1 описується законом Пуасона з параметром a.

Знайдемо закон розподілу та числові характеристики випадкової величини послідовності подій в СТУ:

$$Z = \sum_{i=1}^{Y} X_i \tag{13.4}$$

Закон розподілу суми $\sum_{i=1}^{n} X_i$ являє собою закон Ерланга (n-1)-го порядку з параметром λ.

$$f^{(n)}(x) = \frac{\gamma(\lambda x)^{n-1}}{(n-1)!} e^{-\lambda x} \quad x>0 \tag{13.5}$$

Згідно з формулою повної ймовірності густина розподілу випадкової величини z буде:

$$\varphi(z) = \sum_{n=1}^{\infty} f^{(n)}(z) P_n = \sum_{n=1}^{\infty} \frac{\lambda(\lambda z)^{n-1}}{(n-1)!} e^{-\lambda x} \frac{a^{n-1}}{(n-1)!} e^{-a} = \lambda e^{-\lambda x - a} \sum_{k=0}^{\infty} \frac{(\lambda z a)^k}{(k!)^2} \text{ при z>0.} \tag{13.6}$$

Ця густина може бути виражена через модифіковану циліндричну функцію

$$I_0(x) = \sum_{k=0}^{\infty} \frac{(x/2)^{2k}}{(k!)^2}; \tag{13.7}$$

$$\varphi(z) = \lambda e^{-\lambda z - a} I_0(2\sqrt{xza}) \text{ при } z=0.$$

Припустимо, що $Y = n$. Тоді умовне математичне очікування:

$$M[Z_n] = M\left[\sum_{i=1}^{n} X_i\right] = n m_x . \tag{13.8}$$

Повне математичне очікування:

$$m_z = M[Z] = \sum_{n=1}^{N} n m_x P_n = m_x m_y , \text{ де } m_y = \sum_{n=1}^{N} n P_n . \tag{13.9}$$

Отже,

$$M[z] = m_x m_y = \frac{a+1}{\lambda} . \tag{13.10}$$

За тієї ж умови $Y = n$, знайдемо умовний другий початковий момент:

$$M[Z_n^2] = M\left[\left(\sum_{i=1}^{n} X_i\right)^2\right] = \left[\sum_{i=1}^{n} X_i^2 + 2\sum_{i=j} X_i X_j\right] = nD_x + n_x^2 m_x^2 , \tag{13.11}$$

де $D_x = D[x_i] = \int_{-\infty}^{\infty} (x - m_x)^2 f(x) dx$.

Другий початковий момент випадкової величини z:

$$a_{2z} = M[Z^2] \sum_{n=1}^{N} M[Z_n^2] P_n = \sum_{n=1}^{N} (nD_x + n^2 m_x^2) P_n = D_x m_y + m_x^2 a_{2y} a_{2z} , \tag{13.12}$$

де $D_{2y} = \sum_{n=1}^{N} n^2 P_n = D_y + m_y^2$.

Дисперсія випадкової величини *z:*

$$D_z = a_{2z} - a_z^2 = D_x m_y + m_x^2 a_{2y} = D_x m_y + m_x^2 D_y . \quad (13.13)$$

Маємо остаточно

$$D[z] = D_x m_y + m_x^2 D_y = \frac{a+1}{\lambda^2} + \frac{a}{\lambda^2} = \frac{2a+1}{\lambda^2} . \quad (13.14)$$

Надані результати дають змогу вирішувати задачі обчислення числових характеристик процесу аудиту на основі статистики елементарних подій, знаходження періодичності перегляду і аналізу даних в залежності від важливості даних та ефективного використання продуктивності мережі.

13.5 Аудит інформаційної безпеки на відповідність міжнародному стандарту ISO/IEC 27001:2005

Міжнародний стандарт ISO/IEC 27001:2005 представляє собою перелік вимог до системи менеджменту інформаційної безпеки, обов'язкових для сертифікації. Стандарт встановлює вимоги до розробки, впровадженню, функціонуванню, моніторингу, аналізу, підтримки та вдосконалення документованої системи менеджменту інформаційної безпеки у контексті існуючих бізнес-ризиків організації.

Цей вид аудиту передбачає проведення таких робіт: підготовчого етапу, аналізу ризиків, розробки плану обробки ризиків, аналіз документації організації з системи менеджменту інформаційної безпеки,

На підготовчому етапі визначаються границі проведення аудиту, надаються вхідні дані щодо області діяльності системи менеджменту інформаційної безпеки замовника, виконавцем вивчаються вхідні дані, а за необхідності проводиться документальний опис області діяльності системи менеджменту інформаційної безпеки у відповідності з вимогами стандарту ISO/IEC 27001.

На етапі аналізу ризиків визначаються основні бізнес-процеси та технологічні процеси організації та їх взаємодія, виділяються істотні ресурси, розробляється й узгоджується із замовником методика оцінки ризиків, проводиться робота з оцінки ризиків із складанням детального звіту, визначаються прийнятні рівні ризиків, готується документ щодо прийняття остаточних ризиків.

На етапі розробки плану обробки ризиків дослджуються та аналізуються заходи захисту, які вже були визначені й реалізовані в організації. При цьому аналізуються:

- застосовані організаційні заходи в області планування, впровадження, аудиту й модернізації заходів із забезпечення інформаційної безпеки;

- використані програмно-технічні засоби та механізми захисту інформації.

На цьому ж етапі неодмінно розробляються додаткові заходи для зниження рівня ризиків, цілі й механізми контролю, які направлені на зниження ризиків. Етап завершується оформленням загального плану обробки ризиків.

На етапі аналізу документації організації в області системи менеджменту інфрмаційної безпеки аналізуються розроблені в організації політики, стандарти, процедури тощо, виробляються рекомендації з розробки організаційно-нормативної бази, необхідної для функціонування системи менеджменту інформаційної безпеки, документів, необхідність яких витікає з результатів аналізу ризиків та власних вимог організації до захисту інформації.

У результаті проведеного аудиту на відповідність міжародному стандарту ISO/IEC 27001 замовник отримує:

- опис області діяльності системи менеджменту інформаційної безпеки;
- методику визначення суттєвих активів та ресурсів;
- перелік суттєвих активів та ресурсів організації та їх цінність чи критичність;
- методику оцінки ризиків;
- звіт із оцінки ризиків;
- критерії для прийняття ризиків;
- заяву щодо ухвалення остаточних ризиків;
- план обробки ризиків;
- перелік політик, керівництв, процедур, інструкцій, необхідних для функціонування системи менеджменту інформаційної безпеки, а також рекомендації з їхньої розробки.

Стандарт ISO/IEC 27001 та ряд споріднених стандартів прийняті до застосування в Україні практично без змін. Підприємства, організації, що проводять свою діяльність в Україні, можуть добровільно проводити аудит і сертифікацію на відповідність цим стандартам, маючи на меті підвищити ефективність свого бізнесу і довіру споживачів та партнерів.

Контрольні запитання та завдання

1. Поясніть роль та значення аудиту інформаційної безпеки.
2. Дайте визначення поняття «аудит».
3. Назвіть та поясніть, що є результатом та вихідними документами аудиту.
4. Дайте визначення поняття «об’єкт аудиту».
5. Які є загальні принципи аудиту?
6. Дайте визначення універсального закону нерівності – закону Парето.
7. Що називають свідоцтвом аудиту, які критерії аудиту та принципи проведення аудиту?
8. Обґрунтуйте вплив на результативність аудиту мотивації керівництва та персоналу організації.

9. Поясніть основні положення кодексу аудитора інформаційної безпеки.

10. Чим відрізняється внутрішній аудит від зовнішнього?

11. Які є види аудиту за метою його проведення?

12. Де застосовуються періодичний та безперервний аудит?

13. Які є цілі проведення аудиту?

14. Які є етапи робіт з проведення аудиту?

15. Які види кримінальних злочинів у комп'ютерній сфері розглядаються законодавством?

16. Опишіть модель оцінки процесів забезпечення інформаційної безпеки.

17 Які є види вимірювання атрибутів процесів?

18. Які існують шкали вимірювання величин?

19. Як із часткових показників функціонування процесів формуються узагальнені та комплексні показники?

20. Поясніть основні принципи оцінювання інформаційної безпеки, яке засноване на моделі зрілості інформаційних процесів.

21. Наведіть основні характеристики системи безперервного аудиту інформаційної безпеки телекомунікаційних мереж.

22. Який зміст робіт з аудиту інформаційної безпеки на відповідність міжнародному стандарту ISO/IEC 27001:2005?

Завдання до самостійної роботи

1. Проаналізуйте цілі, етапи та метод проведення робіт зовнішнього аудиту:

- сформулюйте цілі зовнішнього аудиту інформаційної безпеки;
- які є етапи проведення робі зовнішнього аудиту?
- які роботи проводяться на етапі ініціації процедури аудиту?
- перелічіть та поясніть зміст робіт на етапі збору інформації аудиту.
- які методи аналізу даних аудиту застосовуються на етапі аналізу даних?
- які методи та розрахункові процедури використовуються на найбільш складному та важливому етапі – аналізу ризиків?
- які задачі виконуються на етапі використання методів аналізу ризиків?
- які методи використовуються і які документи створюються на етапах оцінки відповідності вимогам стандартів, вироблення рекомендацій та підготовки звітних документів?

2. Проаналізуйте визначення, алгоритми формування та вибору часткових, узагальнених та комплексних показників функціонування процесів.

3. Проаналізуйте завдання, цілі й зміст робіт та результуючі документи з аудиту інформаційної безпеки на відповідність міжнародному стандарту ISO/IEC 27001:2005

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ITU – (International Telecommunication Union) Міжнародний союз електрозв'язку

NGN – (Next Generation Networks) Мережі третього покоління

TCO – (Total Cost of Ownership) Загальна вартість володіння

АС – Автоматизована система

АТС – Автоматична телефонна станція

ВВС – Взаємодія Відкритих Систем

ДССЗЗІ – Державна служба спеціального зв'язку та захисту інформації

ЕОМ – Електронно-обчислювальна машина

ЕОД – Електронний обмін даними

ЕЦП – Електронний цифровий підпис

ЗМІ – Засоби масової інформації

ІБ – Інформаційна безпека

ІР – Інформаційні ресурси

ІС – Інформаційна система

ІКТ – Інформаційно-комунікаційні технології

ІТ – Інформаційні технології

КЗМЗ – Комплекс засобів і механізмів захисту

КЗІ – Комплексний захист інформації

КСЗІ – Комплексна система захисту інформації

КСІБ – Комплексна система інформаційної безпеки

ЛОМ – Локальна обчислювальна мережа

МПД – Мережа передавання даних

МЗК – Мережі загального користування

МТЗ – Міський телефонний зв'язок

МТС – Матеріально-технічні засоби

ОІД – Об'єкт інформаційної діяльності

ПЕМВН – Побічні електромагнітні випромінювання та наводок

РНБО – Рада національної безпеки та оборони

РСО – Режимно-секретний орган

СЗІ – Система захисту інформації

СЗН – Соціальний захист населення

СІБ – Система інформаційної безпеки

СЦЗІ – Соціальний захист інформації

ТЗІ – Технічний захист інформації

ТМЗК – Телекомунікаційні мережі загального користування

ФВА – Функціонально-вартісний аналіз

ФЗП – Фонд заробітної плати

ФПЗ – Функціональні послуги захисту

ЦСК – Цифрові системи комутації

СЛОВНИК ТЕРМІНІВ

Автентифікація повідомлень – метод, який використовується для виявлення несанкціонованих змінень, які вносяться до переданих електронних повідомлень, чи їхнього ушкодження.

Аудит – систематичний, незалежний та документований процес отримання свідоцтв аудиту та об'єктивного їх оцінювання з метою встановлення степені виконання узгоджених критеріїв аудиту.

Блокування інформації – дії, наслідком яких є припинення доступу до інформації.

Витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї.

Втрата інформації – дія, внаслідок якої інформація в автоматизованій системі перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі.

Виявлення загроз – дії по визначенню конкретних загроз і їхніх джерел, що приносять той або інший вид збитку.

Інформація – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, виробничих процесів, що спрямовані на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки.

Інформаційна безпека (у вузькому розумінні) – стан захищеності інформації підприємства від дестабілізуючого впливу зовнішніх та внутрішніх загроз.

Інформаційна безпека (у широкому розумінні) – складова національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз.

Інформаційний продукт (продукція) – документована інформація, підготовлена і призначена для задоволення потреб користувачів.

Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Інформаційна система – система оброблення даних засобами накопичення, зберігання, обновлення та їх пошуку і відображення.

Інформаційна послуга – дії суб'єктів щодо забезпечення споживачів інформаційними продуктами.

Інформаційний ресурс – сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо).

Інформаційне суспільство – суспільство з наступними головними прикметами:

- створюється мережа взаємопов’язаних загальнодоступних для кожного громадянина банків знань і даних;

- більшість трудящих зайняті у сфері послуг та виробництва інформації;

- інформація стає товаром і поряд з інформаційною технологією займає ключове місце у економіці.

Інформаційно-телекомунікаційна система – сукупність інформаційних та телекомунікаційних систем, які у процесі обробки інформації діють як єдине ціле.

Електронний цифровий підпис – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердні й його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Захист інформації – діяльність, яка спрямована на забезпечення конфіденційності, цілісності та доступності інформації в процесі одержання, зберігання, оброблення і поширення за допомогою організаційних, правових, технічних та економічних засобів.

Несанкціонований доступ – доступ до інформації, що здійснюється з порушенням встановлених в автоматизованій системі правил розмежування доступу.

Обробка інформації – вся сукупність операцій (збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних.

Оператор телекомунікацій – суб’єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій із правом на технічно обслуговування та експлуатацію телекомунікаційних мереж;

Особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу.

Підробка інформації – навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС (автоматизованих системах).

Провайдер телекомунікацій – суб'єкт господарювання, який має право на здійснення діяльності у сфері телекомунікацій без права на технічне обслуговування та експлуатацію телекомунікаційних мереж і надання в користування каналів електрозв'язку.

Припинення або локалізація загроз – дії, спрямовані на усунення діючої загрози і конкретних злочинних дій.

Ресурси телекомунікаційних мереж – наявні в телекомунікаційних мережах кількість номерів (номерний ресурс), кількість і пропускна спроможність проводових ліній з металевими жилами, оптичними волокнами, радіоліній, каналів, трактів для передавання інформації, комутаційних станцій та вузлів, радіочастотний ресурс.

Складові інформаційної безпеки підприємства - сукупність основних напрямів його інформаційної безпеки, істотно відмінних один від одного за своїм змістом.

Соціальний капітал – набір неофіційних вартостей чи норм, які є спільними для членів групи і дозволяють їм взаємодіяти.

Соціологічна інформація – документовані або публічно оголошені відомості про ставлення окремих громадян і соціальних груп до суспільних подій та явищ, процесів, фактів.

Соціальний захист інформації – вид захисту інформації, спрямований на забезпечення за допомогою організаційних та психологічних заходів, а за необхідності інженерно-технічних та криптографічних засобів, унеможливлення впливу на інформацію, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Споживач телекомунікаційних послуг (споживач) – юридична або фізична особа, яка потребує, замовляє та/або отримує телекомунікаційні послуги для власних потреб.

Суб'єкти ринку телекомунікацій – оператори, провайдери телекомунікацій, споживачі телекомунікаційних послуг, виробники та/або постачальники технічних засобів телекомунікацій.

***Телекомунікації (електрозв'язок*)** – передавання, випромінювання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводних, оптичних або інших електромагнітних системах.

Телекомунікаційна мережа – комплекс технічних засобів телекомунікацій та споруд, призначених для маршрутизації, комутації, передавання та/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Телекомунікаційна послуга – продукт діяльності оператора та/або провайдера телекомунікацій, спрямований на задоволення потреб споживачів у сфері телекомунікацій.

Телекомунікаційна система – сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб.

Управління інформаційною безпекою – забезпечування механізмів, які дозволяють реалізовувати інформаційну безпеку.

Чистий дисконтований доход – сучасна вартість майбутніх чистих грошових потоків, дисконтована на рівень граничної вартості капітальних вкладень.

Шифрування – перетворення електронного документа із застосуванням криптографічних методів з метою захисту його змісту.

ДОДАТОК А

НАВЧАЛЬНА ПРОГРАМА ДИСЦИПЛІНИ
„МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ”
(для студентів напряму 1601 Інформаційна безпека)

Модуль 1 – „Менеджмент інформаційної безпеки”

СТРУКТУРА ЗАЛІКОВОГО МОДУЛЯ 3

№ пп..	**Змістовий модуль**	Лекції (год.)	Заняття		Самостійна робота	Індивідуальна робота
			практ.	лаб.		
Модуль 3: ***Менеджмент інформаційної безпеки (1,5 кредити 54 год.)***						
1	Організаційно-правові основи системи управління інформаційною безпекою	4	2	-	2	-
2	Принципи, методи і технологія управління інформаційною безпекою	14	6	-	8	-
3	Організаційні основи і принципи діяльності служби захисту інформації	8	4	-	6	-
Разом модуль 3, год.		26	16	-	16	-

Зміст змістових модулів (лекційних годин):

1.1. Організаційно-правові основи системи управління інформаційною безпекою (4 год.). Висвітлюються основні поняття та задачі менеджменту інформаційної безпеки в умовах формування інформаційного суспільства та характеризується сучасна національна та міжнародна нормативна база у сфері інформаційної безпеки.

1.2 Принципи, методи і технологія управління інформаційною безпекою (14 год.). Розглядаються основні цілі, задачі та функції забезпечення інформаційної безпеки, джерела загроз та засоби їх впливу на об’єкти інформаційної безпеки, особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки. Детально вивчається технологічне управління інформаційною безпекою.

1.3 Організаційні основи і принципи діяльності служби захисту інформації (8 год.). Розглядаються методичні основи оцінки економічної доцільності захисту інформації та ризики інформаційної безпеки, особливості організації служби інформаційної безпеки підприємства та менеджменту персоналу у сфері інформаційної безпеки, а також перспективи розвитку інформаційної безпеки в Україні.

ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ

№ тижня	Місяць, числа тижня	Теми та зміст двогодинної лекції, додатковий матеріал самостійного вивчення, розглядувані питання	Години лекцій	Години самостійного вивчення	Номери семінарів, практ. занять, колоквіумів, контр. робіт	Література по темі
МОДУЛЬ № 3.3 Найменування: Менеджмент інформаційної безпеки **Навчальний час: лк – 26г., пр-12г., лб – 0г., СРС – 16г., кредитів ECTS – *1,5***						
1	8.02 – 14.02	ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ **Тема 1.** Основні поняття та задачі менеджменту інформаційної безпеки в умовах формування інформаційного суспільства	2	2	№ 1	1-9
2	15.02 – 21.02	**Тема 2.** Характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки	2	-		1-9
3	22.02 – 28.02	ПРИНЦИПИ, МЕТОДИ І ТЕХНОЛОГІЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ **Тема 3.** Основні цілі та задачі забезпечення інформаційної безпеки	2	2	№ 2	1-9
4	1.03 – 7.03	**Тема 4.** Складові інформаційної безпеки підприємства	2	-		1-9
5	8.03 –14.03	**Тема 5.** Особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки	2	2	№ 3	1-9
6	15.03 – 21.03	**Тема 6.** Забезпечення відтворення соціального капіталу	2	-		1-9
7	22.03 –28.03	**Тема 7.** Захист соціальної інформації та соціально-психологічний захист інформації	2	2		1-9
8	29.03 – 04.04	**Тема 8.** Технологічне управління інформаційною безпекою	2	-	№ 4	1-9
9	05.04 – 11.04	**Тема 9.** Технологічне управління інформаційною безпекою	2	2		1-9
10	12.04 – 18.04	ОРГАНІЗАЦІЙНІ ОСНОВИ І ПРИНЦИПИ ДІЯЛЬНОСТІ СЛУЖБИ ЗАХИСТУ ІНФОРМАЦІЇ **Тема 10.** Методичні основи оцінки економічної доцільності захисту інформації	2	-	№ 5	1-9
11	19.04 – 25.05	**Тема 11.** Ризики інформаційної безпеки	2	2		1-9
12	26.05 – 02.05	**Тема 12.** Організація служби інформаційної безпеки підприємства	2	2	№ 6	1-9
13	03.05 –09.05	**Тема 13.** Аудит інформаційної безпеки	2	2		1-9

ПЕРЕЛІК ПРАКТИЧНИХ ЗАНЯТЬ

Теми практичних занять модуля 3

„Менеджмент інформаційної безпеки”

№ пп.	Теми	Годин
1	Основні поняття та задачі менеджменту інформаційної безпеки в умовах формування інформаційного суспільства.	2
2	Основні цілі та задачі забезпечення інформаційної безпеки, складові інформаційної безпеки підприємства.	2
3	Особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки.	2
4	Технологічне управління інформаційною безпекою.	2
5	Методичні основи оцінки економічної доцільності захисту інформації та визначення ризиків інформаційної безпеки.	2
6	Організація служби інформаційної безпеки підприємства та менеджмент персоналу у сфері інформаційної безпеки.	2

ПЕРЕЛІК ЗНАНЬ І ВМІНЬ, ЯКІ ПОВИНЕН НАБУТИ СТУДЕНТ В ПРОЦЕСІ ВИВЧЕННЯ МАТЕРІАЛУ ДАНОГО МОДУЛЯ

Вихідні знання та уміння з модуля 3

№ пп.	Зміст знань	Шифр
1	Визначення основних понять у сфері інформаційної безпеки та основні задачі менеджменту інформаційної безпеки і характеризувати стан інформаційної безпеки в Україні	ЗН.1
2	Правові і нормативні акти, які визначають систему інформаційної безпеки	ЗН.2
3	Основні цілі, задачі, функції, складові системи інформаційної безпеки	ЗН.3
4	Особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки	ЗН.4
5	Оволодіти концептуальними моделями розробки, розподілення, обробки, використання та зберігання конфіденціальних документів, стратегією вибору систем виявлення атак, навичками роботи з пристроями безпеки в локальних і глобальних комп’ютерних мережах з метою використання їх, можливостей для покращення показників безпеки в них	ЗН.5
6	Існуючі методи оцінки інформаційної безпеки підприємства	ЗН.6
7	Основні методи, засоби та особливості організації служби інформаційної безпеки підприємства та вміти розробляти організаційну структуру служби інформаційної безпеки підприємства	ЗН.7
8	Особливості менеджменту персоналу у сфері інформаційної безпеки	ЗН.8
	Зміст умінь	
1	Характеризувати сучасну національну та міжнародну нормативну базу у сфері інформаційної безпеки	УМ.1
2	Визначати основні загрози та засоби їх впливу на об’єкти інформаційної безпеки та вміти застосовувати основні методи захисту конфіденційної інформації на підприємстві, приймати рішення про додержання чи наявність факту порушення конфіденційності інформації обмеженого доступу	УМ.2
3	Зафіксувати інформацію з додержання чи факту порушення конфіденційності інформації у відповідних документах	УМ.3

4	Вміти будувати архітектуру телекомунікаційних мереж відповідно до вимог інформаційної безпеки	УМ.4
5	Використовуючи діючі на підприємстві положення та інструкції про режимно-секретні підрозділи, в умовах забезпечення режиму секретності, уміти розробити план заходів для запобігання розголошення чи витоку відомостей, документації обмеженого доступу-під час виконання робіт з системами технічного захисту інформації	УМ.5
6	Вміти на практиці розраховувати оцінку витрат на створення і впровадження системи забезпечення інформаційної безпеки будь-якого підприємства	УМ.6
7	Використовуючи обчислювальну техніку, уміти на підставі плану та інструкцій з додержання основних характеристик інформаційної безпеки забезпечити цілісність, конфіденційність та доступність до інформаційних ресурсів	УМ.7
8	Складати виписки із нормативної та службової документації для передавання їх відповідальним особам, що задіяні у проведенні службових розслідувань за приписом керівництва та із дотриманням діючих норм та правил брати участь у проведенні службових розслідувань	УМ.8

ТЕСТИ ДЛЯ ПЕРЕВІРКИ ОДЕРЖАНИХ ЗНАНЬ І ВМІНЬ

Види тестів	Нумерація питань
Завдання – тести для перевірки знань і вмінь для обов'язкової частини програми модуля	1, 2, 3, 4, 5, 7, 8, 10, 12,13.
Завдання – тести для перевірки знань та вмінь більш поглибленного вивчення програми	6, 9, 11, 14,15.
Завдання – тести для ректорської та галузевих перевірок	1, 2, 3, 4, 5, 7, 8, 10, 12,13.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчик, С.М. Паук, В.Г. Потапов. – К.: МК-Пресс, 2005. – 288 с.

2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

3. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. – К.: Кондор, 2004. – 384 с.

4. Малюк А.А. Информационная безопасность: концептуальне и методологические основы защиты информации: Учеб. пособ. для вузов. – М: Горячая линия – Телеком, 2004. – 280 с.

5. Методика информационной безопасности / Сост. Ю.С. Уфимцев, В.П. Буянов, Е.А. Ерофеев и др. – М.: Экзамен, 2004. – 544 с.

6. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

7. Основи підприємництва, менеджменту та маркетингу в галузі зв'язку: Навч. посіб. / А.М. Богатирьов, Л.Д. Богатирьова, О.С. Редькін, Т.М.

Тардаскіна; За ред. д.е.н., проф. О.С. Редькіна: Ч.1. Основи підприємництва. – Одеса: ОНАЗ ім. О.С. Попова, 2007. – 212 с.

8. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации – К.: Юниор, 2003. – 504 с.

9. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособ. – М.: Академия, 2005. – 256 с.

ТЕСТИ ДЛЯ ПЕРЕВІРКИ ОДЕРЖАНИХ ЗНАНЬ

1. Інформаційна безпека – це:

а) стан захищеності системи, яка забезпечує формування та розвиток цієї системи в інтересах особистості, суспільства та держави;

б) захист інформації про стан нематеріальних активів і їхніх носіїв;

в) захист інформації про стан і рух матеріальних активів;

г) усі вищезгадані відповіді вірні.

2. Загрози інформаційній безпеці поділяються на:

а) суб'єктивні а об'єктивні;
б) навмисні та випадкові;
в) техногенні та антропогенні;
г) усі вищезгадані відповіді вірні.

3. Першочергові заходи забезпечення інформаційної безпеки повинні включати:

а) визначення складу, послідовності і порядку розробки законодавчих і нормативно-правових актів з питань інформаційної безпеки, а також механізмів їх введення в дію (правове забезпечення);

б) розробку і створення організаційної структури системи інформаційної безпеки України;
в) забезпечення реальних потреб системи інформаційної безпеки в кадрах, матеріально-технічних і фінансових коштах (ресурсне забезпечення);
г) усі вищезгадані відповіді вірні.

4. Складовими глобальної безпеки є:

а) інформаційна, політична, економічна;
б) інформаційна, військова, економічна, соціальна;
в) інформаційна, військова, економічна, політична;
г) інформаційна, військова, економічна, політична, соціальна.

5. Захист інформації:

а) стан захищеності інформації підприємства від дестабілізуючого впливу зовнішніх та внутрішніх загроз;

б) діяльність, яка спрямована на забезпечення конфіденційності, цілісності та доступності інформації в процесі одержання, зберігання, оброблення і поширення за допомогою організаційних, правових, технічних та економічних засобів;

в) захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати збитку власникам або користувачам інформації і підтримуючій інфраструктурі;

г) стан захищеності інформаційного середовища суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій і держави.

6. Витік інформації це:

а) результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

б) дії, наслідком яких є припинення доступу до інформації;

дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які в) мають право власності на неї в повному чи обмеженому обсязі.

7. Комерційна таємниця – це:

а) відомості, пов’язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) які може заподіювати збиток його інтересам;

б) відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їхнім бажанням відповідно до передбаченими ними умовами;

в) відомості, пов’язані з секретною інформацією, що включає відомості в сфері оборони, економіки зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може заподіяти шкоду життєво важливим інтересам України;

г) усі вищезгадані відповіді вірні.

8. Державна таємниця – це:

а) відомості, пов’язані з виробництвом, технологічною інформацією, управлінням, фінансами й іншою діяльністю підприємства, що не є державною таємницею, розголошення (передача, витік) які може заподіювати збиток його інтересам;

б) відомості, що знаходяться у володінні, користуванні або розпорядженні окремих фізичних або юридичних осіб і поширюються за їхнім бажанням відповідно до передбаченими ними умовами;

в) відомості, пов’язані з секретною інформацією, що включає відомості в сфері оборони, економіки зовнішніх відносин, державної безпеки й охорони правопорядку, розголошення яких може заподіяти шкоду життєво важливим інтересам України;

г) усі вищезгадані відповіді вірні.

9. Розвиток нормативно-правової бази стосовно інформаційної безпеки інформаційно-телекомунікаційних систем поділяють на:

а) два етапи;

б) три етапи;

в) чотири етапи;

г) п’ять етапів.

10. До методів захисту конфіденційної інформації на підприємстві відносяться:

а) правові методи;

б) програмно-технічні методи;

в) організаційно-економічні методи;

г) усі вищезгадані відповіді вірні.

11. Віброакустичний канал витоку це:

а) можливість прослуховування приміщень через природні і штучно створені отвори і щілини в стінах, стелях, через різні воздуховодні і вентиляційні шахти і т.д.;

б) можливість прослуховування приміщень за допомогою електроакустичних перетворень акустичних сигналів на електричні і включають перехоплення акустичних коливань через допоміжні технічні засобі й системи, яким є притаманний „мікрофонний ефект”, а також шляхом високочастотного нав’язування;

в) можливість прослуховування приміщень за допомогою електронних стетоскопів, що перетворять вібраційні коливання будівельних конструкцій в електричний сигнал;

г) усі вищезгадані відповіді вірні.

12. Перелічіть фактори, що впливають на стан інформаційної безпеки:

а)

б)

в)

13. Перелічіть відомі Вам методи за допомогою яких оцінюється доцільність витрат на забезпечення інформаційної безпеки підприємства:

а)

б)

в)

г)

д)

є)

ж)

з)

14. Перелічіть причини захисту відкритої інформації:

а)

б)

в)

г)

д)

15. Соціальний захист інформації це:

а) це вид захисту інформації, спрямований на забезпечення за допомогою організаційних та психологічних заходів, а за необхідності інженерно-технічних та криптографічних засобів, унеможливлення впливу на інформацію, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

б) діяльність, яка спрямована на забезпечення конфіденційності, цілісності та доступності інформації в процесі одержання, зберігання, оброблення і поширення за допомогою організаційних, правових, технічних та економічних засобів;

в) комплекс організаційних, правових і технічних заходів для запобігання загрозам інформаційної безпеки й усуненню їхніх наслідків.

ЛІТЕРАТУРА

1. Абалкин Л.И. Экономическая безопасность России: угрозы и их отражение // Вопросы экономики. – 1994. – № 12. – С. 4-13.

2. Абдеев Р.Ф. Философия информационной цивилизации. – М.: ВЛАДОС, 1994. – 336 с.

3. Алексеевский В.С. Синергетика менеджмента устойчивого развития: Монография. – Калуга: Манускрипт, 2006. – 328 с

4. Аничкин С.А. Протоколи информационно-вычислительных сетей: [Справочник] / С.А. Аничкин, С.А. Белов, А.В. Бернштейн и др.; Под ред. И.А. Мизина, А.П.Кулешова. − М.: Радио и связь, 1990. − 504 с.

5. Астахов А. Аудит безопасности информационных систем CISA. – 2002 – 23 с. – Режим доступу: http://www.iso27000.ru/chitalnyi-zai/audit-informacionnoi-bezopasnosti/audit-bezopasnosti-informacionnyh-sistem/

6. Ахромеева Т.С., Малинецкий Г.Г. Пятое «И» или вариации на темы развития // Институт прикладной математики им. М.В. Келдыша РАН (http://spkurdyumov.narod.ru/ahromeeva.htm). – 13 с.

7. Білорус О.Г. Економічна система глобалізму / НАН України. – К.: КНЕУ, 2003. – 360 с.

8. Безштанько В.М. Основні види загроз інформаційним активам організації. Бизнес и безопасность. №5 – 2006 – с.80.

9. Богатырева Л.Д, Тардаскина Т.М. Экономическая безопасность и ее основные характеристики // Azərbaycan Respublikasinin Rəhbərliyinə gəlməsinin 37-ci il dönümünə həsr olunmuş Beynəlxalq elmi-praktik konfrans. – Mingəçevir, 2006. – С. 243-250.

10. Бонгард М.М. Проблема узнавания. – М.: Наука, 1967. – 320 с.

11. Бондаренко М., Скрыпник Л, Потий А. Перспективы применения международного стандарта ISO/IEC в Украине // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2001. – Вип. 3. – С. 7-26.

12. Браіловський М., Дорошко В. Підготовка фахівців з інформаційної безпеки для підрозділів органів внутрішніх справ // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2004. – Вип. 8. – С. 154-159.

13. Брединский А. Люди – источник конфиденциальной информации // Защита информации. Конфидент. – 2004. – № 1. – С. 32-35.

14. Бриллюэн Л. Наука и теория информации / Пер. с англ. А.А. Харкевича. – М.: Физматиз, 1960. – 392 с.

15. Бриллюэн Л. Научная неопределенность и информация / Пер. с англ. Т.А. Кузнецовой; Под ред. и с пред. д.ф.н., проф. И.В. Кузнецова. – М.: Мир, 1968. – 272 с.

16. Великий тлумачний словник сучасної української мови / Уклад. і голов. ред. В.Т. Бусел. – К.: Ірпінь: ВТФ „Перун”, 2002. – 1440 с.

17. Велленройтер Х. Функционально-стоимостной анализ в рационализации производства / Сокр. пер. с нем. В.В. Просветова; Предисл. Б.И. Майданчика. – М.: Экономика, 1984. – 111 с.

18. Вернадский В.И. Химическое строение биосферы Земли и ее окружения. – М.: Наука, 1965. – 286 с.

19. Винер Н. Кибернетика или управление и связь в животном и машине / Пер. с англ. И.В. Соловьева и Г.Н Поварова. – 2-е изд. – М.: Советское радио, 1968. – 328 с.

20. Воробиенко П.П., Нечипорук О.Л., Щербина Ю.В. Модели угроз информационным ресурсам систем и сетей связи // Зв'язок. – 2003. – № 6. – С. 39-41.

21. Воробиенко П., Нечипорук О., Щербина Ю. Принципы построения моделей угроз информационным ресурсам систем и сетей связи // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2003. – Вип. 7. – С. 11-13.

22. Гайдай Ю.В. Становлення концептуальних основ процесу економічної глобалізації // Економіка: проблеми теорії та практики: Зб. наук. праць. – Дніпропетровськ, 2005. – Т.1, вип. 208. – С. 223-235.

23. Гафт М.Г. Методы оценки технического уровня. Интерактивный подход // Проблемы информационных систем. – 1987. – № 2. – С. 11-21.

24. Герасименко В.А., Малюк А.А. Основы защиты информации. – М.: МИФИ, 1997. – 538 с.

25. Герасименко В.А. Защита информации в автоматизированных системах обработки даннях: В 2-х кн. – М.: Энергоатомиздат, 1994. – 432 с.

26. Глазьєв С.Ю. Развитие российской экономики в условиях глобальных технологических сдвигов // Научный доклад. М.: НИР, 2007. (http://spkurdyumov.narod.ru/GlazyevSUr.htm). – 78 с.

a. Глобализация и безопасность развития: (Монография) / О.Г. Белорус, Д.Г. Лукьяненко и др.; НАН Украины; Ин-т мировой экономики и международных отношений. – К.: КНЕУ, 2001. – 733 с.

b. Глобальные трансформации и стратегии развития; Под ред. О.Г. Белоруса. – К.: Орияне, 2000. – 424 с.

c. Голибардов Е.И., Кудрявцев А.В., Синенко М.И. Техника ФСА. – К.: Тєхника, 1989. – 239 с.

30. Горицький В.М. Сучасний стан і перспективи розвитку інформаційного суспільства в Україні // II Науково-практична конференція „Безпека інформаційно-комунікаційних технологій", 2005. – Київ: Діпрозв'язок. – С. 8.

31.Гукасьян Г.М. Экономическая теория: проблемы „новой экономики". – 2-е изд. – С.Пб: Питер. 2003. – 192 с.

32. Данилов-Данильян В.И. Устойчивое развитие (теоретико-методологический анализ) // Экономика и математические методы. Т.39, № 2. 2003. С. 123–135.

33.Домарев В.В. Безопасность информационных технологий. – С.Пб.: ДиаСофтЮП, 2004. – 992 с.

34. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.: Диасофт, 1999. – 480 с.

35. Джонс Дж. К. Методы проектирования / Пер. с англ. – 2-е изд., доп. – М.: Мир, 1986. – 326 с.

36. ДСТУ 3396.0-96. Захист інформації. Технічний захист інформації. Основні положення. – Введ. 01.01.1997. – К.: Держстандарт України, 1996. – 7 с. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

37. ДСТУ 3396.1-96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. – Введ. 01.07.1997. – К.: Держстандарт України, 1997. – 11 с. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

38. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.1998. – К.: Держстандарт України, 1997. – 15 с. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

39. ДСТУ ISO 15408-1: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 1. Вступ і загальна модель. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

40. ДСТУ ISO 15408-2: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 2. Функціональні вимоги безпеки. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

41. ДСТУ ISO 15408-3: 2005. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій. Частина 3. Вимоги до забезпечення захисту. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

42. ДСТУ ISO 17799: 2005. Інформаційні технології. Методи захисту. Практичні рекомендації з управління інформаційної безпеки. – Режим доступу: http://www.iso-17799.com

43. ДСТУ ISO/IEC TR 13335-1: 2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина. 1. Концепції і моделі безпеки. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

44. ДСТУ ISO/IEC TR 13335-2: 2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина. 2. Керування та планування безпеки. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

45. ДСТУ ISO/IEC TR 13335-3: 2003. Інформаційні технології. Настанови з керування безпекою інформаційних технологій (IT). Частина. 3. Методи керування захистом. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

46. ДСТУ ISO/IEC TR 13335-4: 2005. Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання

засобів захисту. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

47. ДСТУ ISO/IEC TR 13335-5: 2005. Інформаційні технології (IT). Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html

48. Ерофеев А.А., Поляков А.О. Интеллектуальные системы управления. – С.Пб.: С.ПбГТУ, 1999 – 264 с.

49. Ершова Т.В. Концептуальные вопросы перехода к информационному обществу XXI века. – Режим доступу: http://intra.rfbr.ru/pub/vestnik/V3_99/1_5.htm#4

50. Єршов Ю.В. Європейський вибір України та побудова інформаційного суспільства // Современные проблемы телекоммуникаций: Сб. докладов 6-й Международной научно-технической конференции. Одеса, 19-22 августа, 2003 г. – Одесса, 2003. – Ч.1. – С.161-163.

51. Закон України „Про Службу безпеки України" від 25.03.1992 р. № 2229-XII. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40966&cat_id=38828

52. Закон України „Про інформацію" від 02.10.1992 р. № 2657-XII. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40968&cat_id

53. Закон України „Про захист інформації в автоматизованих системах" від 5.06.1994 р. № 81/94-ВР. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40966&cat_id=38828

54. Закон України „Про наукову і науково-технічну експертизу" від 10.02.1995 р. № 51/95-ВР. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40958&cat_id=38828

55. Закон України „Про Національну програму інформатизації" від 04.02.1998 р. № 74/98-ВР. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=74%2F98%2D%E2%F0&p=1181903521686018

56. Закон України „Про державну таємницю" від 21.09.1999 р. № 1079-XIV. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=40966&cat_id=38828

57. Закон України „Про Національну систему конфіденційного зв'язку" від 10.01.2002 р. № 2919-III. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=43399&cat_id=38828

58. Закон України „Про основи національної безпеки України" від 19.06.03 р. № 964-IV. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=43411&cat_id=38828

59. Закон України „Про електронний цифровий підпис” від 22.05.2003 р. № 852- IV. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=852-15

60. Закон України „Про електронні документи та електронний документообіг” від 22.05.2003 р. № 851-IV. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=851-15

61. Закон України „Про телекомунікації” від 18.11.03 р. № 1280-IV. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1280%2D15&p=1

62. Закон України „Про захист інформації в інформаційно-телекомунікаційних системах” від 31.05.2005 р. №2594-IV. – Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=43417&cat_id=38828

63. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 09.01.07 р. № 537-V. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1280%2D15&p=1

64. Защита информации в телекоммуникационных системах / Г.Ф. Конахович, В.П. Климчик, С.М. Паук, В.Г. Потапов. – К.: МК-Пресс, 2005. – 288 с.

65. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

66. Иноземцев В.Л. На рубеже эпох. Экономические тенденции и их неэкономические следствия. – М.: Экономика, 2003. – 703 с.

67. Информационная безопасность в условиях информатизации общества. – Режим доступу: http://www.ase.moldnet.md/~osa/Publication/pubru06.html

68. Кабелев Д., Князев А., Ловцов Д. Теоретико-концептуальный подход к проблеме качества и ценности информации в эргасистеме // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2003. – Вип. 7. – С. 25-31.

69. Кадомцев Б.Б, Рыдник В.И. Волны вокруг нас. – М.: Знание, 1981. – 151 с.

70. Калашников М., Русов Р. Сверхчеловек говорит по-русски. Историко-футуристическое расследование. – М.: АСТ. Астрель, 2006. – 639 с.

71. Калюжний Р., Гавловський В., Цимбалюк В. Питання державного управління у сфері інформаційної безпеки в умовах переходу України до інформаційного суспільства (організаційно-правовий аспект) // Суспільні реформи та становлення громадянського суспільства в Україні: Матеріали науково-практичної конференції. Київ, 30 травня 2001 р. – Київ, 2001. – С. 292-297.

72. Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ; Под науч. ред. О.И. Шкаратана – М.: ГУ ВШЭ, 2000. – 608 с.

73. Килин С.Я. Квантовая информация // Успехи физических наук. – 1999. – Т. 169, № 5. – С. 509-527.

74. Кільчицький Є.В., Перевозчикова О.А., Савельєв Д.Ю. Центральний засвідчувальний орган національної системи електронного цифрового підпису починає діяти // Зв'язок. – 2005. – № 5. – С. 18-21.

75. Клейнер Г.Б., Тамбовцев В.Л., Качалов Р.М. Предприятие в нестабильной экономической среде: риски, стратегии, безопасность. – М.: Экономика, 1997. – 288 с.

76. Климов С.М. Интеллектуальные ресурсы общества. – С.Пб.: ИВЭСЭП, Знание, 2002. – 199 с.

77. Князєва Н.О., Баландін І.О. Методика розрахунку собівартості послуг місцевого телефонного зв'язку // Зв'язок. – 2005. – №1. – С. 9-15.

78. КНД 45-076-98. Система автоматизованого телефонного зв'язку для мереж загального користування. Основні положення. – Режим доступу: http://www.stc.gov.ua

79. КНД 45-164-2001. Технічний захист інформації в галузі зв'язку України. Типова модель загроз для інформаційних ресурсів цифрових АТС, що використовуються в мережах електрозв'язку загального користування України. – Режим доступу: http://www.stc.gov.ua

80. Коган И.М. Прикладная теория информации. – М.: Радио и связь, 1981. – 216 с.

81. Колмогоров А.Н. Основные понятия теории вероятностей. –2-е. изд. – М.: Наука, 1974. – 119 с.

82. Кононович В., Тардаскин Н., Тардаскина Т. Функционально-стоимостной анализ системы обеспечения информационной безопасности телекоммуникационных сетей общего пользования // Безопасность информации в информационно-телекоммуникационных системах: Тезисы докладов VIII Международной научно-практической конференции. Киев, 11-13 мая 2005 г. – Киев, 2005. – С.55-56.

83. Кононович В.Г., Тардаскіна Т.М. Цінність інформації з точок зору інформаційної безпеки // Системы и средства передачи и обработки информации: Труды VIII Международной научно-практической конференции. Одесса, 7-12 сентября 2004 г. – Одесса, 2004. – С. 70-72.

84. Кононович В.Г., Тардаскін М.Ф. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування // Захист інформації, № 1, 2006. – 18-30 с.

85. Кононович В.Г., Кононович І.В., Тардаскіна Т.М. Передумови перебудови професійної освіти внаслідок розвитку нанотехнологій // Наукові праці ОНАЗ ім. О.С. Попова. – 2008. – № 1. – С. 88-95.

86. Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Парламент, 1999. – 95 с.

87. Концепція розвитку телекомунікацій в Україні до 2010 року № 316 від 7.06.2006 р. – Режим доступу: http://www.zakon1.rada.gov.ua

88. Концепція технічного захисту інформації в Україні. – 1997. – Режим доступу: http://www.zakon1.rada.gov.ua

89. Концепція технічного захисту інформації в галузі зв'язку України. – 1999. – Режим доступу: http://www.zakon1.rada.gov.ua

90.Копейкин Г.К., Лапина Н.А. Психологические аспекты информационной безопасности организации // Защита информации. Конфидент. – 2003. – №3. – С. 35-37.

91.Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посіб. – К.: Кондор, 2004. – 384 с.

92. Кравченко В.П. Система поддержки принятия решений. – Режим доступу: http://www.it2b.ru/it2b2.viev5.page21.html.

93. Курило А.П., Зефиров С.Л., Голованов В.Б. Аудит информационной безопасности. М.: Издательская группа «БДЦ-пресс». – 2006. – 304 с.

94. Крутских А. Информационный вызов безопасности на рубеже XXI века //Меж-дународная жизнь. – 1999. – № 2. – С. 82-89.

95. Лачинов В.М., Поляков А.О. Информодинамика или путь к Миру открытых систем. – С.Пб: С.ПбГТУ, 1999. – 364 с. – Режим доступу: http//www.polyakov.com/informodynamiks.

96.Ліцензійні умови провадження діяльності у сфері телекомунікацій з надання послуг фіксованого міжнародного міжміського, місцевого зв'язку з правом технічного обслуговування та експлуатації телекомунікаційних мереж і надання в користування каналів електрозв'язку (Наказ Держкомзв'язку № 132 від 17.06.2004 р.). – Режим доступу: http://mintrans.kmu.gov.ua/mintrans/control/uk/publish/category?cat_id=39278&page=7

97.Ліцензійні умови провадження діяльності у сфері телекомунікацій з технічного обслуговування і експлуатації мереж ефірного теле- та радіомовлення та телемереж, надання в користування каналів електрозв'язку" (Наказ Міністерства транспорту та зв'язку України № 984 від 10.11.2004 р.). – Режим доступу: http://mintrans.kmu.gov.ua/mintrans/control/uk/publish/category?cat_id=39278&page=7

98.Лукінов І.І. Економічні трансформації (наприкінці XX сторіччя). — К: НАН України, Ін-т економіки, 1997. – 455 с.

99.Малюк А.А. Информационная безопасность: концептуальне и методологические основы защиты информации: Учеб. пособ. для вузов. – М: Горячая линия – Телеком, 2004. – 280 с.

100. Манойло А. В., Петренко А. И., Фролов Д. Б. Государственная информационная политика в условиях информационно-психологической войны. – М.: Горячая линия – Телеком, 2003. – 541 с.

101. Матов О.Я., Василенко В.С., Будько М.М. Визначення залишкового ризику при оцінці захищеності інформації в інформаційно-телекомунікаційних системах // Реєстрація, зберігання і обробка даних. − 2004. − Т. 6, № 2. − С. 62-74.

102. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. − М.: МГУ, 1999. − 208 с.

103. Методика информационной безопасности / Сост. Ю.С. Уфимцев, В.П. Буянов, Е.А. Ерофеев и др. – М.: Экзамен, 2004. – 544 с.

104. Митилино С. Безопасность и человеческий фактор // Компьютерное обозрение. – 2001. – № 27. – С. 42-43.

105. Моисеев Н.Н. Информационное общество как этап новейшей истории // Сводная мысль. – 1996. – №1. – С. 76-82.

106. Моисеев Н. Стратегия разума // Знание-сила. – 1986. – №3. – С.32-35.

107. Моисеев Н. Стратегия разума // Знание-сила. – 1986. – №10 – С. 24-27.

108. Моль А., Фукс В., Касслер М. Искусство и ЭВМ. – М.: Мир, 1975 – 556 с.

109. НД ТЗІ 1.1-003-99. Термінологія у галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40393&cat_id=38835

110. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40396&cat_id=38835

111. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах НД від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40386&cat_id=38835

112. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40381&cat_id=38835

113. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39738&cat_id=38835

114. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40374&cat_id=38835

115. НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супровадження і модернізації засобів технічного захисту інформації від несанкціонованого доступу. – Режим доступу:
http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=39726&cat_id=38835

116. НД ТЗІ 1.1-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Основні положення. – Режим доступу:

http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40371&cat_id=38835

117. НД ТЗІ 2.5-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40368&cat_id=38835

118. НД ТЗІ 2.5-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації гарантій захисту. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40345&cat_id=38835

119. НД ТЗІ 2.5-003-99. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації довірчих оцінок коректності реалізації захисту. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40342&cat_id=38835

120. НД ТЗІ 2.7-001-99. Технічний захист інформації на програмно-керованих АТС загального користування. Порядок виконання робіт. – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40339&cat_id=38835

121. НД ТЗІ 3.7-002-99. Технічний захист інформації на програмно-керованих АТС загального користування. Методика оцінювання захищеності інформації (базова). – Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=40336&cat_id=38835

122. НД ТЗІ 2.1-001-2001. Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

123. НД ТЗІ 2.5-008-2002. Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

124. Несвіт Г.П. Інформаційна політика держави як фактор реформування суспільства: Автореф. дис. … кандидата політ. наук / Одес. нац. юрид. акад. – Одеса, 2001. – 16 с.

125. Носов В., Манжай А. Метод проектирования оптимальной системы защиты информации // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць.– Київ, 2004. – Вип.8. – С. 94-103.

126. Організація і сучасні методи захисту інформації; За заг. ред. С.А. Дієва та А.Г. Шаваєва – М., 1998. – 52 с.

127. Организация планирование и управление предприятиями связи / Е.В. Демина, Е.К. Иодко, Л.И. Майофис, Н.П. Резникова. – М.: Радио и связь, 1990. – 352 с.

128. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия – Телеком, 2006. – 544 с.

129. Основи підприємництва, менеджменту та маркетингу в галузі зв'язку: Навч. посіб. / А.М. Богатирьов, Л.Д. Богатирьова, О.С. Редькін, Т.М. Тардаскіна; За ред. д.е.н., проф. О.С. Редькіна: Ч.1. Основи підприємництва. – Одеса: ОНАЗ ім. О.С. Попова, 2007. – 212 с.

130. Основи підприємництва, менеджменту та маркетингу в галузі зв'язку: Навч. посіб. / А.М. Богатирьов, Л.Д. Богатирьова, О.С. Редькін, Т.М. Тардаскіна; За ред. д.е.н., проф. О.С. Редькіна: Ч.2. Основи менеджменту та маркетингу. – Одеса: ОНАЗ ім. О.С. Попова, 2007. – 176 с.

131. Павленко Л. Деякі аспекти фінансово-кредитної безпеки як складової економічної безпеки України // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2004. – Вип. 9. – С. 47-56.

132. Панарин И.Н. Информационная война и третий Рим. – Режим доступу: http://top100.km.ru/reader.asp?id=34064&page=1&viewBy=8000&sizechars=150) – 132 с.

133. Пастернак-Таранушенко Г. Економічна безпека держави. Статика процесу забезпечення: Підручник для державних службовців, науковців, студентів і аспірантів вищих навчальних закладів економічного профілю / За ред. проф. Б. Кравченка. – К.: Кондор, 2002. – 302 с.

134. Пастернак-Таранушенко Г. Результаты исследования путей обеспечения экономической безопасности Украины // Экономика Украины. – 1999. – № 2. – С. 21-28.

135. Пастернак-Таранушенко Г. Экономическая и национальная безопасность Украины // Экономика Украины. – 1994. – №2. – С. 51-57.

136. Петренко С. А., Симонов С. Экономически оправданная безопасность // Журнал IT Manager. – 2004. – № 15(3).– С. 23.

137. Петренко С.А., Терехова Е.М. Оценка затрат на защиту информации // Защита информации. INSIDE. – 2005. – №1. – С. 36-48.

138. Петренко С.А., Терехова Е.М. Обоснование инвестиций в безопасность // Защита информации. INSIDE. – 2005. – №1. – С. 49-53.

139. Петренко С.А. Методические основы защиты информационных активов компании. – Режим доступу: http://www.infosecurity.ru/-gazeta/content/031104/article03.-html.

140. Плескач В.Л., Гладун А.Я. Усовершенствование информационной инфраструктуры предприятий в электронном бизнесе // Бизнес и безопасность. – 2005. – № 4-5. – С. 57-59.

141. Плоткин Я.Д., Львов Д.С. Экономическая эффективность новой техники. – Львов: Вища школа, 1986. – 143 с.

142. Попов А.Б. Функционально-стоимостной анализ // Изобретатель в рационализатор. – 1985. – №6. – С. 26-27.

143. Поповский В.В., Персиков А.В. Защита информации в телекоммуникационных системах: Учебник: В 2-х т. – Харьков: ООО „Компания СМИТ”, 2006. – Т.2. – 292 с.

144. Поппер К.Р. Открытое общество и его враги. Т.1: Чары Платона; Т.2: Время лжепророков: Гегель, Маркс и другие оракулы / Пер. с англ.; Под ред. В.Н. Садовского. – М.: Феникс, Международный фонд "Культурная инициатива", 1992. – Т.1. – 448 с.; Т.2. – 528 с.

145. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Проект ДССЗЗІ від 20.02.2008. – С. 3.

146. Порядок захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Затверджено наказом ДСТСЗІ СБ України № 76 від 24.12 2001. – С. 4.

147. Постанова з керування безпекою інформаційних технологій. ДСТУ ISO/IEC TR 13335:2003 року.

148. Потій О., Лєншин А. Методика визначення думок експертів відносно зрілості безпеки інформації із застосуванням математичного апарату суб’єктивної логіки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2004. – Вип. 9. – С. 38-47.

149. Почепцов Г.Г. Информационные войны. – М.: Рефл-бук, – 2001. – 576 с.

150. Пригожин И., Стенгерс И. Порядок из хаоса: Новый диалог человека с природой / Пер. с англ.; Общ. ред. Ю.В. Аршинова, Ю.Л. Климонтовича и Ю.В. Сачкова. – М.: Прогресс, 1986. – 432 с.

151. Проценко Т., Шамрай В. Основні напрямки інформатизації державного управління в процесі становлення громадянського суспільства // Вісник УАДУ. – 2002. – № 1. – С. 339-344 с.

152. Пунченко О.П., Тардаскіна Т.М. Стратегія побудови та розвитку інформаційного суспільства // Науковий журнал „Перспективи”. – 2005. – № 2 (30). – С. 8-18.

153. Ракитов А.И. Философия компьютерной революции. – М.: Политиздат, 1991. – 286 с.

154. Рейман Л.Д. Информационное общество и роль телекоммуникаций в его становлении // Вопросы философии. – 2001. – №3. – С.3-10.

155. Расторгуев С.П. Информационная война. – М.: Радио и связь, 1998. – 416 с.

156. Редькін О.С., Тардаскіна Т.М. Функціонально-вартісний аналіз системи інформаційної безпеки АТС // Економічний вісник Національного гірничого університету. – 2005. – № 4 (12). – С. 47-53.

157. Редькін О.С., Тардаскіна Т.М. Вплив глобальних процесів на інформаційну безпеку // Вісник соціально-економічних досліджень: Зб. наук. праць. – Одеса, 2006. – Вип. 22. – С. 307-311.

158. Редькін О.С., Тардаскіна Т.М. Кадрова політика системи інформаційної безпеки // Маркетинг: теорія і практика: Зб. наук. праць. – Луганськ, 2006. – № 12. – С. 199-205.

159. Ресурс Российской сети информационного общества (Russian Information Society Network). – Режим доступу: http://www.isn.ru.

160. Ролкер Б. Дж., Блей Я.Ф. Безопасность ЭВМ и организация их защиты. – М.: Связь, 1980. – 112 с.

161. Рубан В.Я. Інформаційна безпека України: сутність та проблеми // Стратегічна панорама. – 1998. – № 3-4. – С. 170.

162. Савин В.Л. Некоторые аспекты экономической безопасности России // Международный бизнес России. – 1995. – № 9. – С. 14-16.

163. Словарь иностранных слов; Под ред. Л.С. Шаумяна – 15-е изд., испр. – М.: Русский язык, 1988. – 608 с.

164. Словарь русского языка / Сост. С.И. Ожегов. – 15-е изд. – М.: Русский язык, 1987. – 750 с.

165. Советский энциклопедический словарь; Под ред. А.М. Прохорова. – 2-е изд. – М.: Сов. энциклопедия, 1982. – 1600 с.

166. Современные телекоммуникации; Под ред. С.А. Довгого. – М.: Эко-Трендз, 2003. – 320 с.

167. Стеклов В.К., Кільчицький Є.В. Основи управління мережами та послугами телекомунікацій. Підруч. для студ. вищ. навч. закл. за напрямом „Телекомунікації”; За ред. проф. В.К. Стеклова – К.: Техніка, 2002. – 438 с.

168. Стеклов В.К., Беркман Л.Н. Нові інформаційні технології: Транспортні мережі телекомунікацій. – К.: Техніка, 2004. – 488 с.

169. Стратонович Р.Л. Теория информации. – М.: Сов. Радио, 1975. – 424 с.

170. Сяо Д., Керр Д., Медник С. Защита ЭВМ; Пер. с англ. – М.: Мир, 1982. – 264 с.

171. Тамбовцев В.Л. Формальное и неформальное в управление экономикой / Отв.ред. Е.З. Майминас. – М.: Наука, 1990. – 92 с.

172. Тамбовцев В.Л. Экономическая безопасность хозяйственных систем: структура проблемы // Вестник Московского государственного университета. – 1995. – № 3. – С. 3-9.

173. Тардаскін М.Ф. Особливості стратегії інформаційної безпеки цифрових автоматичних телефонних станцій // Зв’язок. – 2005. – № 1. – С. 31-33.

174. Тардаскін Н.Ф., Кононович В.Г., Тардаскіна Т.М. Моделі цінності інформації з позицій інформаційної безпеки інформаційно-телекомунікаційних систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2004. – Вип. 9. – С. 30-38.

175. Тардаскін М.Ф., Кононович В.Г., Тардаскіна Т.М. Основи концепції системи інформаційної безпеки телекомунікаційних мереж загального користування // Зв’язок. – 2006. – № 3. – С. 15-22.

176. Тардаскін М., Кононович В., Севостяненко А. Модель аудиту безпеки системи технологічного управління телекомунікаційними мережами. //

Науково-техн. збірник “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні” – вип. 3. – 2001. – С. 196 – 201.

177. Тардаскіна Т.М. Аналіз проблеми управління опором персоналу у процесі стратегічних змін // Системы и средства передачи и обработки информации: Труды VIII Международной научно-практической конференции. Одеса, 7-12 сентября 2004 г. – Одесса, 2004. – С. 193.

178. Тардаскіна Т.М. Управління персоналом системи інформаційної безпеки // Економіка: проблеми теорії та практики: Зб. наук. праць. – Дніпропетровськ, 2005. – Т.1, вип. 208. – С. 290-294.

179. Тардаскіна Т.М. Роль управління персоналом в системі інформаційної безпеки // Системи і засоби передачі і обробки інформації: Праці IX Міжнародної науково-практичної конференції. Черкаси, 5-10 вересня 2005 р. – Черкаси, 2005. – С. 230-232.

180. Тардаскіна Т.М. Оцінка витрат на систему інформаційної безпеки телекомунікаційних мереж // Економіка і управління. – 2006. – № 4. – С. 73-78.

181. Тардаскіна Т.М. Суть інформації та її роль в економіці та менеджменті // Вісник Хмельницького національного університету. – 2006. – Т.1, № 6. – С. 175-180.

182. Тардаскіна Т.М. Підходи до оцінки витрат на підтримку та створення системи інформаційної безпеки // Інформаційні технології в економіці, менеджменті і бізнесі. Проблеми науки, практики і освіти: Матеріали XI Міжнародної науково-практичної конференції. Київ, 24-25 листопада 2005 р. – Київ, 2006. – Т3. – С. 286-288.

183. Тардаскіна Т.М. Тенденції становлення інформаційної економіки // XII Международный молодежный форум „Радиоэлектроника и молодежь в XXI веке”: Сб. материалов форума. Харьков, 10-12 апреля 2006 г. – Харьков, 2006. – С. 660.

184. Тардаскіна Т.М. Нові підходи до інформаційної безпеки телекомунікаційних мереж // Світ інформації та телекомунікацій-2006: Матеріали III Міжнародної науково-технічної конференції студентства та молоді. Київ, 26-27 квітня 2006 р. – Київ, 2006. – С. 110.

185. Тардаскіна Т.М. Оцінка ризиків системи інформаційної безпеки // Міжнародні тенденції розвитку бухгалтерського обліку і аудиту та перспективи для України: Тези доповідей міжнародної науково-практичної конференції. Київ, 19 травня 2006 р. – Київ, 2006. – С.185-186.

186. Тардаскіна Т.М. Вплив економічної глобалізації на інформаційну безпеку // Украина в системе современных цивилизаций: трансформации государства и гражданского общества: Материалы международной научно-практической конференции. Одеса, 23-24 червня 2006 р. – Одеса, 2006. – С. 80-81.

187. Тардаскіна Т.М. Залежність цінності інформації від показників конфіденційності, доступності та цілісності // Соціально-економічні напрямки розвитку регіонів в контексті сучасних процесів міжнародної інтеграції: Матеріали міжнародної науково-практичної конференції студентів і молодих вчених. Херсон, 16-19 вересня 2006 р. – Херсон, 2006. – С. 259-262.

188. Тардаскіна Т.М. Функціонування соціального капіталу в умовах інформатизації суспільства // Інноваційні технології в науці, підготовці та перепідготовці фахівців: Матеріали міжнародної науково-практичної конференції. Одеса, 17-18 травня 2007 р. – Одеса, 2007. – С. 38-40.

189. Тардаскина Т.Н. Организационно-экономические составляющие информационной бзопасности в системе управления телекоммуникациями // Проблемы современной радиотехники, телевидения и связи: Труды Международной научно-технической конференции посвященной 50-летию телевидения и 80-летию радио в Азербайджане. Баку, 4-6 июня 2007 г. – Баку, 2007. – С. 291-296.

190. Тейяр де Шарден П. Феномен человека / Пер. с фр. Н.А. Садовского / Предисл. и примеч. А.С. Раутиана. – М.: Устойчивый мир, 2001. – 231 с.

191. Тесля В.Я., Бабосюк А.Л., Сикорский В.В., Рудниченко А.Е. Концептуальные подходы к технологии сетей нового поколения NGN // Зв'язок. – 2004. – № 2. – С. 70-73.

192. Толстой В. Информатизация общества: анализ проблем и поиск решений. – М.: ВНИИ-СИ, 1989. – 96 с.

193. Ушаков В.А. Становление информационной системы: ценностные характеристики // Проблемы современной экономики. – 2002. – №3/4. – С. 12-18.

194. Федоренко Н.В., Пархоменко П.Н., Пархоменко Н.Г. Многоуровневая модель понятійного апарата в области информационного права и информационной безопасности // Защита информации. Конфидент. – 2004.– № 3. – С. 18-24.

195. Философский словарь; Под ред. И.Г. Фролова. – 5-е изд. – М.: Политиздат, 1987. – 462 с.

196. Философский энциклопедический словарь / Сост.: Е.Ф. Губский, Г.В. Кораблева, В.А. Лутченко. – М.:ИНФРА, 1997. – 576 с.

197. Фукуяма Ф. Великий крах. Людська природа і відновлення соціального порядку. Пер. З англ. В. Дмитрука. – Львів: Кальварія, 2005. – 380 с.

198. Фукуяма Ф. Наше постчеловеческое будущее. Последствия биотехнологической революции. – М.: АСТ, ЛЮКС, 2004. – 349 с.

199. Хакен Г. Інформація та самоорганізація. Макроскопічний підхід до складних систем. – М.: КомКнига, 2005. – 245 с.

200. Харкевич А.А. Избранные труды: В 3-х т. – Т.3: Теория информации. Опознание образов. – М.: Наука, 1973. – 524 с.

201. Хорошко В.А., Чекатков А.А. Методы и средства защиты информации – К.: Юниор, 2003. – 504 с.

202. Хартия Глобального информационного общества. Принята 22 июля 2000г., Окинава / Информация. Дипломатия. Психология. – М.: Известия, 2002. – С. 602-610.

203. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособ. – М.: Академия, 2005. – 256 с.

204. Хоффман Л.Дж. Современные методы защиты информации / Пер. с англ. – М.: Советское радио, 1980. – 264 с.

205. Цимбалюк В. Окремі питання щодо визначення категорії „інформаційна безпека” у нормативно-правому аспекті // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Зб. наук. праць. – Київ, 2004. – Вип.8. – С. 30-33.

206. Чернавский Д.С. Синергетика и информация (динамическая теория информации); Послеслов. Г.Г. Малинецкого. – М.: Едиториал УРСС, 2001. – 288 с.

207. Черноруцкий И.Г. Методы оптимизации и принятия решений. – С.Пб.: Изд-во „ЛАНЬ”, 2001. – 384 с.

208. Чубкова О.Ю. Організаційні засади формування інформаційної економіки // Проблеми науки. – 2002. – №4. – С. 7-14.

209. Шеннон К. Роботы по теории информации и кибернетике / Пер. с англ.; Под ред. Р.Д. Добрушина, О.Б. Лупанова. – М.: Изд. ин. лит., 1963. – 830 с.

210. Широчкин В.П. Архитектоника мышления и нейроинтеллект; Под ред Ю.С. Ковтанюка – К.: Изд-во „Юниор”, 2004. – 560 с.

211. Шорошев В.В., Близнюк І.П. Огляд способів вчинення комп’ютерних злочинів // Бизнес и безопасность. – 2004. – №2. – С. 44-50.

212. Шорошев В.В., Близнюк И.Л., Балина С.Н. Классификация угроз для компьютерных данных и систем по рекомендациям Конвенции Совета Европы о киберпреступности // Бизнес и безопасность. – 2005. – №1. – С. 36-39.

213. Эшби У.Р. Введение в кибернетику / Пер. с англ. Д.Г. Ламути; Под ред. В.А. Успенского. – М.: Изд-во „Иностр. лит.”, 1959. – 432 с.

214. Юзвишин И.И. Информациология или закономерности информационных процессов и технологий в микро- и макромирах Вселенной. – 3-е изд., испр. и доп. – М.: Радио и связь, 1996. – 215 с.

215. Яглом А., Яглом Н. Вероятность и информация. – М.: Гостехиздат, 1957. – 160 с.

216. ISO/PAS 22399:2007(E). Societal security – Guideline for incident preparedness and operational continuity management // Firs edition 2007-12-01.

217. ITU-T Recommendation X.200. Reference model of open systems interconnection for CCITT applications. – Geneva, 1991. – 75 с. – Режим доступу: http://www.itu.int/net/home/index.aspx

218. ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. – Geneva, 1991. – 48 с. – Режим доступу: http://www.itu.int/net/home/index.aspx

219. ITU-T Recommendation X.805. Security architecture for system providing end-to-end communications. – Geneva, 1991. – 28 с. – Режим доступу: http://www.itu.int/net/home/index.aspx

220. ITU-T recomendation X.816. Information technology – Open System Interconnection – Security frameworks for Open systems: Security audit and alarms framework.

ЗМІСТ С.

ВСТУП .....
Розділ 1 ОСНОВНІ ПОНЯТТЯ ТА ЗАДАЧІ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ФОРМУВАННЯ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА .....
1.1 Роль та місце інформаційної безпеки в інформаційному суспільстві
1.2 Сутність та зміст понять у сфері інформаційної безпеки .....
1.3 Задачі менеджменту та функції управління інформаційною безпекою .....
Контрольні запитання та завдання .....
Розділ 2 ХАРАКТЕРИСТИКА СУЧАСНОЇ НАЦІОНАЛЬНОЇ ТА МІЖНАРОДНОЇ НОРМАТИВНОЇ БАЗИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ .....
2.1 Етапи розвитку нормативної бази у сфері інформаційної безпеки ...
2.2 Звід та характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки .....
Контрольні запитання та завдання .....
Розділ 3 ОСНОВНІ ЦІЛІ ТА ЗАДАЧІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ .....
3.1 Основні цілі та задачі забезпечення інформаційної безпеки .....
3.2 Джерела загроз та засоби їх впливу на об’єкти інформаційної безпеки .....
3.3 Основні фактори, що впливають на стан інформаційної безпеки .....
3.4 Основні функції системи інформаційної безпеки .....
Контрольні запитання та завдання .....
Розділ 4 СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ...
4.1 Складові інформаційної безпеки підприємства .....
4.2 Джерела загроз інформаційної безпеки підприємства .....
4.3 Методи та засоби захисту конфіденційної інформації на підприємстві .....
Контрольні запитання та завдання .....
Розділ 5 ОСОБЛИВОСТІ ПОБУДОВИ АРХІТЕКТУРИ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ ВІДПОВІДНО ДО ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ .....
5.1 Особливості побудови архітектури телекомунікаційних мереж відповідно до вимог інформаційної безпеки .....
5.2 Механізми забезпечення інформаційної безпеки .....
5.3 Принципи та засади інформаційної безпеки телекомунікаційних мереж загального користування .....
Контрольні запитання та завдання .....
Розділ 6 ЗАБЕЗПЕЧЕННЯ УСТАЛЕНОГО ВІДТВОРЕННЯ СОЦІАЛЬНОГО КАПІТАЛУ .....
6.1 Соціальний капітал, соціологічна та соціальна інформація .....

6.2 Залежність соціального капіталу від циклічності розвитку та зміни технологічних укладів ……
6.3 Загрози соціальному капіталу та соціальній інформації в умовах зміни технологічних укладів
6.4 Менеджмент соціальних технологій з відновлення соціального капіталу ……..
Контрольні запитання та завдання ……
Розділ 7 ЗАХИСТ СОЦІАЛЬНОЇ ІНФОРМАЦІЇ ТА СОЦІАЛЬНО-ПСИХОЛОГІЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ .....
7.1 Феномен та роль соціальної інформації у соціальній та інформаційній безпеці ……
7.2 Причини, за якими необхідно захищати відкриту інформацію …….
7.3 Поняття про систему соціального захисту інформації ……...
7.4 Основи стратегії управління соціальним захистом інформації …….
Контрольні запитання та завдання ……
Розділ 8 ТЕХНОЛОГІЧНЕ УПРАВЛІННЯ МЕХАНІЗМАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ……
8.1 Загальні принципи управління безпекою об’єкта інформаційної діяльності …….
8.2 Система управління інформаційною безпекою ……..
8.3 Функції технологічного управління механізмами безпеки …….
Контрольні запитання та завдання ……
Розділ 9 ПЛАНУВАННЯ ЗАХИСТУ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ……..
9.1 Принципи управління інформаційною безпекою інформаційних систем ……
9.2 Загальні положення з управління інформаційною безпекою ……
9.3 Фізична безпека й безпека навколишнього середовища ……
9.4 Адміністрування комп’ютерних систем і обчислювальних мереж ...
9.5 Управління доступом до систем. Розробляння і супроводження інформаційних систем ……
9.6 Планування безперебійної роботи підприємства та аудит безпеки ...
Контрольні запитання та завдання ……
Розділ 10 МЕТОДИЧНІ ОСНОВИ ОЦІНКИ ЕКОНОМІЧНОЇ ДОЦІЛЬНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ .....
10.1 Методичні основи оцінки економічної доцільності захисту інформації …….....
10.2 Приклад розрахунку оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової автоматичної телефонної станції .....
Контрольні запитання та завдання ……
Розділ 11 РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ .....
11.1 Методи оцінки ризиків інформаційної безпеки .....
11.2 Удосконалення системи інформаційної безпеки телекомунікаційних

мереж за допомогою страхування ризиків ……..
Контрольні запитання та завдання ……
Розділ 12 ОРГАНІЗАЦІЯ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА …….....
12.1 Організація служби інформаційної безпеки підприємства .....
12.2 Менеджмент персоналу у сфері інформаційної безпеки .....
Контрольні запитання та завдання ……
Розділ 13 АУДИТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ .....
13.1 Загальні принципи аудиту інформаційної безпеки …….....
13.2 Цілі та метод проведення зовнішнього аудиту ……
13.3 Оцінка інформаційної безпеки ……..
13.4 Безперервний внутрішній аудит інформаційної безпеки телекомунікаційних мереж ……
13.5 Аудит інформаційної безпеки на відповідність міжнародному стандарту ISO/IEC 27001:2005 ……
Контрольні запитання та завдання …….
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …….
СЛОВНИК ТЕРМІНІВ …….
ДОДАТОК А – Навчальна програма дисципліни „Менеджмент інформаційної безпеки” (для студентів напряму 0925 Інформаційна безпека) …….....
ДОДАТОК Б ТЕСТИ ДЛЯ ПЕРЕВІРКИ ОДЕРЖАНИХ ЗНАНЬ .....
ЛІТЕРАТУРА .....