Якименко І.З.

Конспект лекцій з дисципліни

МЕНЕДЖМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тернопіль - 2019

Тема 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.

1.1. Роль та місце інформаційної безпеки в інформаційному суспільстві

Інформаційна безпека є однією із важливих складових глобальної безпеки, невід'ємною умовою глобалізації та одним із факторів 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 взаємопов'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 головною характеристикою розвитку будь-якої соціально-економічної системи на макро- та мікрорівнях.

Особливості необмеженого і 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 низка 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, поширенні масової інформації, 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:

– 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.

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

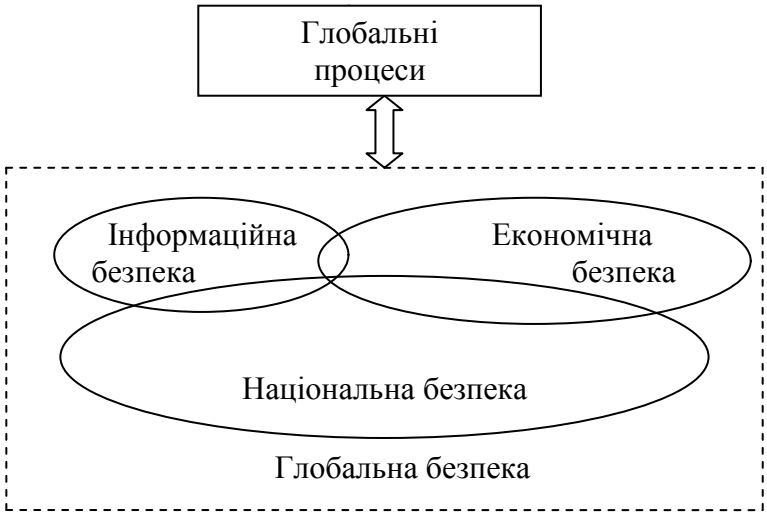


Рисунок 1.1 – Роль та місце інформаційної безпеки у процесі глобалізації

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

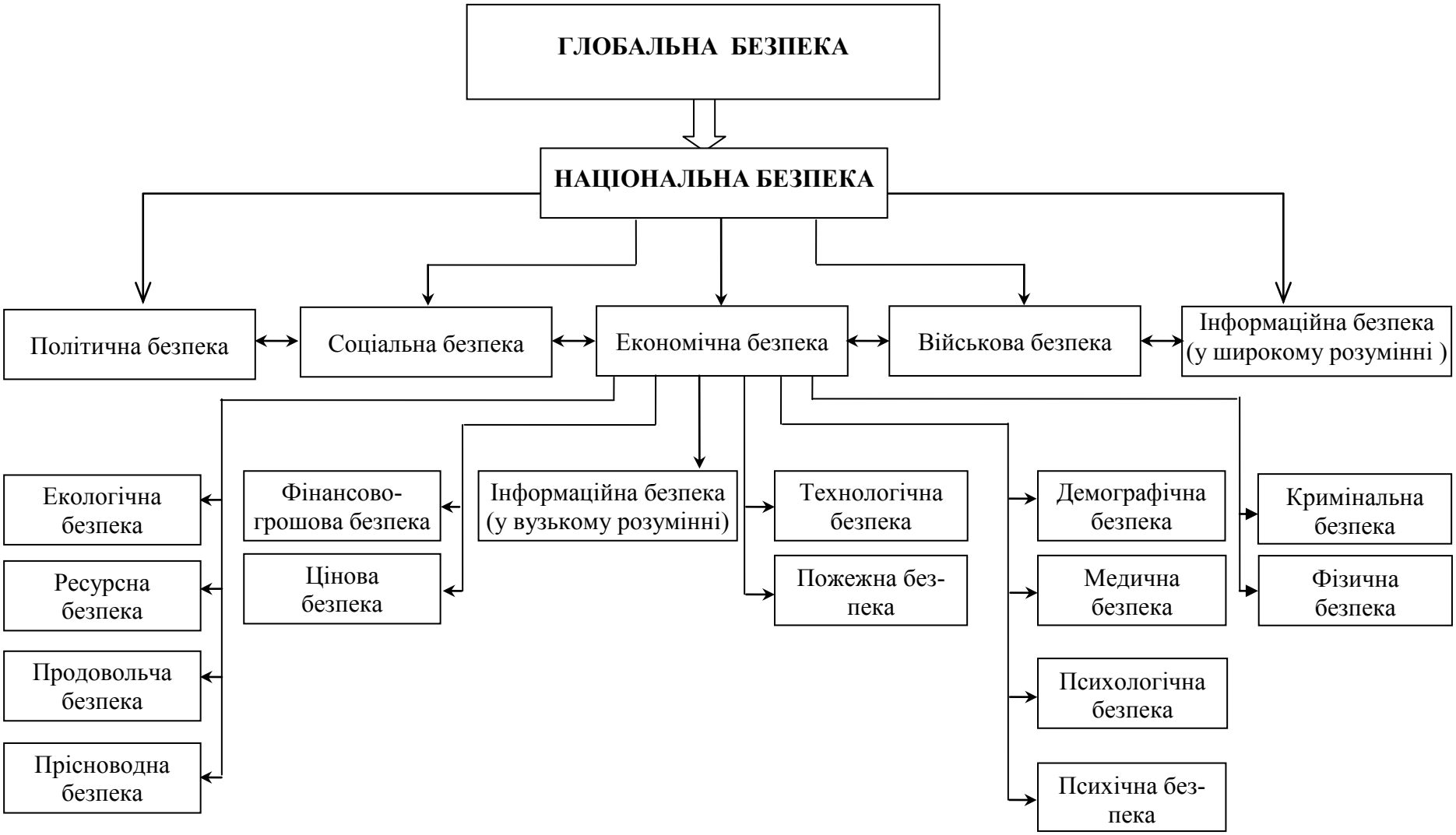


Рисунок 1.2 – Складові глобальної безпеки

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.

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.

В умовах глобалізації посилюється значимість проблем, які пов'язані з інформаційною безпекою, а саме:

– 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, отже, 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], 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”. 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 з 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”.

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.

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.

Автори книги 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 уточнені 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.

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".

На думку Н. Мойсеєва під інформаційною безпекою системи розуміється: „…властивість захищеності її інформаційної сфери (сукупності інформаційних ресурсів й 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".

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”.

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 завдають 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 постає більш широка задача: 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 й 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 підприємства, 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 щодо них необхідно здійснити низку заходів:

– проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і підведені комунікації;

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

Основні поняття та їх зміст наведені у табл. 1.1.

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

№	Визначення	Джерело
1	**2**	**3**
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 ав-	*Закон України „Про захист*

	томатизованій системі (АС) перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі	*інформації в автоматизованих системах*" *від 05.07.94 р. № 81/94-ВР*

Продовження табл. 1.1

1	2	3
4	**Інформація** – відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб	*Закон України „Про 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 працівників 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*

Продовження табл. 1.1

1	2	3
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, проводових, оптичних або інших електромагнітних системах	*Закон України „Про телекомунікації" від 18.11.03 р. № 1280-IV*

Продовження табл. 1.1

1	2	3
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 телекомунікацій	*Закон України, „Про телекомунікації" від 18.11.03 р. № 1280-IV*
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

Задачі менеджменту інформаційної безпеки в галузі зв'язку. 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 удосконалення системи інформаційної безпеки і процесу менеджменту інформаційної безпеки.

Система менеджменту інформаційної безпеки є частиною загальної системи менеджменту організації і призначена для створення, реалізації, експлуатації, моніторингу, аналізу, підтримки й підвищення інформаційної безпеки з урахуванням усіх ризиків організації. Система менеджменту інформаційної безпеки включає:

1. Планування заходів та розробку комплексної системи захисту інформації (КСЗІ) підприємства.

2. Організацію забезпечення інформаційної безпеки підприємства (організація відповідного підрозділу, який забезпечує захист інформації на підприємстві, розробка відповідних задач, політики та стратегії щодо захисту інформації). 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.

3. Мотивацію персоналу, який забезпечує інформаційну безпеку підприємства (впровадження організаційно-психологічних засобів). Співробітники підприємства можуть виступати як об'єктом, так і суб'єктом загроз, спрямованих на порушення економічної стабільності підприємства. Діяльність з управління персоналом є важливою гарантією того, що підприємство буде жити і процвітати. Ефективність системи менеджменту інформаційної безпеки багато у чому залежить від дотримання та виконання

правил політик інформаційної безпеки всіма без винятку співробітниками організації.

4. Контроль діяльності щодо забезпечення інформаційної безпеки підприємства. Проведення діючого контролю і перевірки ефективності планування й реалізації правових форм, методів захисту інформації відповідно до обраної стратегії та концепції безпеки.

Функції управління інформаційною безпекою в галузі зв'язку. 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 усюди 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 й 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. До складу 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 в їхніх частинах мережі;

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

– аналіз даних користувача, які характеризують його характерну поведінку;

– дослідження крадіжки службових послуг за даними його характерної поведінки;

– дослідження внутрішнього трафіка, даних характерної поведінки та інформації контрольного журналу для виявлення злому 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 необхідний для відмови у доступі зловмиснику, ліквідація порушень, зроблених зловмисником, відновлення роботи системи захисту. До цього набору 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 або ізоляції обладнання або даних, виключення прав доступу, а також запитів на відновлення спотворених даних або 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 усіх ключів та сертифікатів замовника послуг, конфігурації мережі, контролю доступу, які підозрюються у непрацездатності внаслідок порушення безпеки;

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

Набір функцій адміністрування безпеки необхідний для планування та адміністрування політики безпеки та безпеки відносно ділової інформації. До цього набору входять функції захисту:

– політики безпеки, який забезпечують доступ до директив компанії для установлення 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 установлюються сценарії послідовного використання функцій безпеки для виявлення, стримування та ліквідації порушень інформаційної безпеки

Тема 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.

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. Інформаційна 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 і 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;

– удосконалення 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;

– застосування 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 складова інформаційно-телекомунікаційних мереж, стала важливою техніко-економічною й політичною проблемою.

Розвиток нормативно-правової бази стосовно інформаційної безпеки інформаційно-телекомунікаційних систем можна поділити на декілька 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 СНД щодо взаємного захисту інформації, яка становить державні таємниці, ці 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 або 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, політики в галузі захисту інформації, служби 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 з цими концепціями 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.

Протягом 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. У цей самий період почала активно діяти низка 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'єкта захисту – захисту 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:

– розв'язання задач щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, розповсюдження якої заборонено відповідно до законодавства;

– посилення відповідальності за порушення установленого порядку доступу до електронних інформаційних ресурсів усіх 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. Державній адміністрації зв'язку 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 у мережі передавання даних (МПД).

Відповідно до пп. 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 подання, 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;

– у 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 з установленими 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 з спробами доступу до інформації, здійснювати періодичний контроль за такими подіями та забезпечувати захист реєстраційної інформації від несанкціонованого модифікування, руйнування або 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 установлення належності інформації, яка передається МПД, певному користувачеві;

– має забезпечуватись можливість установлення факту передавання або одержання оператором або користувачем певної інформації;

– повинне унеможливлюватися несанкціоноване або 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 з захисту інформації, який надається за результатами державної експертизи в сфері технічного захисту інформації.*

Протягом 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.

Наприклад, 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 ІТ-безпеки). Така модель впроваджується міжнародним стандартом ISO/IEC 15408 "Єдині критерії оцінювання безпеки інформаційних технологій" і визначає принципово нову технологію створення систем ІТ-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 урахування 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 факторів;

– 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;

– показників 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 перегляду.

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 оброблення 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 або в інший спосіб.

Інформаційно-телекомунікаційна система – це сукупність інформаційних та телекомунікаційних систем, які у процесі оброблення 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, а також Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

У Документі: „ПРАВИЛА забезпечення захисту інформації *в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах*", *установлюється, що захисту в системі підлягає*:

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 установлена законом, у тому числі конфіденційна інформація про фізичну особу;

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

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

У системі здійснюється обов'язкова реєстрація:

– результатів ідентифікації та автентифікації користувачів;

– результатів виконання користувачем операцій з оброблення інформації;

– спроб несанкціонованих дій з інформацією;

– фактів надання і позбавлення користувачів права доступу до інформації та її оброблення;

– 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 оброблення, контроль за цілісністю засобів захисту в системі здійснюються автоматизованим способом.

Передавання конфіденційної й 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 оброблення інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації. Контролюється також цілісність програмних та технічних засобів захисту

інформації. У разі порушення їх цілісності оброблення 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 українською мовою 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.

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

№ з/п	Дата прийняття і номер	Назва нормативно-правового акту
1	**2**	**3**
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. № 75/98-ВР	**Закон України** „Про Концепцію Національної програми 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.	**Закон України** „Про електронний цифровий підпис"

	№ 852- IV.	
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 удосконалення криптографічного захисту інформації в телекомунікаційних та інформаційних системах

Продовження табл. 2.1

1	2	3
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)	

Продовження табл. 2.1

1	**2**	**3**
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. Ч. 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. Ч. 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 за-	

	гального 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

Продовження табл. 2.1

1	2	3
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.	

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 пакета 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 урегулювання всіх 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.

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

Тема 3 ОСНОВНІ ЦІЛІ ТА ЗАВДАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Основні цілі і завдання 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.

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 зазначених 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 й 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, удосконалення її організації, форм, методів і засобів запобігання, відбивання і нейтралізації загроз інформаційній безпеці та 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 приховують 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 компоненти: конфіденційність (захист конфіденційної інформації від несанкціонованого розкриття або перехоплення), цілісність (забезпечення точності та 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 її інформаційні системи і мережі, що підтримують є дорогими 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 з зростаючою загрозою порушення режиму безпеки, що витікає 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 більш небезпечні і витончені. У той самий 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 й 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 й ефективніше вони будуть для неї згодом.

Аналіз стану справ в області інформаційної безпеки показує, що у деяких розвинених державах склалася й успішно функціонує повністю стабільна інфраструктура системи інформаційної безпеки (СІБ), тобто системи заходів, що забезпечують 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 удосконалювати 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, яка включає державну таємницю й обмежений доступ, комерційну таємницю й обмежений доступ, комерційну таємницю й 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 збирання, оброблення, зберігання і передавання інформації, науково-технічний та обслуговуючий персонал;

– інформаційну інфраструктуру, що включає центри обробки й аналізу інформації, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж, зокрема системи та 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 й 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), право на доступ до якої юридично закріплене за її власником і ним 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) якої неминуче призведе 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, спрямована 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 установлених регламентів збирання, оброблення і передавання 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.

До інформаційних засобів відносяться:

– порушення адресності і своєчасності інформаційного обміну, протизаконне збирання і використання інформації;

– несанкціонований доступ до інформаційних ресурсів;

– маніпулювання інформацією (дезінформація, 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 оброблення 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 оброблення 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.

У 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 й 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 та інших рішень; підрив 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 й 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 й аморальності. Надто суттєвий економічний збиток в різних сферах суспільного

життя і в сфері бізнесу може бути причинною в результаті порушень законодавства в інформаційній сфері і комп'ютерних злочинів.

Загрози інформаційній безпеці можуть завдавати 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.

З метою запобігання, відбивання 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 документах 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 впроваджених програмних або апаратних закладних пристроїв; виключення перехоплення інформації технічними засобами; вживання криптографічних засобів захисту інформації при передавання 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 фактори, які необхідно враховувати при оцінці реального стану інформаційної безпеки і визначенні ключових проблем в цій області. Їх можна поділити на політичні, економічні й організаційно-технічні.

До політичних факторів відносяться:

– зміна геополітичної обстановки внаслідок фундаментальних змін у різних регіонах світу, зведення до мінімуму ймовірності світової ядерної і звичайної воєн;

– інформаційна експансія США та 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 більш тісної співпраці із зарубіжними країнами в процесі проведення реформ на основі максимальної відвертості сторін;

– низька загальна правова й 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, із зарубіжними країнами в розвитку інформаційної інфраструктури України, що розширюється.

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, оброблення і передавання 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, відбивання 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.

Тема 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.

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, суттєво 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 або в пристроях, що пов'язані з подібною апаратурою за допомогою стандартного інтерфейсу.

Рисунок 4.1 – Складові інформаційної безпеки підприємства

Канали витоку інформації у свою чергу підрозділяються на акустичні, віброакустичні, електроакустичні, радіоелектронні, 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.

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 найпростішого оброблення 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 із самих зручних для зловмисника видів знімання інформації.

По-перше, він не вимагає проникнення у зацікавлене приміщення, по-друге, стетоскопи відносно недорогі, легко установлюються 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 стетоскопу 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 у 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 відбуваються в приміщеннях, де установлено 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, в яких передавання 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 будь-яких 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 модулюючі коливання.

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 напрями нормативно-правового забезпечення захисту інформації в Україні наведені на рис. 4.2 та 4.3 відповідно.

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

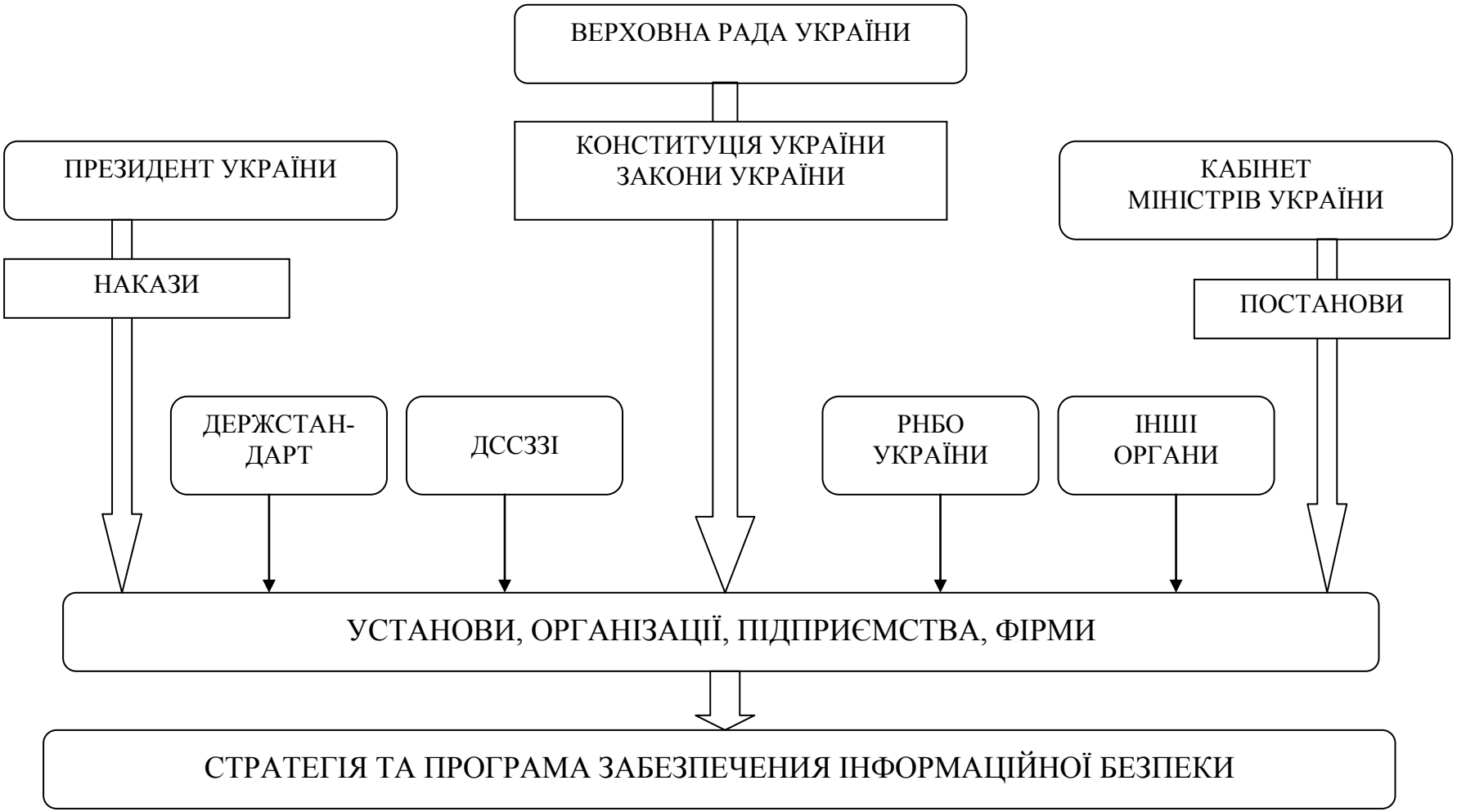


Рисунок 4.2 – Механізм формування вимог до інформаційної безпеки

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

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.

Будемо розрізняти 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 надто загальний характер, а основний зміст статей, присвячених інформаційній безпеці, зводиться до необхідності використовувати виключно сертифіковані засоби, що, взагалі вірно, але далеко не достатньо. Це, безумовно, кроки в правильному напрямі, оскільки робиться спроба охопити всі категорії суб'єктів інформаційних відносин.

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

У 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 (суттєвіша) – домінування апаратно-програмних продуктів зарубіжного виробництва. На законодавчому рівні повинно отримати рішення питання про відношення до таких виробів. Тут необхідно виділити два аспекти: незалежність в області інформаційних технологій та 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. У той самий час, в переважній більшості випадків потенційні загрози інформаційної безпеки носять винятково внутрішній характер. За таких умов 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 й інші розробки американських компаній. Входження України в цю систему та участь українських фахівців у сертифікованих випробуваннях спроможні зняти наявну суперечність між незалежністю в області інформаційних, технологій та 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 розв'язання відповідних задач, повинні бути скоординовані наукові, навчальні 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 у своїй практиці, хоча закон, строго кажучи, цього не вимагає.

Підводячи підсумок, можна накреслити такі наступні основні напрями діяльності в організаційно-правовому аспекті: розробка нових законів з урахуванням інтересів усіх категорій суб'єктів інформаційних відносин; орієнтація на творчі, а не каральні закони; інтеграція – у 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 чиняться керівництвом організації, є політика безпеки та особливості управління персоналом. Належний рівень інформаційної безпеки значною мірою залежить від складу кадрів, їхнього інтелекту та професіоналізму. Питанню 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 та асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації в 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, такі розділи: ввідний, підтверджує заклопотаність вищого керівництва проблемами інформаційної, безпеки; організаційний, такий, що містить опис підрозділів, комісій, груп тощо, що відповідають за роботу в 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, що висвітлює 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, спрямовані на забезпечення безперервної роботи організації; юридичний розділ, що підтверджує 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 займає інформаційною безпекою, не пропонує типових розробок в даній області. Жоден навчальний заклад не готує фахівців з складання політики безпеки. Мало хто з керівників знає, що таке політика безпеки, ще менше число організацій таку політику мають. У той самий час, без подібної основи інші заходи інформаційної безпеки виснуть у повітрі, вони не можуть бути всеосяжними, систематичними й ефективними. Наприклад, заходи захисту від зовнішніх хакерів і від власних скривджених співробітників повинні бути абсолютно різними, тому в першу чергу необхідно визначитися, які загрози здатні нанести найбільшого збитку. Через це зазначимо, що, за статистикою, найбільший збиток відбувається 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, навчальні 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 бажати від керівників наявності політики безпеки (і в перспективі це правильно), але спочатку потрібно пояснити, 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 суттєвого 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 відновлювальних робіт.

Управління персоналом у контексті інформаційної безпеки, як вже говорилося вище, залишається не проробленим та нерозвиненим 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 пояснювати 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. 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 або 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. В 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, суттєво 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 усіх 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 принаймні менші за втрати внаслідок знищення, перекручення, блокування інформації, її несанкціонованого витоку або від порушення установленого 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 інформаційній безпеці, що мають політико-правовий характер і включають:

– внутрішні негативні дії;
– зовнішні негативні дії;
– форсмажорні обставини.

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

Саме тому організаційно-економічний аспект відіграє 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 з сучасним переконанням, у рамках інформаційних систем повинні бути доступні принаймні такі механізми безпеки: ідентифікація і перевірка справжності (автентифікація) користувачів; управління доступом; протоколювання й 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 самий 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 кожному 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 заміж мережного доступу основним є протокол TCP/IP.

Для побудови ешелонованої оборони подібної інформаційної системи необхідні принаймні наступні захисні засоби програмно-технічного рівня: міжмережні екрани (розмежування міжмережного 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 й 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 й апаратно-програмних платформ.

Комерційні структури, на відміну від держструктур, певною мірою більш вільні у своєму виборі захисних засобів. Проте, через цілу низку 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, тому що на захист інформації будь-якого підприємства або 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, оцінки втрат від можливих перешкод та

зловживань, оцінки можливих ризиків та їх страхування та оцінки 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 установленого порядку маршрутизації інформації.

Неможливо створити абсолютно надійну систему безпеки. Здебільшого через те, що постійно розробляються нові види загроз, яким система не спроможна 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 в 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 напряму найбільшої уразливості.

Існує низка 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 уводити особисті емпіричні дані;

– 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, спрямованих 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).

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 розвинені держави світу вже пройшли початковий етап становлення суспільства інформаційної демократії, інші знаходяться на заключній фазі індустріалізму, треті – ще не мають навіть більш-менш розвинен індустріального сектора. Але так чи інакше світ все більше залежить від влади інформації.

Інформація в сучасному світі вже є засобом і метою повноцінної життєдіяльності та набуває чітких рис реальної влади, яка тісно вплетена в усі сфери функціонування суспільства та всі інші види влади. Людство, таким чином, безупинно 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, удосконаленню управління економікою, соціально-економічних відносин, збагаченню духовного життя та подальшої демократизації суспільства. Тому соціальна складова є також невід'ємною для забезпечення інформаційної безпеки.

У 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 розд. 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 групувань, 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 установлення залежності між ними;
– оцінювання активів та установлення 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.

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 усіх 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 удосконаленням загроз такий перелік потрібно періодично переглядати та вносити до нього зміни.

За природою походження джерела їх можна поділити на:

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 поділити на навмисну чи випадкову. *Навмисна* – пов'язана з діями людини, спрямованими на отримання певної вигоди, а *випадкова* пов'язана з помилками людини, її недбалістю, проектно-технологічними недоліками в програмному та апаратн. забезпеченні тощо. Приклади загроз наведені в табл. 4.1.

Таблиця 4.1 – Приклади загроз

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

Загрози можуть бути викликані однією або кількома навмисними, або випадковими подіями. Перелік можливих загроз наведений у табл. 4.2. Наведені в таблиці загрози інформаційним активам є прикладом. Не можливо скласти єдиний вичерпний їх перелік універсальний для всіх підприємств. У кожному випадку для визначення загроз інформаційним активам потрібно застосовувати індивідуальний підхід. **Таблиця 4.2 – Перелік можливих загроз**

№ пп	Загроза	Суб'єктивна		Об'єктивна
		навмисна	випадкова	
1	**2**	**3**	**4**	**5**
1	Землетрус			+
2	Повінь	+	+	+
3	Буревій			+
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 неуповноваженими користувачами	+	+	

Продовження табл. 4.2

1	**2**	**3**	**4**	**5**
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 не уповноваженими користувачами	+		
34	Використання мережних засобів не уповноваженим способом	+		
35	Технічна несправність мережних компонентів		+	
36	Помилка під час пересилання інформації		+	
37	Пошкодження ліній зв’язку	+	+	
38	Перевантаження трафіка	+	+	
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, які 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 поділити на дві групи.

Зовнішні фактори: зміна форми власності, зміна пріоритетів держави щодо промислової політики; зміна оточення (споживачі – постачальники); зниження виробничого і споживчого попиту та 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 були проаналізовані 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 й 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 передаванні каналами зв'язку.

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих систем згідно з вимогами 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 збирання, передавання, оброблення і зберегання.

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

Виявлення має на меті проведення заходів щодо збирання, нагромадження й аналітичного оброблення 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 та 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 уповноважені 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 суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та 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 суттєво ускладнюють несанкціонований, незаконний доступ до засекреченої інформації та 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 вимагаються більш значне завдання: забезпечити безпеку інформації. Це обумовлено низкою обставин, і в першу чергу тим, що все більш широке застосування в накопичуванні й обробленні інформації, що захищається, отримують ЕОМ, в яких може відбуватися не тільки витік інформації, але і її руйнування, перекручування, підроблення, блокування та інші втручання в інформацію й інформаційні системи.

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

– забезпечення своїх прав на володіння, розпорядження і керування інформацією, що захищається;

– запобігання витоку і втрати інформації;

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

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

Завдання 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 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 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 до збереження довірених їм відомостей (інформації).

3. Створення таких адміністративних умов, за яких виключаються 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 отримання). 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 оброблення інформації, що захищається.

4. Облік просторових факторів:

– уведення контрольованих (охоронюваних) зон;

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

5. Облік тимчасових факторів:

– обмеження часу оброблення інформації, що захищається – 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, 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 низку заходів: проаналізувати специфічні особливості розташування будинків, приміщень у будинках, територію навколо них і підведені комунікації; виділити ті приміщення, всередині яких циркулює конфіденційна інформація і врахувати технічні засоби, використані в них.

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

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 показаний наступною по слідовністю дій:

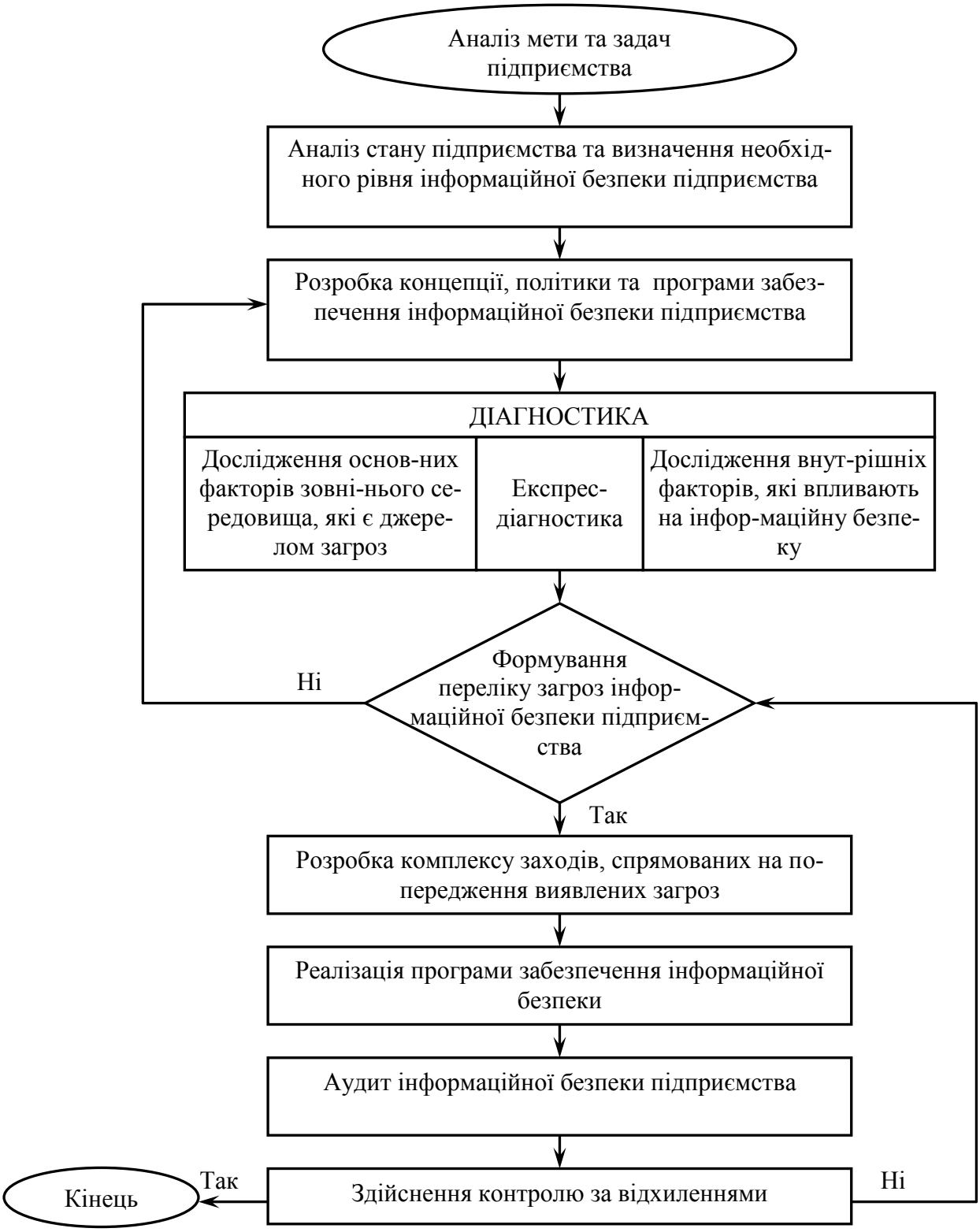


Рисунок 4.4 - Алгоритм створення системи забезпечення інформаційної безпеки підприємства

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 фактори зовнішнього середовища, які є джерелом загроз, та внутрішні фактори, 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.

Тема 5 ТЕХНОЛОГІЧНЕ УПРАВЛІННЯ МЕХАНІЗМАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

5.1. Загальні принципи управління безпекою об'єкта інформаційної діяльності.

5.2. Система управління інформаційною безпекою.

5.3. Функції технологічного управління механізмами безпеки.

5.1. 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 або 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 ета-

пах життєвого циклу ОІД. Технологічне управління інформаційної безпеки є одним із 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, або 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, що стосується безпеки ОІД. Кожна кінцева система може містити необхідну локальну інформацію, щоб давати можливість здійснювати відповідну політику. SMIB є базою розподілу інформації, яка необхідна для здійснення послідовної політики безпеки в кінцевих системах.

SMIB може бути реалізована, наприклад, у вигляді:

– таблиці даних;

– файлу;

– даних або правил, впроваджених у межах програмного забезпечення або апаратних засобів реальних відкритих систем.

Управління безпекою може обмінюватись інформацією стосовно безпеки поміж різними адміністративними системами, для того аби установити 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.

Крім 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 або дистанційно доступних механізмів безпеки, які потребують попереднього узгодження управління;

– звернення 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.

5.2. 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 в 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 перевірку безпеки.

Управління відновлюванням безпеки може включати: технічне обслуговування правил реагування на реальні або підозрювані порушування безпеки; дис-

танційний запис виявлених порушень системи безпеки; взаємодію адміністраторів безпеки.

Адміністратори розподілених відкритих систем мають підтримувати політику 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.

5.3. Функції технологічного управління механізмами безпеки

Управління механізмами безпеки є головною частиною завдань технічної експлуатації механізмів безпеки. Послуги й механізми безпеки можуть бути активізовані управлінням об'єкта через інтерфейс управління та/чи через послугу звернення.

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 або 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 або неявно ключа. *Життєвий цикл* ключа обмежується часом або 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. Наприклад, ключі, призначені для послуг конфіденційності, не можуть використовуватися для послуг цілісності або 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 або 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 або послуг захисту від невизнання участі (у процесі або прийманні повідомлення) з доведенням походження в протоколі управління ключами для передавання відкритих ключів. Ці послуги може бути надано через використання симетричних та/або асиметричних алгоритмів криптографії.

Управління шифруванням включає:

– взаємодію з управлінням ключами;

– установлення параметрів криптографії;

– синхронізацію криптографії.

Застосовування механізму шифрування потребує використання управління ключами й 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 подібне до управління шифруванням.

Управління контролем доступу може включати розподіл атрибутів безпеки, в тому числі паролі, або відновлювання списків контролю доступу, або 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 між відповідними суб’єктами, які здійснюють автентифікування, описової інформації, паролів або

ключів, використовуючи управління ключами. Також може використовуватись протокол між 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 або 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 або під мереж, які мають бути або безпечними, або довірчими, відповідно до притаманних критеріїв.

Управління нотаризацією може включати в себе:

– поширення інформації стосовно нотаріусів;

– використання протоколу між 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 звернення 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.

Тема 6 ПЛАНУВАННЯ ЗАХИСТУ ТА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

6.1. Принципи управління інформаційною безпекою інформаційних систем.

6.2. Загальні положення з управління інформаційною безпекою.

6.3. Фізична безпека й безпека навколишнього середовища.

6.4. Адміністрування комп'ютерних систем і обчислювальних мереж.

6.5. Управління доступом до систем. Розробляння і супроводження інформаційних систем.

6.6. Планування безперебійної роботи підприємства та аудит безпеки.

6.1. Принципи управління інформаційною безпекою інформаційних систем

Управління інформаційною безпекою є важливою функцією технічної експлуатації й 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 за-

хисту – 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 аналіз 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 установлених правил ознайомлення з нею, тобто її захищено від несанкціонованого розкривання або перехоплення.

Інформація та інформаційні ресурси зберігають цілісність у разі дотримування установлених правил її модифікування або вилучення й забезпечує при цьому точності й повноти інформації та комп'ютерних програм.

Інформація й важливі для користувачів послуги зберігають доступність, якщо зберігається можливість ознайомлення або модифікування інформації, або використання послуг відповідно до установлених 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 доробляння 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, які 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 або 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 порушення безпеки, який складається із загроз, яким піддаються інформаційні ресурси, їхніх слабкостей 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 ризику, 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 розроблення 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 забезпечення інформаційної безпеки. Для оцінювання ризиків слід:

– визначати й аналізувати потенційні загрози, яким піддаються комп'ютерні системи та їхні уразливості;

– розглядати збитки, які можуть нанести діяльності підприємства серйозне порушування інформаційної безпеки, з урахуванням можливих наслідків порушення конфіденційності, цілісності й доступності інформації;

– розглядати реальну ймовірність такого порушування захисту від суттєвих загроз за наявності засобів контролю.

Оцінка ризику залежить від таких факторів:

– 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 слабкостей інформаційних ресурсів та рівня їхньої захищеності має ґрунтуватися на цінності й важливості цих ресурсів;

– ознайомлення з системою безпеки всіх керівників та рядових співробітників підприємства;

– вивчення співробітниками політики та стандартів інформаційної безпеки;

– урахування конкретних інформаційних технологій, функцій підприємства та виробничого або обчислювального середовища.

6.2 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 забезпечування 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 забезпечення 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 цих нарадах мають розглядатися такі питання:

– аналізування й затвердження змінень політики інформаційної безпеки й розподіл загальних обов'язків;

– відстежування основних загроз, яким піддаються інформаційні ресурси;

– аналізування і спостерігання за інцидентами в системі безпеки;

– затвердження ініціатив, спрямованих на посилення захисту інформації.

Один із керівників має бути відповідальним за впровадження політики безпеки.

На великому підприємстві потрібне 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 забезпечення захисту, наприклад, за плануванням 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 або 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, який відповідатиме за кожен ресурс або процес забезпечення захисту, а його обов'язки задокументувати.

3. Чітко окреслювати й задокументувати рівні повноважень.

Процедура впровадження нових інформаційних систем має гарантувати, що установлене обладнання 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 установлені системи відповідатимуть вимогам з політики безпеки. Слід перевіряти, особливо в мережному середовищі, що всі пристрої, приєднані до комунікаційних мереж, мають саме той тип, що його було затверджено.

Реальні процедури забезпечування інформаційної безпеки мають бути піддані незалежному аналізу, щоб 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 порушення 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 якому має бути перелічено всі необхідні умови безпеки, щоб 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 кожної 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 установлення обладнання й програмного забезпечення та їхнього супроводження;

– право перевіряти договірні зобов’язання;

– обмеження на копіювання й розкриття інформації;

– заходи щодо забезпечування повернення або 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 обладнання, магнітні носії даних, стрічки й диски, інше технічне обладнання, 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 або спеціального доступу. Категорії таємності й пов'язані з ними захисні засоби для виробничої інформації мають враховувати виробничу необхідність у використанні інформації або обмежуванні доступу до неї, а також збитки для підприємства, спричинені несанкціонованим доступом чи ушкодженням інформації. Розглядають виробничу необхідність забезпечення таких заходів:

– конфіденційності: необхідність обмеження доступу до конфіденційної інформації й засобів, використовуваних для обмеження доступу до інформації;

– цілісності: необхідність здійснення контролю за внесенням змін в інформацію й засоби, використовувані для забезпечування точності й повноти інформації;

– доступності: необхідність забезпечування доступу до інформації й потрібні для цього засоби контролю.

Тут категорія таємності розглядається лише для комерційної інформації. Відповідальність за надання категорії таємності документу, файлу даних або дискеті, а також за періодичну перевірку цієї категорії, покладають на особу, яка 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.

6.3. Фізична безпека й безпека навколишнього середовища

Для запобігання несанкціонованому доступу до інформаційних послуг, ушкодженню й створенню перешкод в їхній роботі утворюють захищені території. Інформаційні системи, які підтримують критично важливі або 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 установлення на підприємстві низки перешкод, розташованих у стратегічно важливих місцях. Вимоги до кожної захисної перешкоди і її 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.

Пропоновані такі рекомендації:

– периметр безпеки має відповідати цінності захищених ресурсів та послуг;

– периметр безпеки має бути чітко окреслений;

– фізичні перешкоди мають за потреби простягатись від стелі до стелі, щоб запобігти несанкціонованому доступу до приміщення;

– не слід без потреби надавати стороннім особам інформацію про те, що відбувається в захищених областях;

– можливе установлення заборони на роботу поодинці без належного контролю. Це необхідно для безпеки праці й для запобігання зловмисним діям;

– комп'ютерне обладнання, яке належить підприємству, розміщують в спеціально призначених для цього місцях, окремо від обладнання, контрольованого сторонніми організаціями;

– у неробочий час захищені області мають бути фізично неприступні – замкнені й періодично перевірятися охороною;

– персоналу, 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 відеоапаратури має бути заборонено, за винятком санкціонованих випадків.

У захищених областях слід установити належний контроль доступу до приміщення, щоб лише персонал, який має відповідні повноваження, мав до них доступ. Пропонується увести 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; крім того, слід рекомендувати їм запитувати перепустку у незнайомих осіб;

– слід негайно вилучати права доступу до захищених областей у співробітників, які 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 обладнання 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 обладнання й носії інформації, на яких зберігаються резервні копії, слід розміщувати на безпечній відстані, щоб уникнути їхнього ушкодження в разі аварії або стихійного лиха на основному робочому місці;

– слід встановлювати сертифіковане сигнальне й захисне обладнання, наприклад, теплові й димові детектори, пожежну сигналізацію, засоби пожежогасіння, а також передбачати пожежну драбину. Сигнальне і захисне обладнання слід регулярно перевіряти відповідно до інструкцій виробників. Співробітники мають бути належним чином підготовлені до використання цього обладнання;

– процедури реагування на надзвичайні ситуації слід повністю задокументувати й регулярно тестувати;

– двері і вікна мають бути замкнені, коли в приміщенні нікого немає. Слід розглядати можливість захисту вікон ззовні.

Ізольовані місця розвантаження й завантаження обладнання та матеріалів. Комп'ютерні зали мають бути захищені від несанкціонованого доступу. Рекомендовано надавати приміщення для розвантаження й завантаження матеріалів та обладнання 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 персоналу, який має відповідні повноваження;

– складське приміщення має бути так сплановано, щоб матеріали можна було розвантажувати без отримання доступу до інших приміщень будівлі;

– зовнішні двері до складського приміщення мають бути замкнені, коли відкриті 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, щоб зменшити ризик несанкціонованого доступу, втрати й ушкодження інформації неробочого часу. Носії інформації, залишені на робочих столах, може бути ушкоджені чи знищені 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 або 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 або інших засобів контролю.

Співробітникам заборонено виносити обладнання, дані та програми за межі підприємства без письмового дозволу керівництва.

Захист обладнання. Обладнання захищають з метою запобігти втратам, ушкодженню й компрометації ресурсів та перебоям в роботі підприємства. Слід також приділити увагу проблемам розміщення обладнання та його утилізації. Обладнання інформаційних систем має бути так розміщено й фізично захищено, щоб зменшити ризик впливу навколишнього середовища й несанкціонованого доступу. Пропоновані такі рекомендації:

– обладнання розміщувати у такий спосіб, щоб за можливістю звести до мінімуму зайвий доступ до робочих приміщень. Робочі станції, які підтримують конфіденційні дані, мають бути розташовані так, щоб вони були завжди на очах;

– доцільно розглянути можливість ізоляції областей, які потребують спеціального захисту, щоб 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.

Обладнання слід захищати від збоїв у системі електроживлення й інших несправностей в електричній мережі. Джерело живлення має відповідати специфікаціям виробника устаткування.

Для обладнання, яке підтримує критично важливі виробничі послуги, рекомендовано установлювати джерело безперебійного живлення. План дій у надзвичайних ситуаціях має включати заходи, яких слід вживати по закінченні терміну придатності джерел безперебійного живлення. Обладнання, 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, які спрямовано до інформаційних систем, мають бути проведено за можливістю під землею або захищено у належний спосіб за допомогою інших засобів;

– слід користуватись екранами або прокладати ці лінії у такий спосіб, аби вони не проходили через загальнодоступні місця.

Для винятково уразливих або критично важливих систем можливе є вживання додаткових заходів, таких як:

– шифрування даних;

– установлення броньованих екранів і використання приміщень, які замикаються;

– використання інших маршрутів або середовищ передавання даних.

Має здійснюватись належне технічне обслуговування обладнання, задля забезпечення його повсякчасної доступності й цілісності. Пропоновані такі рекомендації:

– технічне обслуговування обладнання має здійснюватися через проміжки часу, рекомендовані постачальником, і відповідно до інструкцій;

– ремонт й обслуговування обладнання має виконувати лише експлуатаційний персонал, який має відповідні повноваження;

– слід реєструвати всі несправності й збої.

Використання обладнання інформаційних систем, які підтримують виробничі процеси, за межами підприємства має бути санкціоноване керівництвом; рівень захисту такого обладнання має бути таким самим, як і для обладнання, розташованого на території підприємства. Пропоновані такі рекомендації:

– співробітникам забороняється використовувати персональні комп'ютери для продовження роботи вдома, якщо не установлено процедуру перевіряння на наявність вірусів;

– під час поїздок забороняється залишати обладнання 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, щоб запобігти НСД до інформації, яка в них зберігається;

– слід завжди дотримуватись інструкцій виробника, стосовних захисту обладнання, наприклад, захисту устаткування від впливу потужних електромагнітних полів.

Ризики порушування безпеки, наприклад ушкодження, викрадання, перехоплення, можуть значно варіюватись від місця до місця.

Дані підприємства можуть бути скомпрометовано внаслідок недбалої утилізації обладнання. Перед утилізацією обладнання всі його компоненти, включаючи носії інформації, наприклад, тверді диски, слід перевіряти, щоб 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 або позбутися їх.

6.4. Адміністрування комп'ютерних систем і обчислювальних мереж

Рівень деталізації процедур, необхідних для адміністрування й забезпечування функціонування комп'ютерних систем та обчислювальних мереж, суттєво змінюється залежно від розміру підприємства й типу обладнання, 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 адміністру-

вання й забезпечування функціонування всіх комп'ютерів та мереж. Це має бути підкріплене відповідними робочими інструкціями й процедурами реагування на події. Для зменшення ризику недбалого або несанкціонованого використання систем слід застосовувати принцип розподілу 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 обладнання, 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 звернення за допомогою до експлуатаційного персоналу в разі виникнення проблем, пов'язаних з експлуатацією комп'ютерних систем;

– спеціальні інструкції з оперування вихідними даними, такими, як використання спеціального паперу для друкувальних пристроїв, або адміністрування конфіденційних вихідних даних, включаючи процедури надійного вилучення вихідної інформації від збійних завдань;

– процедури пере запускання й відновлювання працездатності систем, які використовують у разі відмови останніх.

Операційні процедури розглядаються як формальні документи, змінення до яких слід вносити лише після їхнього затвердження керівництвом, наділених відповідними повноваженнями.

Серед завдань адміністрування найбільш складним є мережне адміністрування. Метою мережного адміністрування є забезпечування захисту інформації, яка 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 мають бути за потреби розподілено;

– слід визначати обов'язки та процедури з управління віддаленим обладнанням, у тому числі обладнанням на робочих місцях користувачів;

– для забезпечування конфіденційності та цілісності даних, переданих мережами загального користування, і для захисту приєднаних до них систем потрібний 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 або неточності виробничих даних;

– випадки порушування конфіденційності;

б) крім звичайного плану дій в екстремальних ситуаціях, призначеного для того, щоб 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 або 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 або 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 персоналу, 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.

Розподіл обов'язків або зон відповідальності дозволяє звести ризик недбало-

го або несанкціонованого використання систем до мінімуму і зменшити ймовірність несанкціонованого модифікування або використання даних та послуг. Зокрема рекомендується, щоб виконання наведених нижче функцій не було доручено одним і тим самим співробітникам:

– використання виробничих систем;

– уведення даних;

– забезпечення функціонування комп'ютерів;

– мережне адміністрування;

– системне адміністрування;

– розробляння і супроводження систем;

– управління процесом внесення змінень;

– адміністрування засобів захисту;

– контроль (аудит) засобів захисту.

Розподіл програмних засобів розробляння і робочих програм. Роботи, пов'язані з розробляннням і тестуванням систем, можуть призвести до ненавмисного внесення змін у програми й дані або несанкціонованого доступу до робочого програмного забезпечення й виробничих даних. Доцільно було б здійснювати розподіл програмних засобів розробляння і робочих програм. Пропоновані такі засоби контролю:

– програмні засоби розробляння й робочі програми мають за можливістю запускатись на різних процесорах або 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 зі сторони до адміністрування комп'ютерних мереж може призвести до додаткового ризику порушування режиму безпеки, наприклад, до можливості компрометації, ушкодження або 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 перевірення дотримання стандартів безпеки. Слід розглянути такі питання:

– необхідність ідентифікації особливо уразливих або 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 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. Щоб 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 або 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, задокументовувати і перевіряти вимоги й критерії приймання нових комп'ютерних систем. Пропоновано розглянути таке:

– вимоги щодо продуктивності й навантажувальної здатності комп'ютерів;

– підготовку процедур відновлювання й перезапускання систем після збоїв, а також планів дій в екстремальних ситуаціях;

– підготовку й тестування повсякденних операційних процедур відповідно до заданих стандартів;

– перевірка того, що установлення нової системи не матиме згубних наслідків для функціонуючих систем, особливо в періоди пікового навантаження на процесори, наприклад, наприкінці місяця;

– підготовку персоналу до використовування нових систем.

Для підтвердження цілковитої відповідності всім критеріям приймання систем, слід провести відповідні випробування.

Планування переходу на аварійний режим. Аварійне резервне обладнання надає можливість тимчасового продовження опрацювання даних у разі ушкодження або відмови головного обладнання. 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 обладнання й процедури переходу на аварійний режим слід регулярно тестувати.

Недостатній контроль за процесом внесення змін до робочих інформаційних систем є поширеною причиною їхніх відмов і порушення режиму безпеки. Слід визначати формальні управлінські процедури й обов'язки для забезпечування задовільного контролю за внесенням усіх змінень в обладнання, програми й процедури. Зокрема, слід розглянути такі пункти:

– виявлення й реєстрування суттєвих змін;

– оцінювання можливих наслідків від таких змін;

– процедура затвердження пропонованих змін;

– доведення деталей пропонованих змін до відома всіх причетних осіб;

– процедури й обов'язки з ліквідації невдалих змін та відновлення систем після їхнього внесення.

Для забезпечення цілісності даних та програм важливі 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", мережний „черв'як", „троянський кінь", 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 або виявлення його впровадження. Детально ці питання розглянуто у розд. 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, стосовно проблем з комп'ютерними й комунікаційними системами, слід заносити до журналу реєстрування. Мають існувати чіткі правила опрацювання зареєстрованих збоїв, включаючи такі:

– аналіз журналу реєстрування збоїв для забезпечує їхнього усунення;

– аналіз коригувальних заходів, мета яких полягає в перевіринні того, або не скомпрометовано засоби управління безпекою й або є заходи санкціонованими.

Для визначення умов, які можуть несприятливо позначитися на роботі комп'ютерного обладнання 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 обладнання. Треба контролювати комп'ютерні носії даних і за-

безпечувати їхній фізичний захист, щоб запобігти ушкодженням інформаційних ресурсів та перебоям у роботі підприємства.

Для забезпечення можливості відновлення всіх критично важливих виробничих даних і програм після виходу з ладу комп'ютера або відмовлення 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 забезпечення 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, щоб уникнути наслідків від аварії на головному робочому місці. Слід створити принаймні три покоління резервних копій даних для важливих виробничих застосувань.

2. Резервні копії мають бути у належний спосіб захищені 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, щоб бути впевненим, 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, в якій забороняється використовувати описові позначки, щоб за позначками не можна було визначати, які саме дані зберігаються на запам'ятовувальному пристрої;

– стирання попереднього вмісту повторно використовуваних носіїв інформації, які підлягають вилученню, якщо вони більше не потрібні. Одержання письмової санкції на вилучення носіїв інформації з організації й реєстрування усіх випадків їхнього вилучення в контрольному журналі;

– зберігання всіх носіїв інформації в надійному, захищеному середовищі відповідно до інструкцій виробників.

Усі процедури й рівні повноважень мають бути чітко задокументовані.

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. Пропоновано розглянути такі пункти:

– оперування з носіями вхідної й вихідної інформації та їхнє маркування;

– реєстрування отримувачів даних, які мають відповідні повноваження;

– забезпечення повноти вхідних даних;

– пітвердження отримання переданих даних (за потреби);

– надавання доступу до даних мінімальній кількості осіб;

– чітке маркування всіх копій даних для отримувача, який має відповідні повноваження;

– перевірка списків отримувачів 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 обмежений, 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 вилучення комп'ютерних носіїв даних. Для вилучення більш не потрібних носіїв даних слід використовувати чіткі, надійні і перевірені процедури. Носії даних, які містять конфіденційну інформацію, слід надійно знищувати, наприклад спалюючи їх або подрібнюючи, або очищувати від даних для іншого їх використання всередині підприємства.

Для ідентифікації носіїв даних, які можуть мати потребу надійного вилучання, пропоновано використовувати такий контрольний список: вхідна документація, наприклад, телекси; копіювальний папір; вихідні звіти; одноразові стрічки для принтерів; магнітні стрічки; знімні диски або касети; роздруківки програм; протестовані дані; системна документація.

Кожен випадок вилучення носіїв конфіденційної інформації слід, за можливості, реєструвати в контрольному журналі для майбутніх довідок.

За нагромадження інформації, яка підлягає вилученню, слід враховувати ефект акумуляції. Може статись, що значна кількість нетаємної інформації стає більш конфіденційною, ніж мала кількість таємної інформації.

З метою запобігання втраті, модифікуванню і несанкціонованому використанню даних обмін даними й програмами між організаціями треба контролювати. Такі обміни слід здійснювати на підставі офіційних угод. Мають бути установлені 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.

Між організаціями мають бути укладені офіційні угоди про обмін даними й програмами – електронний або за допомогою кур'єрів, – у тому числі, угоди про зберігання програмного забезпечення. В угодах мають бути задані належні умови безпеки, включаючи таке:

– обов’язки з контролю й повідомлення про передавання й отримання даних;

– процедури повідомлення про передавання й отримання 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;

– забезпечення належного захисту вмісту пакетів від можливого фізичного ушкодження під час транспортування відповідно до інструкцій виробників;

– вживання спеціальних заходів (за потреби) для захисту конфіденційної інформації від несанкціонованого розкриття чи модифікування.

Приклади:

– використовування контейнерів закритого типу;

– доставка за допомогою кур’єрів;

– упаковка, захищене від стороннього втручання, яке дозволяло б виявляти спроби її розкриття;

– 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. Крім того, можливо буде потрібне підтвердження щодо передавання чи отримання 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 мають бути погоджено з партнерами й постачальниками мережних послуг.

Захист електронної пошти. Електронна пошта все частіше використовується для передавання інформації між 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. Пропоновано

розглянути такі пункти:

– уразливість електронних повідомлень стосовно несанкціонованого перехоплення й модифікування;

– уразливість даних, які надсилаються електронною поштою, стосовно помилок, наприклад, хибна адресація або спрямовування повідомлень не за призначенням, а також надійність і доступність сервісу в цілому;

– вплив зміни характеристик комунікаційного середовища на виробничі процеси, наприклад, вплив підвищеної швидкості передавання даних або змінена системи адресації;

– правові положення, такі, як необхідність перевірки джерела повідомлень;

– наслідки для системи безпеки від розкриття вмісту каталогів;

– необхідність уживання захисних заходів для контролю віддаленого доступу користувачів до електронної пошти.

Підприємства мають задавати чіткі правила, стосовно 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, що пов’язані з використанням електронного офісу, потрібні чіткі правила. Пропоновано розглянути такі пункти:

– необхідність вилучення 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 обмеження доступу до персональної інформації стосовно окремих осіб, наприклад персоналу, який працює над конфіденційними проектами;

– придатність системи для підтримки виробничих застосувань;

– категорії персоналу й підрядників або партнерів, яким дозволено використовувати систему й місця, з яких можна отримати доступ до неї;

– необхідність обмеження доступу конкретним категоріям користувачів;

– необхідність зазначення статусу користувачів, наприклад, співробітників підприємства або підрядників, у каталогах до відома інших користувачів;

– правила, стосовно періоду схоронності й резервного копіювання інформації, що зберігається в системі;

– вимоги й процедури переходу до аварійного режиму.

6.5. 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 розмежову-

вання 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 або 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 доступу 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 вилучення облікових записів користувачів, які 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 наведені у розд. 8.

Розробляння і супроводження інформаційних систем. Для забезпечення змонтованості засобів захисту до інформаційних систем, вимоги щодо безпеки систем має бути визначено й погоджено до розроблення 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 задокументовувати їх у рамках загального плану робіт зі створення інформаційної системи.

Аналіз і задавання вимог щодо безпеки слід проводити на стадії аналізу вимог щодо кожного проекту розробки систем. При формулюванні виробничих вимог до нових систем чи модернізації 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 порушення режиму безпеки або відсутності засобів захисту для виробничих процесів. Основою аналізу вимог щодо безпеки становлять:

– розгляд необхідності забезпечення конфіденційності, цілісності й доступності інформаційних ресурсів;

– визначення можливостей використання різних засобів контролю для запобігання й виявлення випадків порушення захисту, а також відновлення працездатності систем після виходу з ладу й інцидентів у системі безпеки.

Зокрема при проведенні такого аналізу 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 або спеціальних розслідувань;

– перевірка і забезпечення цілісності життєво важливих даних на всіх або обраних стадіях їхнього опрацювання;

– захисту конфіденційних даних від несанкціонованого розкриття, у тому числі використання засобів шифрування даних у спеціальних випадках;

– виконання вимог інструкцій та чинного законодавства, а також договірних вимог;

– знімання резервних копій з критично важливих виробничих даних;

– відновлення систем після їхніх відмовлень, 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;

– забезпечення 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 втрати, модифікування і несанкціонованого використання 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 забезпечення надійного захисту, визначеним у практичних правилах та законодавстві.

Системи, які підтримують або впливають на винятково уразливі, дорогі або критично важливі інформаційні ресурси підприємства, можуть потребувати вживання 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.

Для забезпечення правильного уведення даних до прикладних систем, необхідно перевірка вірогідності вхідних даних. Пропоновано такі засоби контролю:

а) перевірка з метою виявлення таких помилок, як:

– величини, що виходять за задані межі;

– помилкові символи в полях даних;

– пропущені або неповні дані;

– перевищені верхні й нижні межі щодо обсягу даних, які вводяться;

– несанкціоновані або суперечливі управляючі дані;

б) періодичне аналізування змісту ключових полів або файлів даних для підтвердження їхньої вірогідності й цілісності;

в) огляд друкованої вхідної документації на предмет внесення несанкціонованих змінень у вхідних даних (слід отримати дозвіл на внесення всіх змін до вхідних документів);

г) процедури реагування на помилки, пов'язані з перевіркою вірогідності вхідних даних;

д) визначення обов'язків усіх співробітників, які беруть участь у процесі уведення даних.

Перевірка вірогідності внутрішнього опрацювання даних. Дані, які було правильно уведено до прикладної системи, може бути ушкоджено внаслідок помилок опрацювання або навмисних дій. Щоб виявити такі випадки ушкодження даних, слід вмонтовувати засоби перевірки до систем. Необхідні для цього засоби контролю визначаються характером застосовування й наслідками від ушкодження даних для підприємства. Прикладами вмонтованих засобів перевірки 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 звірки початкового сальдо з попереднім кінцевим сальдо:

– контроль за виконанням операцій;

– підведення підсумків з відновлення файлів;

– контроль за виконанням програм;

в) перевірка вірогідності даних, генерованих системою;

г) перевірка цілісності даних та програм, які надсилаються між 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 або при зберіганні. У цьому процесі використовуються алгоритм шифрування й інформація про таємні ключі, що 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, які підтримують функцію шифрування.

Автентифікація повідомлень — це метод, який використовується для виявлення несанкціонованих змін, які вносяться до переданих електронних повідомлень, чи їхнього ушкодження. Його можна реалізовувати на апаратному або програмному рівнях за допомогою фізичного пристрою автентифікування повідомлень або програмного алгоритму. Можливість автентифікування повідом-

лень слід розглядати 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.

Автентифікація 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 автентифікації повідомлень, який ґрунтується на методах шифрування з відкритим ключем, який забезпечує автентифікування відправника, а також гарантує цілісність вмісту повідомлення.

Захист файлів прикладних систем. Для забезпечення надійного здійснення проектів розробки інформаційних систем та їхньої експлуатації доступ до системних файлів слід контролювати. Підтримка цілісності прикладних систем має бути обов'язком користувача або групи розробників, яким прикладна система або програмне забезпечення належать.

Треба здійснювати твердий контроль за експлуатацією робочого програмного забезпечення. Для зведення ризику ушкодження робочих систем до мінімуму, слід зреалізувати вже згадувані засоби контролю:

– відновлення робочих бібліотек програм має здійснювати лише призначений бібліотекар після отримання санкції на доступ до застосування від керівника персоналу, який 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 оновлено;

– 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, які 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 забезпечення захисту прикладного програмного забезпечення та даних контролюють безпеку в середовищі розробки та робочому середовищі.

Адміністратори, які відповідають за прикладні системи, мають також відповідати за захист середовища розробляння й робочого середовища. Вони мають аналізувати всі зміни, які пропоновано внести до системи, щоб гарантувати, що вони не порушать безпеку системи або робочого середовища.

Задля зведення ризику ушкодження інформаційних систем до мінімуму, слід здійснювати твердий контроль за внесенням змін до них й розробляти процедури управління процесом внесення змін. 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 змін групою, яка обслуговує інформаційні системи;

– повноваження користувачів на подання запитів на внесення змінень;

– рівні повноважень користувачів на приймання докладних пропозицій;

– повноваження користувачів на приймання внесених змін;

б) приймання змінень, пропонованих лише зареєстрованими користувачами;

в) перевірка засобів управління безпекою та процедур забезпечення цілісності на предмет їхньої компрометації внесеними змінами;

г) виявлення всіх комп'ютерних програм, файлів даних, баз даних та апаратних засобів, які потребують внесення виправлень;

д) затвердження наданих пропозицій до початку роботи;

е) забезпечення приймання пропонованих змін зареєстрованими користувачами до їхнього внесення;

ж) відновлення системної документації після завершення процесу внесення кожної зміни, а також архівація або знищення старої документації;

з) здійснення контролю над версіями всіх оновлених програм;

и) реєстрування всіх запитів на внесення змін у контрольному журналі.

Технічний аналіз змін, внесених до операційної системи. Необхідність у внесенні змін до операційної системи виникає періодично, наприклад, інсталяція нової версії, наданої постачальником. У таких випадках слід здійснювати аналіз прикладних систем на предмет можливого порушення режиму безпеки, що виникає від таких змін. Цей процес має містити в собі таке:

– перевірку процедур контролю застосувань й забезпечення цілісності на предмет компрометації внаслідок внесення змін до операційної системи;

– забезпечення включення до щорічного плану експлуатації перевірки й тестування систем, пов'язані зі зміна, внесеними до операційної системи, а також надавання для цього необхідних фінансових коштів;

– забезпечення 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 зміни 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 розгля-

нути таке:

– ризик компрометації вбудованих засобів контролю та процесів забезпечення цілісності;

– необхідність одержання згоди постачальника;

– можливість одержання необхідних змінень від постачальника в межах стандартного відновлювання програм;

– можливість взяття підприємством відповідальності за подальше супроводження програмного забезпечення внаслідок внесених змін.

Якщо зміна вважаються вкрай необхідна, то слід зберегти вихідне програмне забезпечення, а зміну внести до чітко визначеної копії. Ці змінення слід цілковито задокументувати у такий спосіб, щоб їх можна було вносити до майбутніх оновлених версій програм у разі потреби.

6.6. Планування безперебійної роботи підприємства та аудит безпеки

Для захисту критично важливих виробничих процесів від наслідків великих аварій та катастроф слід мати плани забезпечення безперебійної роботи підприємства. Має існувати процес розроблення 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 обладнання, 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 відновлення основних робіт.

Процес планування безперебійної роботи підприємства. Для розробки й здійснення планів забезпечення безперебійної роботи підприємства слід передбачати ідентифікації й зменшення ризиків навмисних або випадкових загроз, яким піддаються життєво важливі послуги. Слід розробляти плани підтримки неперервності виробничої діяльності після відмовлення або ушкодження життєво важливих послуг або систем. Процес планування безперебійної роботи підприємства має містити в собі таке:

– ідентифікацію критично важливих виробничих процесів та 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;

– перегляд й відновлення 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 опра-

цюванням інформації, а не лише на процедурах переходу на аварійний режим для комп'ютерних систем.

Для забезпечення погодженості всіх рівнів планування й визначання пріоритетів для тестування та здійснення, слід мати єдину систему планування безперебійної роботи підприємства. У кожнім плані забезпечення 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 установленим процедурам реагування на надзвичайні ситуації, наприклад, планам евакуації, й ухваленим процедурам переходу до аварійного режиму для комп'ютерних та комунікаційних систем.

Взагалі, можуть знадобитися різні рівні планування, оскільки кожен рівень зосереджено на власному завданні, а в його здійсненні можуть брати участь різні групи з відновлення 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, який загрожуватиме небезпекою роботі підприємства та/або 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 відновлення 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 по 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 забезпечення безперебійної роботи підприємства. Багато планів забезпечення безперебійної роботи організації зазнають невдачі при їхньому тестуванні внаслідок неправильних вихідних припущень, прорахунків або змін, внесених в обладнання. Тому ці плани слід регулярно тестувати, аби убезпечити їхню ефективність. Такі тести мають гарантувати, що всі члени групи з відновлення систем після аварій, постійно пам'ятатимуть про план. Слід скласти графік проведення випробувань плану забезпечення безперебійної роботи організації. Такий графік має зазначати, 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 та ефективність плану впродовж року. Крім того, такий підхід дозволяє уникнути частого проведення вичерпних випробувань повного плану.

Плани забезпечування безперебійної роботи підприємств швидко застарівають унаслідок змін у виробничих процесах й організації, тому їх слід регуля-

рно оновлювати. Прикладами змінень, коли необхідні оновлення планів, є:

– придбавання нового обладнання або модернізація функціонуючих систем;

– нова технологія виявляння проблем, наприклад, виявлення пожеж;

– нова технологія контролю за навколишнім середовищем;

– кадрові або організаційні зміни;

– змінени підрядників або постачальників;

– змінени адрес або телефонних номерів;

– змінени, що вносяться у виробничі процеси;

– змінени, що вносяться до пакетів прикладних програм;

– змінени в робочих процедурах;

– змінени в законодавстві.

Слід призначити відповідальних осіб для ідентифікація та внесення змін до планів. Необхідність в окремих змінах слід переглядати принаймні щомісяця. Цей процес має бути підкріплено коротким щорічним аналізом повного плану. Щоб гарантувати, що наслідки від внесених змінень визначено й доведено до відома співробітників, потрібний 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 наявному 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, або 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 або програм підприємства для використання на комп'ютерах, які не належать підприємству, для цілей, не пов'язаних з основною виробничою діяльністю, може також призвести до порушення закону про авторське право й політики організації;

– в разі потреби інсталювати програмний продукт на додаткових машинах, слід внести пункт щодо цього до ліцензійної угоди або придбати додаткові копії;

– слід регулярно перевіряти використання програмного забезпечення й вести належний облік.

Порушення закону про авторське право може призвести до судових розглядів і навіть до порушення кримінальної справи.

Важливу для підприємства документацію слід захищати від втрати, знищення й підробки. Певні документи мають зберігатись в захищеному місці для задоволення правових вимог, а також для підтримки основної виробничої діяльності. Прикладом 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 або карних позовів, або для підтвердження 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, в якому має бути визначено основні типи документів та терміни їхнього зберігання;

– проводити інвентаризацію всіх джерел основної інформації;

– реалізовувати належні заходи для захисту основної документації від втрати, знищення і підробки.

Згідно з чинним законодавством України, персональні дані про осіб, за якими їх можна ідентифікувати, і які зберігаються або опрацьовується на комп'ютерах, підлягають захисту. 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 забезпечення знання й розуміння принципів захисту інформації, визначених чинним законодавством.

Відомо вісім принципів, застосовних до всіх систем, які 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 або 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 отримувати інформацію від користувача даних про те, чи зберігає він персональні дані, суб'єктом яких є даний співробітник, а також доступ до таких даних;

– за потреби виправляти або стирати вищезазначені дані;

8. Слід вживати належних заходів щодо захисту персональних даних від несанкціонованого доступу, їхні зміни, розкриття й знищення, а також від їхньої випадкової втрати або 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, або 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, щоб усі користувачі отримували письмову санкцію на дозвіл доступу. Користувачів слід попереджати, що вони не мають права доступу, крім випадків, які формально санкціоновано і задокументовано.

Для забезпечення відповідності систем політиці та стандартам безпеки інформаційних систем підприємства потрібна регулярна перевірка безпеки інформаційних систем. Таку перевірку слід провадити виходячи з відповідної політики безпеки, а технічні платформи й інформаційні системи слід перевіряти на відповідність чинним стандартам забезпечення безпеки.

Усі підрозділи підприємства мають регулярно перевірюватись, щоб забезпечувати відповідність чинній політиці та стандартам безпеки. Перевірці підлягають: інформаційні системи та їхні постачальники; інформація та власники даних; користувачі; керівництво. Власники інформаційних систем мають організовувати регулярні перевірку власних систем на відповідність чинній політиці безпеки, стандартам та іншим вимогам щодо їхнього захисту.

Аудит безпеки. *Інформаційні ресурси слід регулярно перевіряти на відповідність стандартам забезпечення безпеки.* Технічна перевірка на таку відповідність містить у собі оглядання робочих систем, щоб гарантувати правильне функціонування засобів управління безпекою програмного й апаратного забезпечення. Така перевірка має проводитися досвідченим системним інженером, який створює технічний звіт для наступного опрацювання фахівцем, вручну або автоматично за допомогою пакета програм. Такі перевірки мають проводитися лише компетентними особами або під їхнім наглядом.

Треба мати засоби контролю для захисту робочих систем і засоби аудиту під час їхньої перевірки. Захист також потрібен для забезпечення 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 перевіркою робочих систем. Пропоновано розглядати таке:

– вимоги щодо аудиту систем мають бути погоджені з керівництвом;

– масштаб перевірок слід погоджувати й контролювати;

– перевірка має бути обмеженою 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 перевірок і зробити їх доступними;

– слід визначати вимоги щодо спеціального або 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, щоб запобігати їхньому можливому несанкціонованому використанню щоб 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.

У штатному розписі підприємства має бути передбачено посаду відповідального, і її має посідати досвідчений фахівець з безпеки. Для невеликих підприємств рекомендовано створювати єдину службу експлуатації, щоб забезпечувати погодженість при ухвалюванні рішень з питань безпеки та сприяти максимальному використанню знань і досвіду співробітників.

Тема 7 МЕТОДИЧНІ ОСНОВИ ОЦІНКИ ЕКОНОМІЧНОЇ ДОЦІЛЬНОСТІ ЗАХИСТУ ІНФОРМАЦІЇ

7.1. Методика оцінки економічної доцільності захисту інформації

7.2. Приклад розрахунку оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки

7.1. Методика 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 за 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 перевірок 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. 7.1).

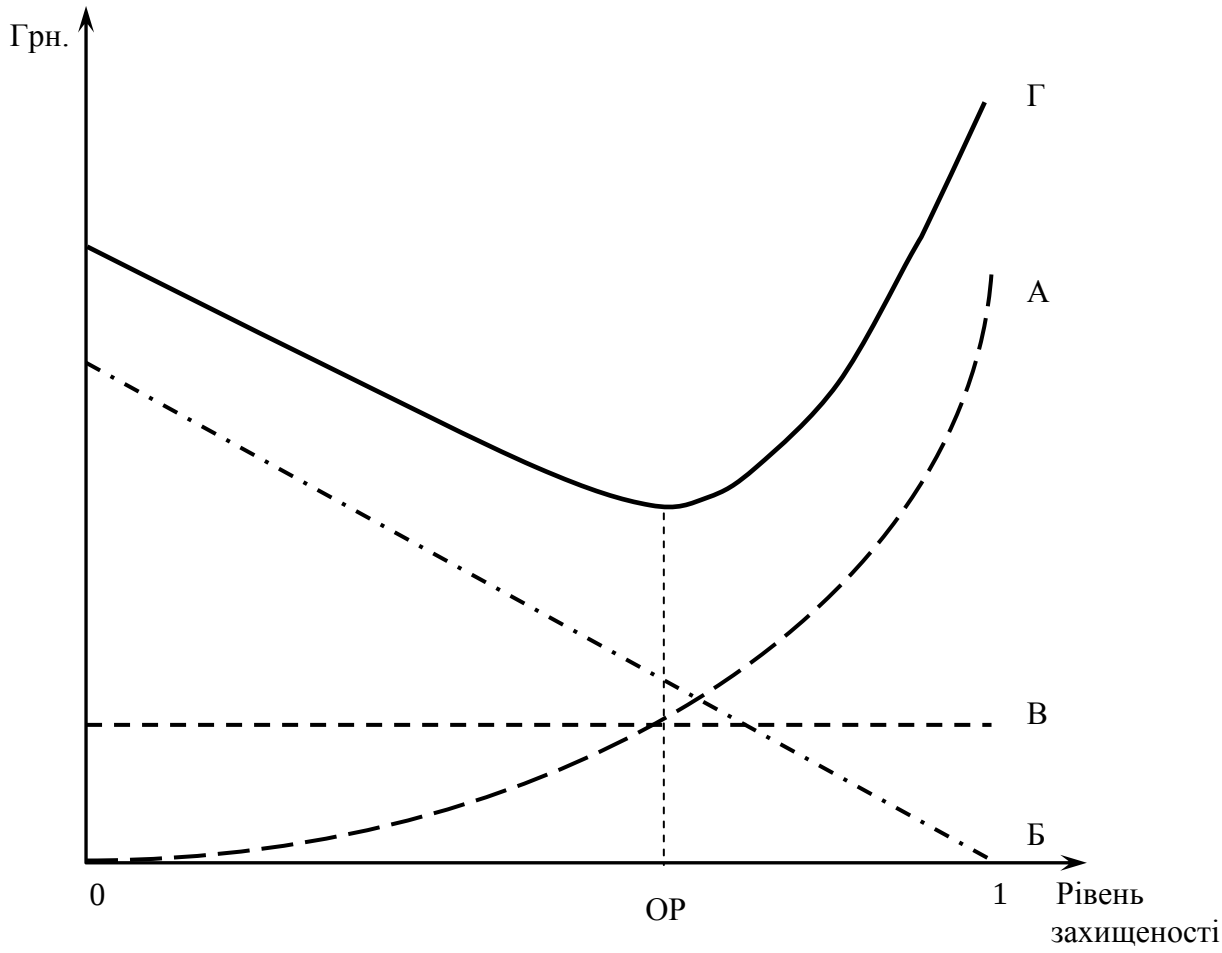
Зі зміною рівня захищеності інформаційного середовища змінюються розміри складових загальних витрат та, відповідно, їхня сума – загальні витрати на безпеку.

На рис. 7.1 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. 7.1 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 обсягу витрат на експлуатацію незначна.

Якщо рухатись за графіком вправо за точку економічної рівноваги (тобто, коли рівень захищеності зростає), 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 7.1 – Взаємозв'язок між витратами на інформаційну безпеку та досягнутим рівнем захищеності

Рис. 7.1 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 впровадження системи інформаційної безпеки, є:

– чистий дисконтований дохід, 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

$$A_{\text{щек}} = A_{\text{втр}}\, E - A_{\text{вит}}\,, \quad (7.1)$$

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, пов’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. 7.1.

Таблиця 7.1 – **Розрахунок показника очікуваних втрат**

	Потенційні загр	Частота вин нення, *f*	Втрат грн.	Втрат %	$A_{втр,}$ г
	2	3	4	5	6

6. Показник $A_{втр}$ обчислюється за формулою:

$$A_{втр} = f*L, \qquad (7.2)$$

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 7.2 - Приклад перетворювання ймовірності загроз до річної частоти

Рівень імовірнос	Опис	Частот
1	2	3
Незначний	Навряд відбудеться	0,05
Дуже низький	Подія відбувається два-три рази на 5 ро	0,6
Низький	Подія відбувається менше одного разу рік або раз на рік	1,0

Середній	Подія відбувається менше одного разу півріччя або раз на півріччя	2,0
Високий	Подія відбувається менше одного разу місяць або раз на місяць	12,0
Дуже високий	Подія відбувається декілька разів на мі	36,0
Екстремальний	Подія відбувається декілька разів на де	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:

$$C_{\text{впр}}=C_{\text{л}}+C_{\text{пр}}+\sum_{s} C_i, \qquad (7.3)$$

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 розд. 10.2., табл. 10.3.

3. Розраховуються на кожен рік накопичені витрати проекту впровадження за формулою:

$$C_{\text{нак }1} = C_{\text{нак поч}} + C_{\text{впр1}},$$
$$C_{\text{нак }2} = C_{\text{нак }1} + C_{\text{впр2}}, \quad (7.4)$$
$$C_{\text{нак }3} = C_{\text{нак }2} + C_{\text{впр3}},$$

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:

$$NPV_{\text{в}} = \sum_{i=0}^{2} \frac{CF}{(1+r)^i} \quad (7.5)$$

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*;
$TCO_{\text{ц}}$ – цільовий показник *TCO*;
$TCO_{\text{ф}}$ – фактичний показник *TCO*.

6. Розраховуються вигоди при оптимізації показника загальної вартості володіння за формулою:

$$\text{В} = TCO_n - TCO_{\text{ф}}, \quad (7.6)$$

де В – накопичений показник вигод при оптимізації показника *TCO*;
$TCO_{\text{п}}$ – поточний показник *TCO*;
$TCO_{\text{ф}}$ – фактичний показник *TCO*.

7. Розраховуються величини щорічної економії за формулою:

$$A_{\text{щек}} = A_{\text{втр}} * E - A_{\text{вит}}, \quad (7.7)$$

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);
$A_{\text{вит}}$ – щорічні витрати на інформаційну безпеку, $A_{\text{вит}} = TCO_{\text{ф}}$

8. Розраховується показник вигод при оптимізації показника *TCO* та щорічної економії за формулою:

$$\text{В}_{tco} = \text{В} + A_{щек}, \quad (7.8)$$

де $В_{тсо}$ – показник вигод при оптимізації показника *ТСО* та щорічних збережень;

В – вигоди при оптимізації показника ТСО;

$А_{щек}$ – величина щорічної економії.

9. Розраховується накопичений показник вигод при оптимізації показника *ТСО* та щорічної економії за формулою:

$$\begin{aligned} В_{нак\ 1} &= В_{тсо1,} \\ В_{нак\ 2} &= В_{нак\ 1} + В_{тсо2,} \\ В_{нак\ 3} &= В_{нак\ 2} + В_{тсо3} \end{aligned} \qquad (7.9)$$

де $В_{нак}$ – накопичений показник вигод при оптимізації показника *ТСО* та щорічної економії;

$В_{тсо}$ – показник вигод при оптимізації показника *ТСО* та щорічних збережень.

10. Розраховується грошовий потік за формулою:

$$CF = В_{тсо} - С_{впр}, \qquad (7.10)$$

де *CF* – грошовий потік;

$В_{тсо}$ – показник вигод при оптимізації показника *ТСО* та щорічних збережень;

$С_{впр}$ – витрати на впровадження.

11. Розраховується накопичений грошовий потік за формулою:

$$CF_{нак} = В_{нак} - С_{нак},, \qquad (7.11)$$

де $CF_{нак}$ – накопичений грошовий потік;

$В_{нак}$ – накопичений показник вигод при оптимізації показника *ТСО* та щорічної економії;

$С_{нак}$ – накопичені витрати проекту впровадження.

12. Розраховується накопичений чистий грошовий потік доходів (відвернутих витрат) від проекту впровадження за наступною формулою:

$$NPV_{д} = \sum_{i=0}^{2} \frac{CF}{(1+r)^{i}}, \qquad (7.12)$$

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.

7.2. Приклад розрахунку оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки

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). У наведеному прикладі враховується 11 потенційних загроз інформаційній безпеці відповідно з [79].

Заповняємо табл. 7.3 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 7.3 – **Розрахунок показника очікуваних втрат**

	Потенціальні загрози	Частота вин нення, f	Вт ти гр	В т	$A_{втр,}$ г
	2	3			6
	Саботаж	0,6	34		209,
	Проникнення у систему	1,0	4		40
	Атаки на ПЕОМ управлін	36	49	1	17 84
	Помилки в роботі з ба даних	36	79	2	28 46
	Телефонне шахрайство	12,0	14 6	5	17 10
	Неавторизований доступ	12,0	95	3	11 41
	Крадіжка обладнання і грам	0,6	1	5	844
	Фінансове шахрайство	1,0	19 6	7	1 988
	Помилки в роботі мереж гналізації, синхронізації та рування	1,0	25		2 54
	Крадіжка приватної ін мації	1,0	60	2	6 00
	Віруси	36,0	10 2	3	375 88
	Всього		26	10	462 7

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. 7.4.

Таблиця 7.4 – Вихідні дані

	Статті витрат	Вартість, грн
	2	3
	Витрати на купівлю ліцензії	150 000
	Витрати на проектні роботи	3 500
	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. 7.5.

Таблиця 7.5 - Розрахунок оцінки витрат на створення і впровадження системи забезпечення інформаційної безпеки на прикладі цифрової АТС

	Показники	По ков тр г	Роки			
						Вс гр
	Витрати на впровадже $C_{впр}$	0	3 5	45	45	243
	Накопичені витрати п кту впровадження, $C_{нак}$	0	153	198	243	-
	Накопичений чи грошовий потік *(NPV)* трат на проект впр дження, $NPV_в$	22				-
	Поточний показник $TCO_п$		8 79	794	794	2 383,
	Цільовий показник $TCO_ц$		6 62	621	621	1 864,
	Фактичний показник $TCO_ф$		8 35	273	621	2225
	Вигоди при оптимі показника *TCO,* В		434	152	217	412
	Показник очікув втрат $A_{втр}$		462	462	462	1 388
	Ефективність системи рпоративного захисту,		85	85	85	-
	Величина щорічної ек номії, $A_{щек}$		384 76	386 3	386 1	1 157 1

	Показник вигод при оп тимізації показника *TC* щорічної економії, B_{mco}		385 35	3 555	388 5	1 161 69
	Накопичений показни вигод при оптимізації п зника *TCO* та щорічної економії, $B_{нак}$		385 35	772 4	1161 9	-
	Грошовий потік, *CF*	- 0	381 35	342 9	343 5	918 2
	Накопичений грошови потік, $CF_{нак}$	- 0	231 35	574 3	918 9	-
	Накопичений чистий грошовий потік *(NPV)* д ходів впровадження *NP*	- 3				-
	Внутрішня норма при ковості, *IRR*	18				-

Записуємо у табл. 7.5 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. 7.5.

Розраховуємо на кожен рік та в цілому показник вигод при оптимізації показника *TCO* та щорічних збережень B_{mco} за формулою (10.8). Маємо послідовно:

$B_{mco1} = B_1 + A_{щек1}$ = 434,59 + 384 947,76= 385 382,35 грн.;

$B_{mco2} = B_2 + A_{щек2}$ = 1521,06 + 386034,23 = 387 555,29 грн.;

$B_{mco3} = B_3 + A_{щек3}$ = 2172,94 + 386 686,11 = 388 859,05 грн.;

$B_{mcoΣ} = B_{mco1} + B_{mco2} + B_{mco3}$ = 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 *TCO* та щорічні збереження за формулами (10.9). Маємо послідовно:

$B_{нак\ 1}$= 385 382,35 грн.;

$B_{нак\ 2}$ = 385 382,35 + 387 555,29 = 772937,64 грн.;

$B_{нак\ 3}$ = 772937,64 + 388 859,05 = 1 161 796,69 грн.

Результати обчислень заносимо в табл. 10.5.

Розраховуємо на кожен рік та в цілому грошовий потік *CF* за формулою (10.10). Маємо послідовно:

$CF_1 = B_{mco1} - C_{впр1}$ = 385 382,35 – 3500 = 381 882,35 грн.,

$CF_2 = B_{mco2} - C_{впр2}$ = 387 555,29 – 45 000 = 342 555,29 грн.,

$CF_3 = B_{mco3} - C_{впр3}$ = 388 859,05 – 45 000 = 343 859,05 грн.,

$CF_{\Sigma} = CF_1 + CF_2 + CF_3 = 385\,382{,}35 + 342\,555{,}29 + 343\,859{,}05 = 918\,296{,}69$ грн. Результати обчислень заносимо в табл. 10.5.

Розраховуємо на кожен рік накопичений грошовий потік $CF_{нак}$ за формулою (10.11). Маємо послідовно:

$CF_{нак1} = В_{нак1} - С_{нак1} = 385\,382{,}35 - 153\,500 = 231\,882{,}35$ 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.

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 *IRR* = 18,5%. При ставці дисконтування 18,5% поточна вартість очікуваних відвернутих збитків буде дорівнюватися поточній вартості необхідних грошових вкладень.

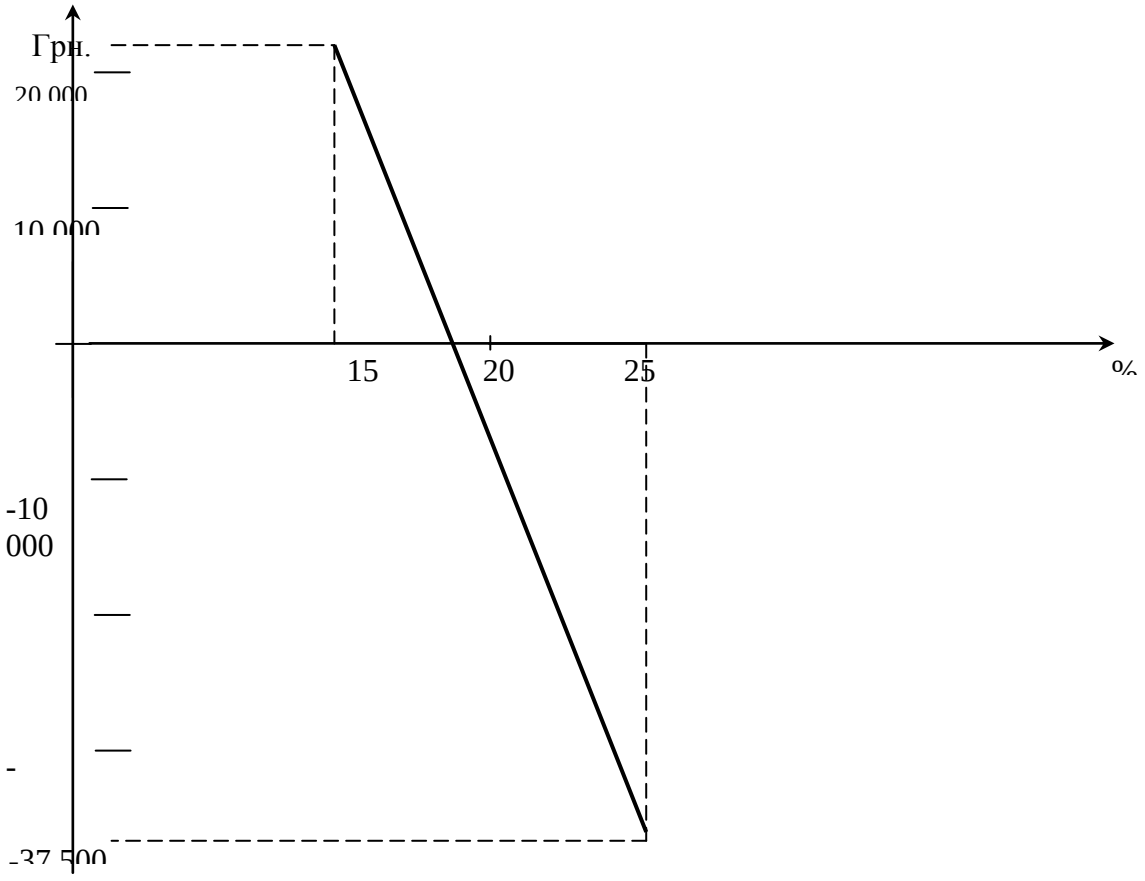


Рисунок 7.2 – Внутрішня норма прибутковості

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. У 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 дохід 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 дохідності від цього вкладення.

Чистий дисконтований дохід 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 його розрахунках випробовується кілька норм дисконту до тих пір, поки не буде знайдено той його рівень, за яким чистий дисконтований дохід дорівнюватиме нулю. Пошук 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 або 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, пов'язаних з інноваційним проектом, є потоком грошових коштів (flow stream).

Для виявлення вихідних даних, особливо потенційної 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.

Тема 8 РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

8.1 Методи оцінки ризиків інформаційної безпеки.

8.2. Удосконалення системи інформаційної безпеки телекомунікаційних мереж за допомогою страхування ризиків.

8.1. Методи 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 двигун. У той самий 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, пов’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, пов’язані з несанкціонованим вторгненням в 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 самий час, заходи протидії не встигають за зростанням числа інцидентів. Як видно з рис. 11.1, б, кількість виявлених уразливостей в системах захисту вже не зростає, стабілізувавшись на рівні 40000 за рік. Поки що у класичному протистоянні злочинності і суспільства в галузі ІКТ виграють злочинці.

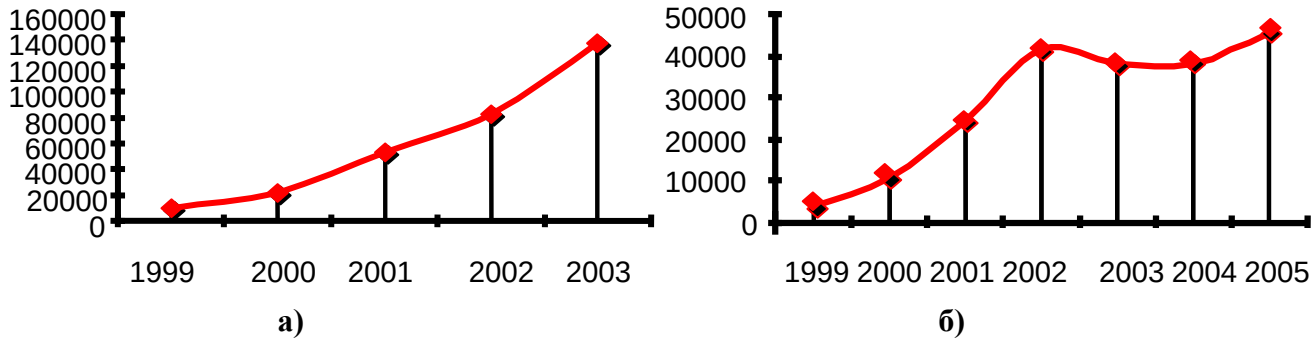


Рисунок 8.1 – Кількість зареєстрованих інцидентів пов'язаних з несанкціонованим вторгненням в інформаційні ресурси США

Україну цей процес теж буде торкатись в міру виконання програми інформатизації та 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 удосконалення існуючої системи інформаційної безпеки. Одним з дієвих способів удосконалення систем інформаційної безпеки є страхування ризиків. Застосування його в галузі безпеки інфотелекомунікацій має свої особливості. вирішенню цієї проблеми і присвячено даний розділ навчального посібника.

Процес створення інформаційної безпеки починається з обстеження об'єкта ІКТ, де, як правило, вже склалась певна система оброблення інформації, баз даних, аналізу знань, прийняття рішень. Метою етапу обстеження є отримання структури інформаційних ресурсів, класифікація, категорію вання 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 уразливості 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 захищуваної 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 за двома факторами, 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, уразливостям і вартості втрат.

Загрозою називають сукупність умов та факторів, які можуть стати причиною порушення цілісності, доступності, конфіденційності інформації.

Уразливість – 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 уразливості від даної загрози.

Цей вираз можна розглядати як математичну формулу, якщо використовуються кількісні шкали, або як формулювання загального принципу, якщо хоча б одна зі шкал є якісною.

Інформаційно-комунікаційним технологіям притаманні різні уразливості, слабкі місця. Зловмисники, кінець кінцем, ці уразливості виявляють і негайно використовують для проникнення. Можна виділити такі види уразливостей 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);

– навмисно закладені;

– випадкові.

Привнесені, випадкові і навмисне закладені уразливості 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 уразливості продовжують виявлятись під час експлуатації систем.

Що стосується природжених уразливостей, 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 й 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 оброблення 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.

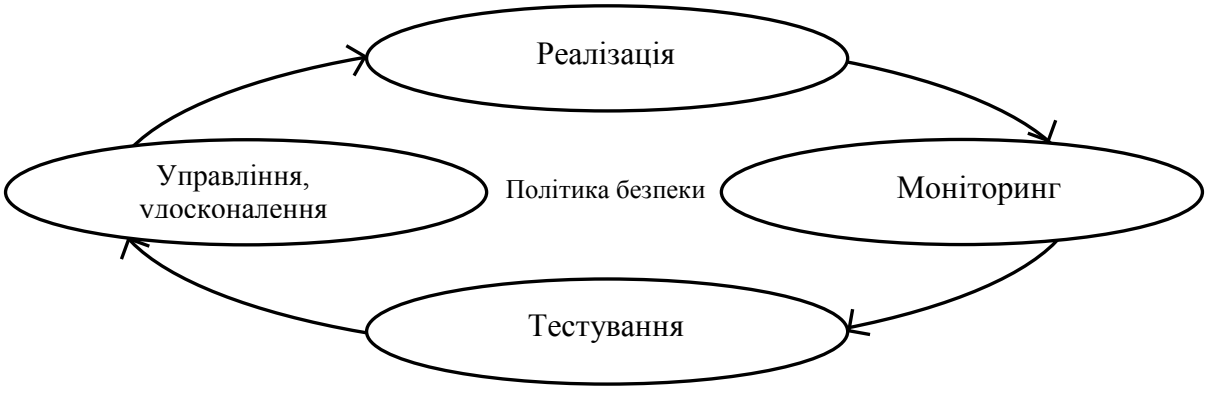


Рисунок 11.2 – Алгоритм використання системи інформаційної безпеки

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 удосконаленні самої ІКТ має бути прийняте рішення на доробку або удосконалення 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 уразливостей 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 й обробляє певний обсяг інформації, частина якої стає спільною, і використовує певні інформаційні ресурси. Кожен з партнерів повинен забезпечити необхідний (або базовий, за домовленістю) 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.

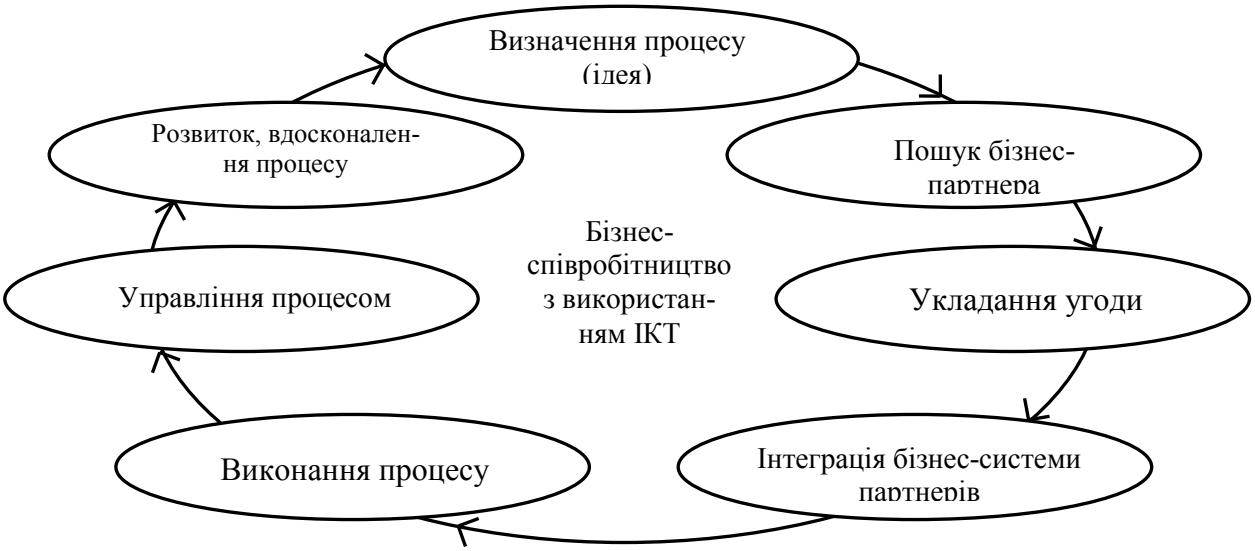


Рисунок 11.3 – Електронна бізнес-співпраця

Щоб стабілізувати рівень злочинності в ІКТ, доцільно забезпечити всіма суб'єктами взаємовідносин однаковий рівень інформаційної безпеки, не нижчий деякого базового. Установлювати 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 у державі повинні нести певні витрати на забезпечення інформаційної безпеки.

Вибір допустимого рівня залишкового ризику пов'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 за яких обставин. Але є і 10% людей які будуть намагатись скоїти злочин, навіть усвідомлюючи невідворотність покарання. Ці люди будуть наполегливо шукати і будуть штучно створювати уразливості ІКТ, щоб їх використати в своїх злочинних цілях. СІБ, як і правоохоронні органи, повинні планомірно і надійно залатати всі „дірки", уразливості і слабкі місця в інформаційній безпеці ІКТ.

Ефективність створеної СІБ залежить, значною мірою, від якості проведення обстеження об'єкта 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 пов'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, Шеннона, Харкевича, Колмогорова тощо відносяться до випадків статистичної цінності інформації і в практиці оброблення 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 оброблення інформації є інша інформація (програми) і підходи до оцінки різних видів інформації можуть бути різними;

– одні види інформації можна оцінити кількісно, інші лише якісно, застосовуючи якісні шкали та експертні методи оцінки.

– кожен вид інформації може оцінюватись багатобічно. За одними критеріями цінність інформації може бути більшою, а за іншими – меншою.

Для усунення зазначених недоліків пропонується новий підхід до інформаційної безпеки. Суть підходу полягає в тому, що для складних систем, значною кількістю потоків інформації різних категорій, спочатку визначається частка витрат на інформаційну безпеку. Величина цієї частки 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 або обороту, тим більша доля витрат на інформаційну безпеку. Відомо, що конфіденційність інформації має тенденцію до підвищення при збільшенні обсягів цієї інформації (даних). Виділивши необхідну частка 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.

У 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.

Зрозуміло, 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 й обирати відповідну стратегію. Предмет страхування в цих умовах є динамічний, постійно змінюваний. Подолання зростання 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 за наявності розвиненої системи інформаційної безпеки усіх без винятку її частин. Стратегії застосування страхування інформаційних ризиків залежать від такого негативного явища, як темпи зростання числа кіберзлочинів і перспектив його стабілізації.

Тема 12

ОРГАНІЗАЦІЯ СЛУЖБИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

12.1. Організація служби інформаційної безпеки підприємства.
12.2. Менеджмент персоналу у сфері інформаційної безпеки.

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 у постановці, відомій із теорії гри. Стосовно проблеми захисту інформації це означає, що для її вирішення 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 розвинених країнах склалася достатньо сформована концепція та інфраструктура захисту, основу якої складають:

– дуже розвинений 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 в усіх структурних елементах виробничої системи і на всіх 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 у залежності від зміни зовнішніх і внутрішніх умов.

Ніяка КСІБ не може забезпечити необхідного рівня забезпечення інформаційної безпеки без належної підготовки користувачів і виконання ними всіх установлених правил, спрямованих 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, де 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;

– установити відповідність змісту запланованих і проведених заходів по забезпеченню інформаційної безпеки системи вимогам розроблених інструкцій, пам'яток та 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, збері-

гання, обліку і 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 урахуванням цього КСІБ повинна мати:

– правове забезпечення (нормативні документи);

– організаційне забезпечення (наявність спеціальних служб: захисту документів; служби режиму, допуску та охорони; служби захисту інформації за 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 у сфері захисту інформації);

– нормативно-методичне забезпечення (методики, які забезпечують діяльність користувачів в умовах жорстких вимог захисту інформації).

КСІБ може бути охарактеризована низькою 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 спрямованість захисту. Розглядаються також такі напрями захисту, як правовий, організаційний і інженерно-технічний захист. Останній реалізується фізичними, апаратними та програмними засобами та математичними методами захисту.

Вирішальна роль людського фактора 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, спрямовані на знищення інформації, або передачу її зацікавленим організаціям.

Неможна, також, не відзначити, що сьогодні, як і завжди між державами світу відбувається постійна боротьба за сфери своїх інтересів. І методи цієї бо-

ротьби 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 напрямів необхідно виділити процес виявлення й 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 отримання від неї потрібної інформації, які завжди активно використовуються зацікавленими сторонами. Методи впливу:

– підкуп;
– шантаж;
– загрози;
– отримання 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 й 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 збирання інформації та контролю за її використанням, підрозділи технічного захисту інформації та підрозділи охорони. Запропонована організаційна структура служби безпеки наведена на рис. 12.1.

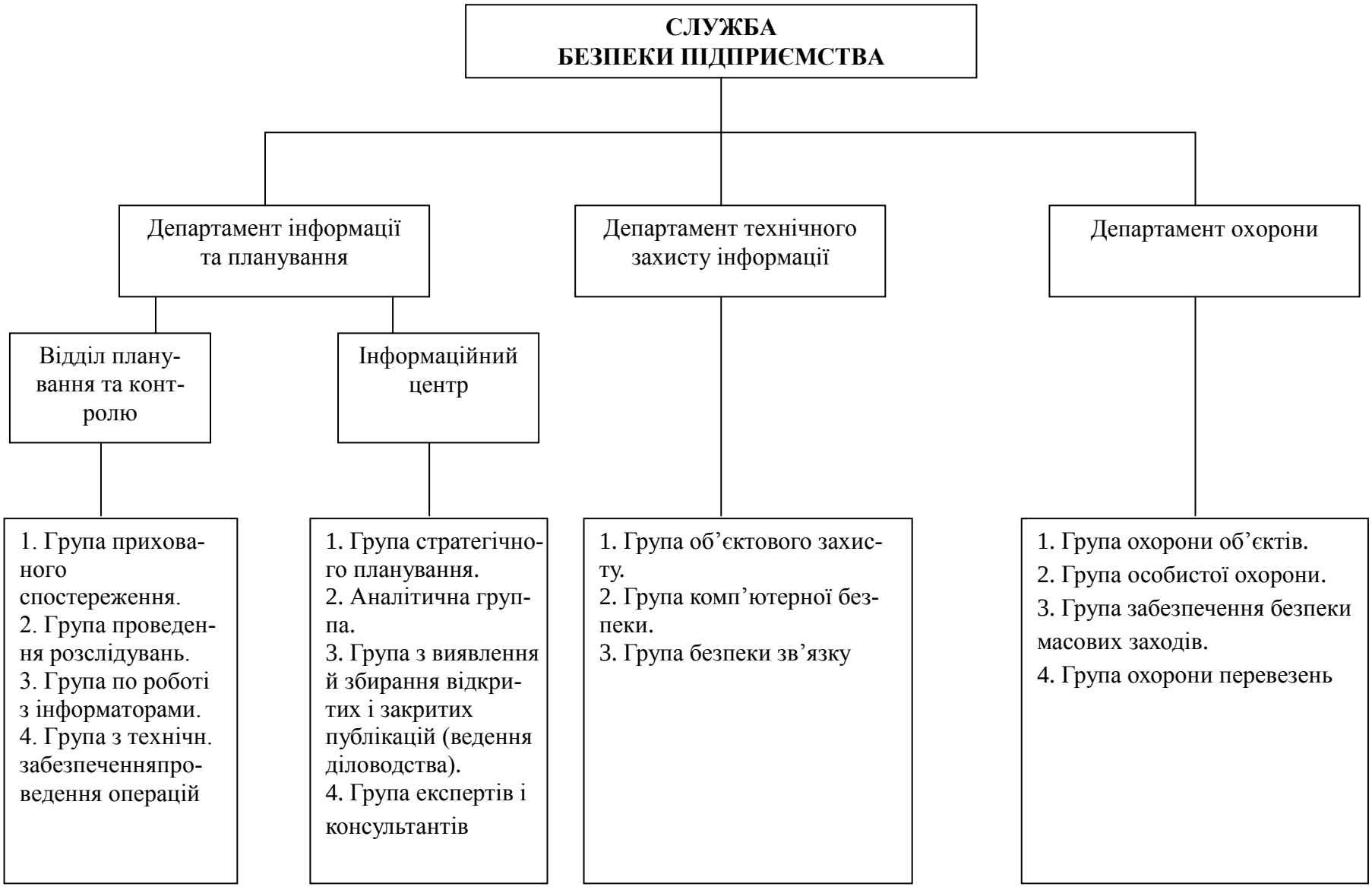


Рисунок 12.1 – Організаційна структура служби безпеки підприємства

До складу підрозділів служби безпеки входять: департамент інформації та планування, департамент технічного захисту інформації, департамент охорони.

Департамент інформації та планування:

Відділ планування та контролю:

Склад:

1. Група прихованого спостереження.

2. Група проведення розслідувань.

3. Група по роботі з інформаторами.

4. Група з технічного забезпечення 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:

1. Група стратегічного планування.

2. Аналітична група.

3. Група з виявлення й збирання відкритих і закритих публікацій (ведення діловодства).

4. Група експертів і консультантів.

Основні завдання інформаційного центру:

– проводить оцінку зовнішніх загроз для організації та розробляє комплекс заходів по їх попередженню;

– проводить збирання та аналізує інформацію в середині організації;

– проводить збір літератури та нормативних документів;

– ведення діловодства;

– проводить оцінку матеріалів.

Департамент технічного захисту інформації:

Склад:

1. Група об'єктового захисту.

2. Група комп'ютерної безпеки.

3. Група безпеки зв'язку.

Основні завдання департаменту технічного захисту інформації:

– проводить установлення та забезпечує функціонування технічних засобів охорони будівель та приміщень організації;

– проводить заходи з забезпечення безпеки інформації при використанні персональних комп'ютерів, а також при їх роботі в мережі;

– проводить заходи по забезпечення безпеки інформації при використанні засобів зв'язку (телефон, факс тощо).

Департамент охорони:

Склад:

1. Група охорони об'єктів.
2. Група особистої охорони.
3. Група забезпечення безпеки масових заходів.
4. Група охорони перевезень.

Основні завдання департаменту охорони:

– проводить заходи з фізичної охорони та оборони будівлі і приміщень організації;

– забезпечує особисту охорону керівництва 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 з підбору та розстановки 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 розвиненою 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.

Перейдемо до ролі менеджменту персоналу у сфері інформаційної безпеки.

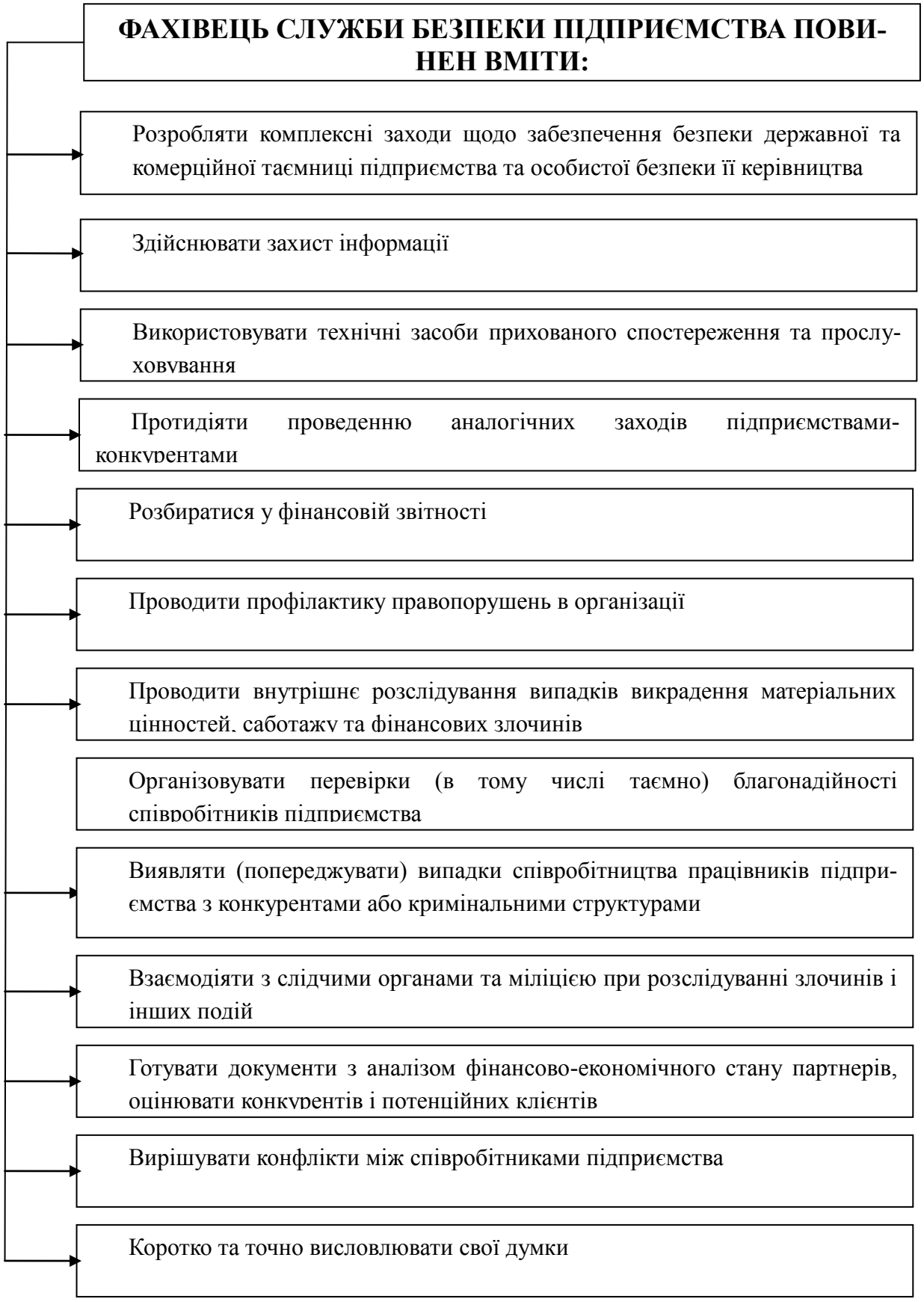


Рисунок 12.2 – Вимоги до фахівця служби безпеки інформації

12.2. Менеджмент персоналу у сфері інформаційної безпеки

Проблема захисту мереж телекомунікацій та інформації, що циркулює в них, вимагає значної уваги через те, 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 кому 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 розроблення, 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 здебільшого протидії техногенним загрозам інформаційним ресурсам. Антропогенні загрози враховуються мало. Водночас, необхідність управління персоналом тісно пов'язана із захистом комерційної таємниці фірми, тому що персонал є одним із основних носіїв інформації, і як вважають фахівці, ймовірність витоку інформації через підкуп, переманювання співробітників складає 43%, а через вивідування – 24%.

Найбільш непередбачувані 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 зале-

жить 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 виміром 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 отримавши 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 зрозуміло 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 пов'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, та регулярно отримувати інформацію щодо змін в них.

Така програма підготовки стосується вимог до забезпечення безпеки, питань юридичної відповідальності і засобів управління 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 співробіт-

ників 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 із 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 або його викрито в промисловому шпигунстві, або перехід до конкурентів), спробувати визначити справжню причину його рішення, проаналізувати і вирішити або потрібно його утримувати, або 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 вирішення подібного роду питань виник кадровий консалтінг.

Кадровий консалтінг – це система організаційно-психологічних заходів щодо діагностики і, за необхідності, 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 виконувати 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 стародавній лозунг „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. Далі переходимо до проблем аудиту інформаційної безпеки.

Таблиця 12.1 – Кадровий консалтинг

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 поєднання матеріальних та моральних складових мотивації працівника
Працівник повинен робити точно те, що йому запропоновано посадовою інструкцією	Підприємство повинно забезпечити працівнику 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	

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

1. 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/
2. Бондаренко М. Перспективы применения международного стандарта ISO/IEC в Украине / Бондаренко М., Скрыпник Л, Потий А. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: зб. наук. праць. – К., 2001. – Вип. 3. – С. 7-26.
3. Браіловський М. Підготовка фахівців з інформаційної безпеки для підрозділів органів внутрішніх справ / Браіловський М., Дорошко В. // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: зб. наук. праць. – К., 2004. – Вип. 8. – С. 154-159.
4. 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. – К., 2003. – Вип. 7. – С. 11-13.
5. Домарев В.В. Безопасность информационных технологий /Домарев В.В./ – С.Пб.: ДиаСофтЮП, 2004. – 992 с.
6. Захист інформації. Технічний захист інформації. ДСТУ 3396.0-96. – [Чинний з 01.01.1997.]. – К.: Держстандарт України, 1996. – 33 с. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html. – (Національний стандарт України).
7. Інформаційні технології. Методи захисту. Критерії оцінки для інформаційних технологій: ДСТУ ISO 15408-1: 2005. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html.

8. Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина. 1. Концепції і моделі безпеки: ДСТУ ISO/IEC TR 13335-1: 2003. – Режим доступу: http://sozinov.blogspot.com/2007/01/security-standarts.html.
9. 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=388.
10. 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.
11. 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=388.
12. 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.
13. 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=388.
14. 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=388.
15. 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=388.
16. 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.
17. 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.
18. 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.
19. 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=388.

20. Защита информации в телекоммуникационных системах / Конахович Г.Ф., Климчик В.П., Паук С.М., Потапов В.Г. – К.: МК-Пресс, 2005.–288 с
21. Зегжда Д.П. Основы безопасности информационных систем / Зегжда Д.П., Ивашко А.М. / – М.: Горячая линия – Телеком, 2000. – 452 с.
22. Калюжний Р. Питання державного управління у сфері інформаційної безпеки в умовах переходу України до інформаційного суспільства (організаційно-правовий аспект) / Калюжний Р., Гавловський В., Цимбалюк В. // Суспільні реформи та становлення громадянського суспільства в Україні: матеріали наук.-практ. конф. (Київ, 30 травня 2001 р.). – К., 2001. – С. 292-297.
23. Кононович В.Г. Основні положення концепції інформаційної безпеки телекомунікаційних мереж загального користування / Кононович В.Г., Тардаскін М.Ф. // Захист інформації. – № 1. – 2006. – С.18-30.
24. Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Парламент, 1999. – 95 с.
25. Концепція розвитку телекомунікацій в Україні до 2010 року № 316 від 7.06.2006 р. – Режим доступу: http://www.zakon1.rada.gov.ua.
26. Концепція технічного захисту інформації в Україні. – 1997. – Режим доступу: http://www.zakon1.rada.gov.ua.
27. Пастернак-Таранушенко Г. Економічна безпека держави. Статика процесу забезпечення: [підруч. для держ. служб., науков., студ. і аспір. вищ. навч. закл. економ. профілю] / Пастернак-Таранушенко Г.; за ред. проф. Б. Кравченка. – К.: Кондор, 2002. – 302 с.
28. Поповский В.В. Защита информации в телекоммуникационных системах: [учебник]: В 2-х т. Т.2. / Поповский В.В., Персиков А.В. – Харьков: ООО „Компания СМИТ", 2006. – 292 с.
29. Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах / Проект ДССЗЗІ від 20.02.2008. – С. 3. – (Офіційне видання).
30. Постанова з керування безпекою інформаційних технологій. ДСТУ ISO/IEC TR 13335:2003 року. – (Офіційне видання).
31. Тардаскіна Т.М. Підходи до оцінки витрат на підтримку та створення системи інформаційної безпеки / Тардаскіна Т.М. // Інформаційні технології в економіці, менеджменті і бізнесі. Проблеми науки, практики і освіти: Матеріали XI між нар. наук.-практ. конф., (Київ, 24-25 листопада 2005 р.) – К., 2006. – Т3. – С. 286-288.
32. Хорошко В.А. Методы и средства защиты информации / Хорошко В.А., Чекатков А.А. – К.: Юниор, 2003. – 504 с.
33. ISO/PAS 22399:2007(E). Societal security – Guideline for incident preparedness and operational continuity management // Firs edition 2007-12-01.
34. 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.

35. 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.
36. ITU-T recomendation X.816. Information technology – Open System Interconnection – Security frameworks for Open systems: Security audit and alarms framework.