МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації

На рецензію	До захисту
Завідувач кафедри УІКБ	Завідувач кафедри УІКБ
доктор економічних наук, доцент	доктор економічних наук, доцент
_____ С.В.Легомінова	_____ С.В.Легомінова
«___»_____20__ р.	«___»_____20__ р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

на тему:

ОРГАНІЗАЦІЯ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА З ВИНИ ПЕРСОНАЛУ

СТУДЕНТ: Клименко Олексій Ігорович _____
(підпис)

КЕРІВНИК: к.держ.упр. Мужанова Тетяна Михайлівна _____
(підпис)

НОРМОКОНТРОЛЕР: к.е.н., доц. Мордас Ірина Василівна _____
(підпис)

Київ – 2020

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В.Легомінова
«_____»_____ 2020 р.

ЗАВДАННЯ

на магістерську атестаційну роботу

студенту Клименку Олексію Ігоровичу

Тема роботи: «ОРГАНІЗАЦІЯ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА З ВИНИ ПЕРСОНАЛУ», затверджена наказом по університету № 81 від «16» березня 2020 р.

1. **Термін здачі** студентом оформленої роботи «___» _____ 2020 р.
2. **Об'єкт дослідження:** забезпечення інформаційної безпеки підприємства.
3. **Предмет дослідження:** організація протидії загрозам інформаційній безпеці підприємства з вини персоналу.
4. **Мета дослідження** полягає у вивченні засад організації протидії загрозам інформаційній безпеці підприємства з вини персоналу.
5. **Перелік питань, які мають бути розроблені:**

5.1 Дослідити основи забезпечення інформаційної безпеки підприємства.

5.2 Проаналізувати особливості роботи з персоналом як напряму запобігання внутрішнім загрозам інформаційній безпеці.

5.3 З'ясувати роль технічних засобів захисту інформації у протидії загрозам з вини персоналу.

6. **Дата видачі завдання «**04» лютого 2020 р.

Науковий керівник _____ Т.М. Мужанова
підпис

Завдання прийнято до виконання _____ О.І. Клименко
підпис

Державний університет телекомунікацій
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою

КАЛЕНДАРНИЙ ПЛАН
виконання магістерської атестаційної роботи

студентом КЛИМЕНКОМ Олексієм Ігоровичем

Дата видачі завдання: «04» лютого 2020 р.

№ з/п	Етапи магістерської атестаційної роботи	Термін виконання етапів	Примітка
1.	Визначення об'єкта, предмета, мети та завдань дослідження.	18.02.2020	
2.	Збір та аналіз літератури.	11.03.2020	
3.	Вивчення основ забезпечення інформаційної безпеки підприємства	25.03.2020	
4.	Дослідження роботи з персоналом як напряму запобігання внутрішнім загрозам інформаційній безпеці	08.04.2020	
5.	Встановлення ролі технічних засобів захисту інформації у протидії загрозам з вини персоналу	22.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	13.05.2020	
8.	Оформлення презентації.	20.05.2020	
9.	Отримання рецензії на роботу.	27.05.2020	
10.	Захист у ДЕК.	12.06.2020	

Студент О.І. Клименко
(підпис)

Науковий керівник Т.М. Мужанова
(підпис)

РЕФЕРАТ

Магістерська атестаційна робота присвячена дослідженню засад організації протидії загрозам інформаційній безпеці підприємства з вини персоналу. Робота складається зі вступу, трьох розділів, що містять 14 рисунків, висновків та списку використаних джерел з 47 найменувань. Загальний обсяг роботи становить 83 аркуша, з яких 5 аркушів займає список використаних джерел.

Об'єктом дослідження є забезпечення інформаційної безпеки підприємства.

Метою роботи є вивчення засад організації протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Для цього у роботі використані методи аналізу, синтезу, класифікацій та порівняння, теорій менеджменту персоналу й інформаційної безпеки, технічного захисту інформації.

Як результат у роботі досліджено основи забезпечення інформаційної безпеки підприємства; проаналізовано особливості роботи з персоналом як напряму запобігання внутрішнім загрозам інформаційній безпеці; з'ясовано роль технічних засобів захисту інформації у протидії загрозам з вини персоналу.

Галузь застосування. Розроблені підходи можуть бути використані при організації та впровадженні комплексу заходів з протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Ключові слова: ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА, ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ, ПРОТИДІЯ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ З ВИНИ ПЕРСОНАЛУ, ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ.

ЗМІСТ

ВСТУП

Актуальність теми. З огляду на наявність в інформаційному середовищі величезної кількості різноманітних загроз жодне сучасне підприємство не може ефективно функціонувати без створення надійної системи забезпечення інформаційної безпеки. Як свідчить статистика у сфері інформаційної безпеки, близько 80% зловмисників є працівниками компанії, тобто інсайдерами.

Деструктивні дії персоналу внаслідок недостатньої кваліфікованості, халатності чи зі злого умислу призводять до значних матеріальних, фінансових та репутаційних збитків підприємства. Аналіз показав, що запобігти та протидіяти більшості із внутрішніх загроз можна шляхом організації та впровадження комплексу нормативних, організаційних та технічних засобів захисту інформації з акцентом на роботу з персоналом.

З огляду на зазначене тема дипломної роботи є актуальною, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки підприємства і, зокрема дотриманню персоналом вимог щодо її забезпечення.

Мета і завдання дослідження. **Мета роботи** полягає у вивченні засад організації протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Для досягнення цієї мети в роботі необхідно виконати наступні **завдання**:

1. Дослідити основи забезпечення інформаційної безпеки підприємства.
2. Проаналізувати особливості роботи з персоналом як напряму запобігання внутрішнім загрозам інформаційній безпеці.
3. З’ясувати роль технічних засобів захисту інформації у протидії загрозам з вини персоналу.

Об’єкт дослідження - забезпечення інформаційної безпеки підприємства.

Предмет дослідження - організація протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу та управління персоналом, теорії інформаційної безпеки та технічного захисту інформації.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації заходів забезпечення інформаційної безпеки підприємства у контексті протидії загрозам з вини персоналу.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, підбору персоналу, що працюватимуть з конфіденційною інформацією, допоможуть підібрати ефективні технічні методи протидії внутрішнім загрозам інформаційній безпеці.

РОЗДІЛ 1.
ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1. Сутність та рівні забезпечення інформаційної безпеки підприємства

Сьогодні стає очевидним, що інформаційний вплив на організацію чи підприємство може бути більш ефективним, ніж матеріальний чи фінансовий, а витрати конкурентів на завдання шкоди інформаційній безпеці є порівняно низькими в порівнянні з деструктивними діями в інших сферах. Саме тому конкурентна боротьба щораз частіше відбувається в інформаційному полі, а роль забезпечення інформаційної безпеки стає першочерговою. Інформаційна безпека на нинішньому етапі має бути нерозривно пов'язана з основною діяльністю будь-якого організаційного суб'єкта.

У науці можна знайти багато підходів до розуміння сутності інформаційної безпеки.

Так, під інформаційною безпекою розуміють захищеність основних інтересів особистості, суспільства і держави в інформаційній сфері, включаючи інформаційну і телекомунікаційну інфраструктуру і власне інформацію та її параметри, такі, як повнота, об'єктивність, доступність і конфіденційність.

Вітчизняні фахівці характеризують інформаційну безпеку (у широкому розумінні) як

– вид суспільних інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов життєдіяльності;

– стан захищеності потреб в інформації особи, суспільства й держави, при якому забезпечується їхнє існування та прогресивний розвиток незалежно від наявності внутрішніх і зовнішніх інформаційних загроз;

– стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації;

– єдність трьох складових: забезпечення захисту інформації; захисту та контролю національного інформаційного простору; забезпечення належного рівня інформаційної достатності [19].

Під інформаційною безпекою організації, підприємства розуміють:

– суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи суб'єкта господарської діяльності;

– збереження конфіденційності, цілісності та доступності інформації. Доступність - це властивість бути досяжним та придатним до використання авторизованими сутностями; цілісність - це властивість захищеності точності та повноти даних; конфіденційність - це властивість захищеності інформації від неавторизованого використання фізичними особами, сутностями та процесами. Інформаційні активи - це знання чи дані, які мають цінність для організації;

– захищеність інформації та підтримуючої її інфраструктури від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації, її власникам або підтримуючій інфраструктурі [19].

Інформаційна безпека організації може розглядатися як сукупність безпечних умов функціонування інформаційних технологій, інфраструктури інформаційного простору, цілісного ринку інформації та проходження інформаційних процесів.

Відповідно, забезпечення інформаційної безпеки організації - це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток [21].

Ключовою метою забезпечення інформаційної безпеки є збереження повноти, цілісності й точності інформації, мінімізація ризику несанкціонованого втручання в інформаційні системи [4].

До основних цілей забезпечення інформаційної безпеки підприємства належать:

- запобігання витоку, втраті, спотворенню, розкраданню чи підробці інформації;

- запобігання несанкціонованим модифікації, спотворенню, копіюванню, блокуванню, знищенню інформації;

- запобігання іншим формам незаконного втручання в інформаційні ресурси і системи, створення умов для дотримання правового режиму документованої інформації як об'єкту власності;

- захист конституційних прав громадян на збереження особистої таємниці і конфіденційності персональних даних, наявних в інформаційних системах;

- збереження конфіденційності документованої інформації відповідно до законодавства [24].

Обов'язковою умовою забезпечення захищеності інформаційного середовища підприємства є створення системи забезпечення інформаційної безпеки.

Основою цієї системи є органи, сили та засоби забезпечення інформаційної безпеки, які здійснюють комплекс нормативно-правових, організаційних (організаційно-адміністративні); програмно-технічних, інформаційно-аналітичних, етичних та інших заходів, спрямованих на забезпечення стійкого функціонування бізнесу чи організації.

Установимо структуру системи забезпечення інформаційної безпеки підприємства, яка є поєднанням таких рівнів: нормативно-правового, організаційного, процедурного (операційного) та контрольного (Рис. 1.1.).

Рис. 1.1. Структура забезпечення інформаційної безпеки підприємства.

На нормативно-правовому рівні відбувається застосування зовнішнього для підприємства законодавства та нормативної бази (законів, нормативних документів держави, стандартів, специфікацій тощо), а також формування і забезпечення виконання комплексної політики інформаційної безпеки підприємства (політик, процедур, інструкцій) та системи внутрішніх вимог, норм і правил.

Головним суб'єктом організаційного блоку є департамент (служба, відділ) інформаційної безпеки, який є вузько спеціалізованим підрозділом і вирішує відповідні завдання.

У рамках процедурного (операційного) рівня розробляється комплекс заходів і дій за всіма напрямами забезпечення інформаційної безпеки і забезпечується готовність підприємства до системних і цілеспрямованих дій у сфері інформаційної безпеки.

Останній контрольний рівень передбачає проведення комплексних перевірок (аудитів) стану інформаційної безпеки на підприємстві. Таким чином, через незалежну перевірку відповідності реального стану справ встановленим правилам і вимогам забезпечується контроль за поточним станом системи заходів щодо захисту інформації й інформаційного середовища підприємства.

Нормативно-правовий рівень

Кожна організація чи підприємство у своїй діяльності із забезпечення інформаційної безпеки має керуватися і дотримуватися загальнодержавних нормативно-правових актів, зокрема норм:

– конституційного законодавства України, яке, зокрема, встановлює право кожного вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір [Конституція];

– загальних законів, кодексів які включають норми з питань інформатизації та інформаційної безпеки;

– законів про організацію управління, стосовно окремих структур господарства, економіки, системи державних органів та визначення їхнього статусу, які також містять окремі норми щодо захисту інформації;

– спеціальних законів у сфері інформаційної безпеки та захисту інформації (Закони України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації», «Про державну таємницю», «Про основні засади забезпечення кібербезпеки України», інші);

– підзаконних нормативних актів із захисту інформації;

– міжнародних, національних, галузевих стандартів, загальнодержавних і відомчих нормативних документів;

– правоохоронного законодавства, яке містить норми про відповідальність за правопорушення у сфері інформатизації [21].

Особливо важливу роль у забезпеченні інформаційної безпеки підприємства відіграє політика інформаційної безпеки. Перш за все політика потрібна для формування на підприємстві розуміння цілей і завдань інформаційної безпеки. Керівництво та персонал мають розуміти, що система забезпечення інформаційної безпеки, будучи засобом розслідування фактів порушення стану інформаційної захищеності підприємства, сприяє мінімізації ризиків для діяльності підприємства, а отже – є запорукою підвищенні її прибутковості.

Політика інформаційної безпеки є сукупністю документів різного рівня, які встановлюють правила, процедури, практичні методи й керівні принципи забезпечення інформаційної безпеки, які використовує підприємство в своїй діяльності.

Відповідно до стандарту ISO / IEC 27001 політика інформаційної безпеки, виходячи з характеристик бізнесу, організації, її розташування, активів і технологій, має:

1) охоплювати основи для встановлення цілей і розробляти загальний зміст регулювання та принципів діяльності щодо інформаційної безпеки;

2) враховувати вимоги бізнесу, правові чи нормативі вимоги, а також контрактні зобов'язання щодо безпеки;

3) узгоджуватися з контекстом стратегічного управління ризиками підприємства, в якому будуть розробляти та підтримувати СУІБ;

4) встановлювати критерії, за якими будуть оцінювати ризики;

5) бути затверджена керівництвом [15].

Загалом виділяють три рівні політики інформаційної безпеки підприємства: верхній, середній і нижній (Рис. 1.2.).

Рис.1.2. Рівні політики інформаційної безпеки

Політика інформаційної безпеки верхнього рівня встановлює позицію керівництва підприємства щодо інформаційної безпеки та відображає загальні цілі підприємства в цій сфері; є основою для розробки галузевих політик безпеки, правил та інструкцій, що регулюють окремі питання; інформує персонал підприємства та представників третіх сторін про основні завдання та пріоритети компанії у сфері інформаційної безпеки.

Політики інформаційної безпеки середнього рівня можуть регламентувати питання інформаційної безпеки у певних сферах діяльності підприємства (фінанси, продажі, маркетинг тощо) або стосуватися певних аспектів використання інформаційних технологій, організації інформаційних потоків та роботи персоналу підприємства незалежно від сфери використання технологій або зайнятості персоналу (наприклад політика

користування мережею Інтернет, політика придбання й оновлення програмного забезпечення, політика забезпечення внутрішнього та пропускного режиму).

Політика інформаційної безпеки нижнього рівня включає документи, що є інструкціями та методиками прямої дії для використання в повсякденній діяльності співробітників підприємства. Ці документи, які є по суті організаційною документацією, можуть включати бланки типових заявок на надання доступу чи отримання дозволу для здійснення окремих видів діяльності, регламенти (процедури) роботи з певними інформаційними та телекомунікаційними системами, програмним забезпеченням і базами даних, посадові обов'язки окремих категорій співробітників відносно забезпечення інформаційної безпеки, а також вимоги до персоналу, типові угоди із зовнішніми сторонами, які стосуються окремих сервісів, процедур та інформаційних систем.

Організаційний рівень

Функціонально забезпечення організаційного блоку здійснюють спеціалізовані підрозділи з інформаційної безпеки або захисту інформації або окремі фахівці підприємства.

Виділяють такі напрями організаційного забезпечення інформаційної безпеки:

- формування, підтримка і документальне забезпечення політики інформаційної безпеки підприємства (консультування керівників і розробка політики безпеки, формування вимог, регламентів, процедур створення типових форм та інших документів, укладання угод, організація роботи з персоналом, консультування фахівців та керівників підрозділів підприємства з питань інформаційної безпеки та розробки внутрішніх документів, контроль їх відповідності та дотримання);

- впровадження засобів захисту інформації, які можуть включати аналіз методик, програмних і апаратних засобів захисту інформації і підготовка пропозицій щодо їх придбання; аналіз і оцінка закуплених продуктів на

предмет їхньої надійності та наявності вразливостей, у тому числі із залученням сторонніх експертів, участь у проектуванні і тестуванні інформаційних систем, розробка техніко-економічного обґрунтування для впровадження засобів захисту інформації тощо;

- адміністрування інформаційних систем і систем захисту інформації (виконання деяких функцій з адміністрування окремих інформаційних систем, адміністрування, конфігурування та встановлення систем захисту інформації, залучення сторонніх організацій для здійснення поточного адміністрування інформаційних систем і систем захисту інформації, а також для консультаційної та технічної підтримки при виникненні інцидентів, пов'язаних з інформаційною безпекою, консультування користувачів та реагування на інциденти інформаційної безпеки;

- контроль за виконанням політики та проведення аудиту інформаційної безпеки, зокрема збір та аналіз відомостей про порушення вимог політики безпеки, перевірка організаційної документації, організація та участь у проведенні аудитів інформаційної безпеки на підприємстві, в тому числі із залученням сторонніх організацій;

- участь у забезпеченні охорони підприємства і вирішенні завдань, пов'язаних із забезпеченням безпеки підприємства у ширшому контексті (охорона території та майна підприємства, дотримання пропускного режиму, контроль за ввезенням і вивезенням матеріалів, документів та іншого майна, організація внутрішніх службових перевірок та розслідувань, контроль за дотриманням режиму роботи і правил внутрішнього розпорядку).

Процедурний (операційний) рівень

Загалом на процедурному рівні здійснюється діяльність за окремими піднапрямами забезпечення інформаційної безпеки підприємства.

Для ілюстрації використаємо рекомендації, визначені у стандарті ISO 27002 [14] (Рис. 1.3.).

Рис.1.3. Напрями (галузі) забезпечення інформаційної безпеки.

Так, наприклад, у межах управління інформаційними активами підприємства мають розроблятися рекомендації, інструкції, вимоги та інші організаційні документи з питань: класифікації інформації, інвентаризації і маркування активів, встановлення відповідальності і належного поводження з інформаційними активами, передачі й утилізації переносних носіїв та інших, відповідно до специфіки діяльності підприємства.

Аналогічно можна розглянути приклад процедурних заходів з управління персоналом, які мають включати заходи щодо формування вимог до працівників у сфері інформаційної безпеки з урахуванням принципу мінімізації загроз несанкціонованого доступу до інформації; ускладнений професійний підбір і відбір персоналу; підвищення обізнаності й навчання персоналу з інформаційної безпеки; контроль і оцінювання діяльності працівників; застосування засобів матеріального і морального стимулювання праці; підтримання сприятливого соціально-психологічного клімату в трудовому колективі; вивільнення персоналу відповідно до спеціальних процедур тощо.

Контрольний рівень

Як зазначалося вище, контрольний рівень передбачає проведення комплексних перевірок (аудитів) стану інформаційної безпеки на

підприємстві, завдяки яким забезпечується ефективне функціонування системи заходів захисту інформації й інформаційного середовища підприємства.

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам.

Відповідно до стандарту ISO 19011:2011 аудит – це систематичний, незалежний та документально підтверджений процес отримання аудиторських доказів та об'єктивної їх оцінки для визначення ступеня виконання критеріїв аудиту.

У практиці забезпечення інформаційної безпеки зустрічаються: внутрішній аудит, який проводиться самим підприємством або від його імені для огляду керівництва та інших внутрішніх цілей (наприклад, для підтвердження ефективності системи управління або отримання інформації для вдосконалення системи управління); зовнішній аудит, який передбачає проведення перевірки, по-перше, сторонами, які зацікавлені в організації, наприклад клієнтами або іншими особами від їх імені, по-друге, незалежними аудиторськими організаціями, такими як регулятори або органи, що надають сертифікацію. Бувають також комбіновані та спільні аудити [6].

Цілями аудиту можуть бути:

– встановлення рівня захищеності інформаційних ресурсів підприємства, виявлення недоліків та визначення напрямків подальшого розвитку системи інформаційної безпеки;

– перевірка керівництвом підприємства та іншими зацікавленими сторонами досягнення системою забезпечення інформаційної безпеки або окремими її складовими поставлених цілей, виконання вимог політики безпеки;

– контроль ефективності та економічної обґрунтованості інвестицій у придбання засобів захисту інформації та реалізацію заходів забезпечення інформаційної безпеки;

– сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність міжнародним стандартам ISO 27001).

1.2. Інформація як основний об’єкт інформаційної безпеки

Безпосереднім об’єктом правопорушень у сфері інформаційної безпеки насамперед є інформація (дані). Правопорушник отримує доступ до інформації, що охороняється, без дозволу її власника, або з порушенням встановленого порядку доступу.

Відповідно до Закону України «Про інформацію» інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. До інформації обмеженого доступу відносять конфіденційну, таємну і службову.

Вітчизняний законодавець установив, що інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою (за винятком органів державної влади) є конфіденційною [32].

Цивільний Кодекс України визначає комерційну таємницю як інформацію, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв'язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію [43].

Комерційну таємницю умовно розділяють на дві групи: комерційну інформацію та технічну інформацію.

До першої групи належать створені підприємством, але незапатентовані науково-технічні розробки, бази даних та комп'ютерні програми, нововведення і винаходи, технічні проекти і зразки продукції, товарні знаки тощо.

Відповідно до іншого бачення, до комерційної таємниці можуть бути віднесені:

– відомості наукового характеру (ідеї, відкриття, винаходи; наукові відкриття і формули; інноваційні технічні проекти; нові методи організації виробництва і праці; програмні продукти; здобутки наукових досліджень);

– технологічні відомості (конструкторські креслення, схеми і записи; описи технологічних процесів; технології «ноу-хау»; характеристики конструкції виробів, параметри розроблених технологічних процесів; відомості про склад продукції загалом та окремих її деталей, характеристики обладнання та умови проведення експериментальних досліджень; новостворені технологічні прилади, верстати, інші елементи устаткування;

– відомості ділового характеру (інформація про заплановані або укладені угоди; дані про клієнтів і постачальників; маркетингові дослідження; інформація про конфіденційні переговори; обрахунки витрат на виробництво, структура цін, обсяги прибутків; плани розвитку та залучення інвестицій (Рис. 1.4.).

Рис. 1.4. Види інформації, що становить комерційну таємницю.

Говорячи про сфери діяльності організації чи підприємства, де створюється і здійснюється робота з комерційною таємницею, виділяють

такі: управління; виробництво; оплата праці; ціни; плани; фінанси; угоди; партнерські відносини [38].

Говорячи про логіку віднесення інформації до комерційної таємниці з економічної точки зору, варто відзначити, що до цієї категорії інформації обмеженого доступу можуть бути віднесені відомості, які генеруються і використовуються підприємством у зв'язку з тими видами діяльності, які відповідають цілям підприємства у даний момент і в перспективі, а прибуток внаслідок цих видів діяльності є вищим, аніж у конкуруючих фірм. Відповідно втрата чи витік такої інформації матиме негативний вплив на конкурентоспроможність підприємства та його позицію на ринку. А, отже, підприємство зацікавлене захищати такі відомості, в тому числі документи в електронному чи паперовому вигляді, креслення, моделі, макети тощо, засоби їх обробки та передачі, а також працівників, які працюють з конфіденційними даними.

Загалом до службової інформації, яка потенційно може містити комерційну таємницю, відносять відомості про:

- фінансову діяльність підприємства (за винятком офіційно встановленої чинним законодавством звітності, яка не може бути засекречена);
- обсяги прибутків, розмір собівартості продукції, рівень цін і наявність товарів, торговельні операції;
- стратегічні і тактичні плани розвитку підприємства;
- конкурентоспроможність продукції, ефективність експорту й імпорту, запланований час виходу товарів на ринок;
- плани маркетингової і рекламної діяльності;
- партнерів, клієнтів, посередників та контракти з ними, а також конкурентів і їхній фінансовий стан [10].

На думку зарубіжних фахівців, за ступенем конфіденційності інформація, яка належить підприємству, може підрозділятися на конфіденційну і строго конфіденційну (комерційну таємницю).

До конфіденційної інформації відносять інформацію про діяльність підприємства, розголошення якої може призвести до зниження ефективності функціонування елементів системи, що забезпечують життєдіяльність підприємства, зокрема планово-аналітичні і звітні матеріали за поточний період часу щодо:

- вивчення і формування нових напрямків інвестиційної політики підприємства;

- методів і форм роботи з активами, структуру інвестиційного портфеля;

- нових напрямів діяльності підприємства, які мають на меті підвищення його ефективності;

- результатів нагляду за роботою організацій, що працюють за участю банківського капіталу, дані про операції з акціями клієнтів;

- додаткових угод, протоколів та інших документів.

Натомість, до комерційної таємниці відносять відомості стратегічного характеру, розголошення яких може призвести до зриву функціонування однієї або кількох систем підприємства, завдання деструктивного впливу на її життєдіяльність і розвиток, в тому числі інформацію про:

- мету й завдання підприємства, шляхи їх реалізації;

- порушення і прорахунки в діяльності підрозділів підприємства;

- причини, що стримують розвиток підприємства, викликані діями державних органів, конкурентів, внутрішніми чинниками, основні проблеми і труднощі підприємства, можливості їх подолання;

- зміст і результати нарад і засідань вищого керівництва підприємства.

З урахуванням прийнятого поділу пропонується наступний приблизний перелік конфіденційних відомостей, які підлягають захисту.

1. Відомості про діяльність та управління підприємством:

- концепція, плани і перспективи розвитку підприємства, включаючи його автоматизовану систему;

- штатні розклади, структури і функціональні обов'язки працівників;

- плани і схеми розміщення службових приміщень і обладнання, розподіл відповідальності за них між посадовими особами установи;

- ділове і службове листування, приватна інформація;

- персональні дані персоналу підприємства та його філій.

2. Відомості про функціонування систем забезпечення безпеки:

- плани розгортання, технічні характеристики систем і засобів безпеки;

- дані про розмежування прав доступу персоналу до конфіденційної інформації і повноваження користувачів;

- розподіл службових автомобілів за посадовими особами підприємства, місця паркування, маршрути руху, станції технічного обслуговування;

- інформація про розташування складів матеріальних цінностей та носіїв інформації, обладнання їх засобами безпеки і порядку доступу до них.

3. Відомості про потужності й організацію функціонування інформаційних систем:

- дані про розробників ІС та засоби її захисту, прийнятих технічних рішеннях захисту інформації;

- інформація про заходи, вжиті для забезпечення безпеки інформаційних ресурсів, інфраструктури та персоналу підприємства;

- вихідний код унікального програмного забезпечення;

- дані про технічні можливості ІС з обробки інформації, що надходить від клієнтів і партнерів [36].

Ще одним видом інформації обмеженого доступу, яка може бути у використанні чи володінні підприємства, є професійна таємниця, під якою розуміють заборонені для розголошення матеріали, документи, інші відомості, якими користується особа в ході та внаслідок виконання своїх професійних обов’язків. Заборону на поширення такої інформації, яка може зашкодити правам або законним інтересам довірителя, встановлено законом. До професійних таємниць належать адвокатська, судова, нотаріальна, аудиторська, журналістська, лікарська та інші.

Окремий великий блок інформації обмеженого доступу, яка сьогодні дуже часто потрапляє у розпорядження багатьох організацій, є персональні дані.

Закон України «Про захист персональних даних» визначає зміст даного поняття як відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [31]. Водночас, на концептуальному рівні відсутні критерії віднесення інформації до персональних даних.

Персональні дані поділяють на дві категорії: загальні та особливі (чутливі).

До загальної категорії віднесено: прізвище та ім'я; дату та місце народження; громадянство; сімейний стан; відомості про соціальне, фінансове і матеріальне становище; підпис; дані з посвідчення водія, актів цивільного стану та дипломів про освіту; пенсійний номер; адресу місця проживання тощо.

Особлива категорія включає інформацію про: національне, етнічне і расове походження; стан здоров'я (медичні); біометричні й генетичні характеристики; світоглядні, політичні й релігійні переконання; членство в політичних партіях, професійних, релігійних, громадських організаціях; притягнення до адміністративної чи кримінальної відповідальності; вчинення щодо особи будь-яких видів насильства тощо [46].

Багато організацій, підприємств, установ у зв'язку із своєю основною діяльністю здійснюють різні дії з даними своїх працівників, клієнтів, партнерів та інших третіх сторін, зокрема збирання, реєстрацію, накопичення, зберігання, зміну, поновлення, використання і поширення знеособлення і знищення персональних даних, насамперед з використанням інформаційних (автоматизованих) систем. І відповідно до законодавства вони зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу.

Таким чином, підприємство має захищати дані, відомості, якими володіє або розпоряджається з дозволу законного володільця. До першої категорії відносять насамперед комерційну таємницю, а також конфіденційну інформацію та професійні таємниці, за умови отримання такої інформації фахівцями підприємства в процесі їх професійної діяльності. Другу категорію становлять насамперед персональні дані, а також будь-яка приватна інформація, яка може потрапити в систему обробки даних підприємства в ході його діяльності. Загальна схема представлена на Рис. 1.5.

Рис.1.5. Види інформації обмеженого доступу підприємства.

1.3. Види загроз інформаційній безпеці підприємства

Аналізу змісту поняття «інформаційна безпека» дослідники зазвичай приділяють значну увагу, у той час як такі поняття, як небезпека і загроза розглядаються дещо спрощено і здебільшого у звуженому плані, відірваному від контексту поняття «інформаційна безпека».

Необхідність у розробленні поняття «загроза» визначається:

1) відсутністю єдиного підходу до дослідження основних понять інформаційної безпеки;

2) недостатньою розробленістю родового поняття «загроза» і питань його відмежування від інших споріднених понять, таких, як «небезпека», «виклик», «ризик», і відповідно видового «інформаційна загроза» і його відмежування від таких понять, як «інформаційне протиборство», «інформаційний тероризм»;

3) наявністю невирішеної проблеми формування категорійно-понятійного апарату теорії інформаційної безпеки;

4) можливістю на підставі теоретичних розробок даного апарату формувати адекватну систему моніторингу та управління загрозами та небезпеками в інформаційній сфері [5, с.118].

Загрози інформаційній безпеці - сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері. Основні загрози інформаційній безпеці можна розділити на три групи:

- загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання);
- загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність на інформацію і речову власність на документовану інформацію; праву на особисту таємницю; праву на захист честі і особистої гідності тощо) [39].

Загроза інформаційній безпеці організації, підприємства - будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку ІТКС. Тобто загроза - це будь-який потенційно можливий несприятливий вплив [5, с. 20].

Також під загрозою мають на увазі явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію бізнес-інтересів в інформаційній сфері та створюють небезпеку для інформації підприємства.

Загрози інформаційній безпеці можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто віднаходження

джерела актуалізації певних подій характеризується таким елементом, як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю відповідно до теорії множин є не вичерпними, а отже і не можуть бути піддані повному описові.

У науці представлено багато підходів до класифікації загроз інформаційній безпеці підприємства. Основні з них представлені на рис. 1.2.

Рис. 1.6. Види загроз інформаційній безпеці.

Розглянемо деякі з представлених видів окремо.

За ймовірністю реалізації:

- ймовірні - такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкту, яке передує самій атаці;

- неможливі - такі загрози, які за виконання певного комплексу умов ніколи не відбудуться. Такі загрози зазвичай мають більше декларативний

характер, не підкріплений реальною і, навіть, потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер;

- випадкові - такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

За характером реалізації загрози поділяють на:

- реальні - активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;

- потенційні - активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування підприємства;

- здійснені - такі загрози, які втілені у життя;

- уявні - псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

За структурою впливу загрози:

- системні - загрози, що впливають одразу на всі складові елементи підприємства. Цей вплив має відбуватись одночасно в декількох найбільш уразливих і важливих місцях. Для підприємства це може бути вплив шкідливого програмного забезпечення, хакерські атаки, використання методів шпигунства, підкуп працівників, поширення дезінформації щодо підприємства тощо.

- структурні - загрози, що впливають на окремі структури системи. Дані загрози є також небезпечними, водночас вони стосуються структури окремих підрозділів або їх елементів;

- елементні - загрози, що впливають на окремі елементи структури системи. Дані загрози носять постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу [8].

За ставленням до загроз:

- об'єктивні - такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта;

- суб'єктивні - така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації тих чи інших обставин та чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці [29, с.8].

За значенням:

- допустимі - такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;

- недопустимі - такі загрози, які: 1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи; 2) можуть призвести до змін, не сумісних із подальшим існуванням системи.

За перебуванням джерела:

- зовнішні;

- внутрішні.

За формами закріплення:

- нормативні - офіційно усвідомлені і визнані як такі в нормативних актах країни;

- ненормативні - існують об'єктивно, але не є усвідомленими вищим політичним керівництвом держави і не знайшли адекватного віддзеркалення у нормативній системі держави.

За джерелами походження:

- природного походження - включають в себе природні явища, що можуть порушити якість зв'язку (повені, буревії, що можуть спровокувати вихід з ладу кабелів зв'язку, систем електропостачання тощо).

- техногенного походження - транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів організацій та установ тощо;

- антропогенного походження - вчинення людиною різноманітних дій з руйнування ІС, ресурсів, програмного забезпечення об'єкта тощо.

До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини (це, наприклад, може бути помилковий запуск програми, ненавмисне інсталяція закладок тощо); навмисні (інспіровані), що стали результатом навмисних дій людей (наприклад: навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне введення вірусів тощо) [8].

Зовнішні загрози можуть бути спрямовані на пасивні носії інформації і виражатися, наприклад, в наступному: спроби викрадення документів або зняття копій з документів, знімних носіїв (флеш-карти), зняття інформації, що виникає в процесі комунікацій; знищення інформації або пошкодження її носіїв; випадкове або навмисне доведення до відома конкурентів документів або матеріалів, що містять комерційну таємницю.

Дії ззовні можуть бути також спрямовані на персонал компанії і виражатися у формі підкупу, погроз, шантажу, вивідування інформації, що становить комерційну таємницю, або припускати переманювання провідних спеціалістів на конкуруючу фірму тощо.

Внутрішні загрози становлять найбільшу небезпеку для новосформованих і не усталених колективів, де не встигли скластися традиції підтримки високої репутації підприємства, однак увагу своєчасному розкриттю цих загроз повинна приділятися повсюдно. Не виключена ймовірність того, що окремі співробітники з високим рівнем самооцінки через незадоволення своїх амбіцій (невдоволення рівнем заробітної плати, відносинами з керівництвом, колегами тощо) можуть вживати заходів щодо ініціативної видачі комерційної інформації конкурентам, а також спробувати знищити важливу інформацію або пасивні

носії (наприклад, внести комп'ютерний вірус). За оцінками психологів, до 25% всіх службовців фірм, прагнучи заробити кошти у будь-який спосіб і за всяку ціну, часто на шкоду інтересам своєї фірми, очікують зручного випадку для розголошення комерційних секретів, їх продажу.

При оцінці загроз інформаційній безпеці та виборі пріоритетів у системі захисту підприємства варто детальніше розглянути джерела загроз.

Як відзначено вище джерела загроз інформаційній безпеці підприємства можна розділити на три групи: антропогенні, техногенні та стихійні.

У групу антропогенних джерел загроз безпеки інформації входять:

- кримінальні структури, рецидивісти і потенційні злочинці;
- недобросовісні партнери і конкуренти;
- персонал установи (банку, його філій).

З урахуванням аналізу міжнародного досвіду захисту інформації та досвіду проведення аналогічних робіт у вітчизняних організаціях зловмисні дії персоналу можна розділити з урахуванням соціальних передумов, характерних для країн пострадянського простору, на чотири основні категорії:

1) переривання - припинення нормальної обробки інформації, наприклад внаслідок руйнування обчислювальних засобів. Такі дії можуть викликати дуже серйозні наслідки, якщо навіть інформація при цьому не піддається ніяким впливам;

2) крадіжка - читання або копіювання інформації, розкрадання носіїв інформації з метою отримання даних, які можуть бути використані проти інтересів власника (власника) інформації;

3) модифікація інформації - внесення в дані несанкціонованих змін, спрямованих на заподіяння шкоди власнику (власнику) інформації;

4) руйнування даних - необоротна зміна інформації, що приводить до неможливості її використання.

До техногенних джерел загроз відносяться:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;

- засоби зв'язку, охорони, сигналізації;
- інші технічні засоби, що застосовуються на підприємстві;
- глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт тощо).

До стихійних джерел загроз відносяться пожежі, землетруси, повені, урагани та інші форс-мажорні обставини. Сюди ж входять і різні непередбачені обставини і нез'ясовні явища.

До внутрішньодержавних джерел загроз інформаційній безпеці відносяться:

- недостатня економічна міць держави і недостатнє фінансування заходів щодо забезпечення інформаційної безпеки;
- критичний стан вітчизняних галузей промисловості;
- відставання України від провідних країн світу за рівнем інформатизації більшості сфер життєдіяльності;
- недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня правозастосовна практика;
- несприятлива криміногенна обстановка, що супроводжується тенденціями зрощування державних і кримінальних структур в інформаційній сфері, отримання кримінальними структурами доступу до конфіденційної інформації, посилення впливу організованої злочинності на життя суспільства;
- недостатня координація діяльності щодо формування та реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки;
- нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком інформаційного ринку України;
- зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки;
- недостатня активність органів державної влади України в інформуванні суспільства про свою діяльність, у роз'ясненні прийнятих рішень, у формуванні відкритих державних ресурсів і розвитку системи доступу до них громадян [8].

Висновки до першого розділу

Встановлено, що забезпечення інформаційної безпеки підприємства – це цілеспрямована діяльність його органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища підприємства, що забезпечує його нормальне функціонування і динамічний розвиток. Структура системи забезпечення інформаційної безпеки підприємства включає такі рівні: нормативно-правовий, організаційний, процедурний (операційний) та контрольний.

Безпосереднім об’єктом правопорушень у сфері інформаційної безпеки насамперед є інформація (дані). Підприємство має захищати дані, відомості, якими володіє або розпоряджається з дозволу законного володільця. До першої категорії відносять насамперед комерційну таємницю, а також конфіденційну інформацію та професійні таємниці. Другу категорію становлять насамперед персональні дані, а також будь-яка приватна інформація, яка може потрапити в систему обробки даних підприємства.

Встановлено, що під загрозою інформаційній безпеці підприємства розуміють явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію власних інтересів підприємства в інформаційній сфері та створюють небезпеку для її інформації.

У науці представлено багато підходів до класифікації загроз інформаційній безпеці, одна загалом їх усіх можна поділити на три групи: загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації); загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (на виробництво інформації, інформаційні ресурси, на системи їхнього формування і використання); загрози інформаційним правам і свободам особистості (праву на виробництво, розповсюдження, пошук, одержання, передавання і використання інформації; праву на інтелектуальну власність, особисту таємницю тощо).

РОЗДІЛ 2
РОБОТА З ПЕРСОНАЛОМ ЯК НАПРЯМ ЗАПОБІГАННЯ ВНУТРІШНІМ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

2.1. Загрози інформаційній безпеці підприємства з вини персоналу

Недостатньо ефективна діяльність із забезпечення інформаційної безпеки на підприємстві, тобто недотримання вимог щодо конфіденційності, цілісності, доступності, достовірності інформації, яка належить підприємству, або знаходиться у його розпорядженні, матиме багато негативних наслідків, які умовно поділити на три рівні.

До першого відносять: збої у функціонуванні систем управління технологічними процесами й іншими критичними системами; розголошення відомостей, що становлять комерційну й інші види таємниць; несанкціонований доступ до персональних даних фізичних осіб тощо.

Наслідки другого рівня включають: погіршення ділових відносин із партнерами; зриви угод і переговорів, втрата інвестицій і контрактів; невиконання договірних зобов'язань; вкладення додаткових коштів у ринкові дослідження тощо Найбільш серйозним наслідком такого ланцюга втрат є фінансові збитки, пов'язані з новими розробками; зниження цін або обсягів реалізації; погіршення ділової репутації; позбавлення вигідних умов кредитування; труднощі в постачанні тощо. За певних умов нехтування питаннями захисту інформації може призвести до повного банкрутства підприємства. Тому питання побудови ефективної системи забезпечення інформаційної безпеки є життєвоважливим для підприємства [17, с. 32].

Значний відсоток загроз інформаційній безпеці підприємства становлять загрози внутрішнього характеру, тобто деструктивні дії з боку персоналу. Однак, дуже часто керівництво компанії не надає достатнього значення цим проблемам. Дії внутрішніх порушників, такі як недбалість, крадіжки інформаційних ресурсів та устаткування ІС, фінансові й інші види шахрайства з

використанням інформаційних систем і ресурсів тощо, набагато рідше стають предметом уваги при розв’язанні проблем інформаційної безпеки.

Саме про це свідчать результати досліджень, відповідно до яких близько 80% зловмисників належить до інсайдерів. У компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових утрат [12].

Виходячи із даних антирейдерського союзу підприємців України 82% загроз реалізується власними співробітниками фірми або за їх безпосередньої або опосередкованої участі; 1% загроз реалізується випадково [17].

Аналіз, проведений на підприємствах середнього бізнесу, показав, що загрози з Інтернету потенційно можуть нашкодити менше, ніж деструктивні дії інсайдерів. Отже, саме протидія внутрішнім загрозам має становити левову частку діяльності підприємства у сфері інформаційної безпеки.

До внутрішніх загроз відносять дії чи бездіяльність персоналу (навмисні чи ненавмисні), які йдуть врозріз з інтересами підприємства, наслідком яких може бути нанесення економічних збитків, втрата інформаційних ресурсів, підрив ділової репутації підприємства, погіршення відносин з партнерами тощо [1, 27].

Внутрішні загрози об’єктам інформаційної безпеки підприємства (тобто загрози з боку персоналу) за способом впливу доцільно об’єднати в п’ять груп: власне інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні (Рис. 2.1.).

Рис. 2.1. Внутрішні загрози інформаційній безпеці підприємства.

Розглянемо кожну з категорій детальніше.

До інформаційних загроз належать:

- порушення персоналом своєчасності інформаційного обміну, незаконні збір і використання інформації;
- несанкціонований доступ до інформаційних ресурсів;
- маніпулювання інформацією (приховування, викривлення інформації, дезінформування);
- протизаконне копіювання інформації в ІТКС;
- викрадення інформації з банків і баз даних, архівних установ;
- недотримання технологій обробки інформації.

До програмно-математичних загроз належать: запуск програм-вірусів; установка програмних і апаратних закладок; зміна і знищення даних в ІТКС.

Фізичні загрози включають:

- руйнування або знищення засобів зв’язку й обробки інформації;
- викрадення, руйнування або знищення носіїв інформації;
- викрадення засобів криптографічного захисту, програмних / апаратних ключів;
- деструктивний вплив на персонал тощо.

До радіоелектронних загроз належать:

- перехоплення конфіденційної інформації технічними каналами;
- вбудовування електронних пристроїв перехоплення інформації в технічні засоби та розміщення їх на об’єктах інформаційної безпеки;
- перехоплення, дешифрування та подання дезінформації в мережах зв’язку і передачі даних;
- вплив на парольні та ключові системи;
- радіоелектронне придушення автоматизованих систем управління і мереж зв’язку.

До організаційно-правових загроз слід віднести:

- придбання ІТ та засобів інформатизації, які містять відомі чи невиявлені недоліки, або є застарілими;

- недотримання вимог законодавства або затримка прийняття необхідних рішень у відповідності з їхніми положеннями в інформаційній сфері на рівні підприємства;

- неправомірне обмеження доступу до документів з важливою для підприємства інформацією [28].

Способи реалізації внутрішніх загроз поділяють на реалізовані:

- технічними каналами (канали побічного електромагнітного випромінювання і наведень, акустичні, оптичні, радіотехнічні, хімічні та інші канали;

- каналами спеціального впливу через формування полів і сигналів із метою порушення цілісності інформації або руйнування системи безпеки;

- методами несанкціонованого доступу шляхом підключення до засобів та ліній зв'язку, маскування під легітимного користувача, подолання заходів захисту для використання наявної інформації або надання хибної інформації, застосування програмно-апаратних закладок і впровадження вірусних програм.

Загрози, реалізовані першими двома способами, це загрози фізичного рівня, а останнім – програмно-математичного.

Водночас, варто виділити і загрози, що реалізуються шляхом психологічного впливу на персонал підприємства, а саме з використанням різноманітних методів соціальної інженерії.

Працівники підприємства, які мають безпосередній законний доступ до автоматизованої системи, можуть реалізувати такі загрози:

– викрасти конфіденційну інформацію - скопіювати інформацію на портативні пристрої, чи на зовнішні носії, опублікувати її на веб-сайті, відправити за помилковою адресою. Такі дії можуть бути вчинені внаслідок помилки або навмисно;

– порушити авторські права на інформацію – несанкціоновано копіювати авторський документ чи його частину, зашифрувати документ з власним паролем, підробити реквізити іншого користувача чи компанії. Найчастіше реалізується через навмисні дії користувачів;

– здійснити шахрайство - спотворити фінансову документацію, перевищити повноваження під час роботи з базами даних, модифікувати важливі дані. Здійснюється навмисно для досягнення деструктивної мети;

– саботувати інформацію, тобто навмисно в прихований спосіб зривати виконання важливих заходів, вказівок щодо роботи з інформацією. Реалізується навмисно задля досягнення певної мети чи для помсти [13].

Аналізуючи чинники виникнення внутрішніх загроз, серед основних виділяють такі:

- непрофесійні дії працівників;
- низький стан виховної та профілактичної роботи на підприємстві;
- недосконала система заробітної плати та стимулювання праці персоналу;
- порушення правил кадрової роботи, невідповідність кадрової політики умовам роботи на підприємстві;
- психологічні та комунікативні особливості працівників;
- відсутність нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу;
- низький стан трудової та виробничої дисципліни, слабка вимогливість керівного складу [1].

На основі зазначеного підходу джерела загроз інформаційній безпеці підприємства з вини персоналу умовно можна поділити на навмисні та ненавмисні. (Рис. 2.2.).

До навмисних варто віднести скривдженість, нелояльність, впровадженість, недосконалість системи заробітної плати та мотивування персоналу. Серед ненавмисних можна виділити халатність, низький стан виховної та профілактичної роботи, психологічні та комунікабельні особливості працівників, низький стан трудової дисципліни, непрофесійні дії, порушення правил кадрової роботи, відсутність нормативної бази, яка б установлювала режим діяльності персоналу, слабкі дії керівного складу.

Рис. 2.2. Джерела загроз інформаційній безпеці з вини персоналу.

Цікавим для розуміння мотивів внутрішнього порушника є факторний підхід, запропонований російськими науковцями [26], відповідно до якого через виявлення факторів ризику з боку персоналу можна ефективніше протидіяти деструктивним діям внутрішніх порушників.

Отже, до факторів ризику фахівці відносять:

– Наявність у працівника мотивів для протиправних дій.

– Надмірна концентрація повноважень в одного працівника.

– Наявність у багатьох працівників ексклюзивних знань про бізнес підприємства та його операційне середовище.

– Недостатність або ускладненість процедур контролю за діяльністю персоналу та виявлення порушень.

– Слабка регламентація (або навіть повна її відсутність) певних видів діяльності, що здійснюються на підприємстві.

– Впровадження змін операційного середовища підприємства, які не є виправданими з точки зору бізнесу.

– Недостатня детермінованість процесів основної діяльності підприємства.

– Неналежне регламентування і здійснення відносин володіння / відповідальності щодо інформаційних активів.

– Змова внутрішнього і зовнішнього зловмисників.

– Неефективний менеджмент персону, наслідком якого є недостатня лояльність і надійність працівників підприємства.

– Об'єктивна невідповідність функціональності ІС підприємства вимогам бізнесу.

– Зловживання довірою інших співробітників підприємства.

– Недооцінка загроз з вини персоналу і недостатність заходів у цьому напрямі [26].

Проаналізувавши представлений перелік факторів ризику, можна з упевненістю сказати, що їх подолання є можливим за умови ефективної організації діяльності підприємства, забезпечення комплексу заходів інформаційної безпеки та налагодження якісної роботи з персоналом.

2.2. Процедури відбору та звільнення фахівців, які працюють з конфіденційною інформацією

Очевидно, що основи для формування кваліфікованого та надійного фонду працівників підприємства у сфері інформаційної безпеки є забезпечення ґрунтовного пошуку і якісної перевірки потенційних працівників. Тому одним із найбільш важливих етапів у роботі з персоналом підприємства є процес відбору можливих кандидатів для призначення на посади з інформаційної

безпеки. При відборі претендентів на зайняття вакантної посади оцінюють відповідність кожного кандидата таким основним вимогам:

- рівень підготовки та кваліфікації, наявність необхідного досвіду роботи;
- морально-ділові й особисті якості;
- ступінь відповідальності за прийняті рішення (для керівних посад).

При відборі кандидатів на посади, що передбачають роботу з конфіденційною інформацією, обов'язковим є врахування рівня кожної конкретної посади з точки зору прийняття й реалізації управлінських рішень, виконання організаторських функцій і завдань з виконання основної діяльності.

На основі зазначених критеріїв, дані посади поділяють на такі групи посад:

- керівники підприємства (директор підприємства, філії, представництва);
- заступники керівників;
- керівники структурних підрозділів;
- керівники служб безпеки та їх заступники;
- співробітники служб безпеки;
- співробітники, які на постійній основі працюють з конфіденційною інформацією у відповідних структурних підрозділах.

При відборі кандидатів на зазначені посади додатково враховують обсяг і важливість відомостей конфіденційного характеру, до яких допускаються працівники [27].

Організаційні заходи при відборі персоналу, що одержує доступ до конфіденційної інформації, умовно розділяють на такі групи:

- проведення ускладнених аналітичних процедур при прийомі і звільненні працівника;
- документування добровільної згоди працівника не розголошувати конфіденційні відомості й дотримуватися вимог інформаційної безпеки;
- інструктування й навчання працівника, як на практиці діяти в умовах забезпечення інформаційної безпеки.

Рис. 2.3. Організаційні заходи при найманні персоналу у сфері інформаційної безпеки.

У ході прийняття документів кандидата на зайняття посади у сфері інформаційної безпеки перевіряють наявність усіх необхідних довідок і документи, аналізують достовірність і правильність їх оформлення (відповідність прізвища, імені та по батькові, інших персональних даних, наявність необхідних відміток, записів і печаток, ідентичність фотокарток і особи громадянина, використання потрібної форми бланка документа, відсутність підчисток, незавірених виправлень, спроб заміни аркушів, фотографій тощо). У випадку виникнення певних сумнівів щодо достовірності документів кандидату пропонують надати зразки документів повторно, завірити виправлення або відмовляють у прийомі на роботу.

Тільки після ретельного аналізу поданих документів з кандидатами на посаду проводиться співбесіда [28].

Важливим етапом підбору персоналу є проведення співбесід з кандидатами на посаду в галузі інформаційної безпеки та захисту інформації, які допомагають з’ясувати реальну причину бажання кандидата працювати в конкретній організації чи на підприємстві; виявити потенційних зловмисників або спробувати схильність кандидата до злочинних дій; переконатися в добровільній згоді кандидата дотримуватися правил захисту інформації й прийняти пов’язані з роботою обмеження у професійному й особистому житті [39].

Окрім співбесіди у кілька етапів (з фахівцем відділу кадрів, представником або керівником підрозділу потенційної роботи, заступником з інформаційної

безпеки тощо) використовують опитувальники для з'ясування причин звільнення кандидата з колишнього місця роботи, джерело інформації про вакансії, наявність досвіду роботи з конфіденційною інформацією, стосунки в сім'ї, рівень добробуту, житлові умови, культурний рівень кандидата тощо.

Доречним є також психологічне тестування, яке дозволяє виявити необхідні для працівника, задіяного у сфері інформаційної безпеки, особисті якості, а також з'ясувати наявність у кандидата небажаних для такої роботи рис (Таблиця 2.1).

Таблиця 2.1

Бажані та небажані особисті якості персоналу у сфері інформаційної безпеки

Бажані особисті якості	**Небажані особисті якості**
Чесність, порядність, принциповість	Емоційні розлади
Відповідальність, організованість	Неврівноважена поведінка, нерозсудливість
Дисциплінованість, старанність,	Відчуженість від колег по роботі
Емоційна стійкість	Розчарування в собі і своїх здібностях
Адекватна самооцінка своїх можливостей і здібностей	Ображене самолюбство, невдоволення службовим становищем
Самоконтроль вчинків	Нечесність, схильність до обману
Помірна схильність до ризику	Надмірний егоїзм
Прагнення до успіху і порядку в роботі	Фінансова безвідповідальність, бажання легкої наживи
Тренована увага, хороша пам'ять	Балакучість, надмірна довірливість
Здатність зберігати таємницю незалежно від стану чи обставин	Алкогольна чи наркотична залежність

Крім традиційних кроків для більш повного ознайомлення з особистістю кандидата можна також звернутися за інформацією до органів внутрішніх справ: довідатися про наявність (відсутність) судимості кандидата й про осіб, що перебувають у розшуку.

Можливою є перевірка потенційного кандидата на зайняття посади, пов'язаної з конфіденційною інформацією, на поліграфі, адже застосування поліграфа в Україні не є забороненим. Хоча проведення такого тестування пов'язано з певними складнощами. Керівники багатьох організацій вважають застосування поліграфа цілком виправданим і корисним [16].

Після прийняття рішення про призначення особи на посаду, пов'язану з конфіденційною інформацією, з претендентом підписують угоду про нерозголошення таємниці підприємства, зокрема, доступних йому конфіденційних відомостей.

Перед зарахуванням до штату з працівником проводять інструктаж, під час якого обговорюють такі питання:

– вимоги політики компанії щодо поводження та захисту конфіденційної інформації;

– положення угоди про конфіденційну інформацію з акцентом на наслідки їх порушення;

– гарантії щодо прав третіх осіб;

– можливі обмеження в обов'язках на новому місці роботи (розбір системи підпорядкованості; ознайомлення з перспективами службового зростання [27].

Підготовка співробітника до виконання обов'язків за новою посадою здійснюється за планом, який затверджується керівником структурного підрозділу, до якого призначений даний співробітник.

Таким чином, процес відбору персоналу забезпечує оцінку й виявлення претендентів, які не відповідають вимогам підприємства, можуть стати потенційними порушниками, не готові взяти на себе зобов'язання щодо захисту інформації та змиритися з обмеженнями, які накладає робота з конфіденційною інформацією.

Особливе місце у роботи з персоналом у сфері інформаційної безпеки займає звільнення працівників, допущених до конфіденційної інформації (або переведення на посади, не пов'язані з конфіденційною інформацією). Після прийняття керівництвом підприємства рішення про звільнення співробітника, допущеного до конфіденційної інформації, або про переведення його на посаду, не пов'язану з доступом до конфіденційної інформації, служба безпеки та кадровий підрозділ проводять низку заходів, спрямованих на запобігання можливому розголошенню звільненим (переведеним) співробітником конфіденційної інформації про діяльність підприємства [39].

Основою проведення цих заходів є прийняття від працівника, що звільняється, письмових зобов'язань про нерозголошення конфіденційних відомостей, доступних йому у період роботи на підприємстві (на конкретній посаді).

Ці зобов'язання оформлюють у вигляді розписки, яка зберігається на підприємстві. Структура зазначеного документа передбачає зазначенням таких відомостей: прізвище, ім'я, по батькові співробітника та найменування останньої займаної посади; перелік відомостей конфіденційного характеру, заборонених до розголошення протягом певного терміну, або посилання на пункти переліку відомостей, віднесених до комерційної таємниці. Працівник підтверджує згоду з умовами нерозголошення перерахованих в розписці відомостей своїм підписом із зазначенням дати. Оформлення розписки здійснює представник служби безпеки або режимно-секретного підрозділу під час бесіди з особою, яка звільняється.

Після оформлення розписки проводиться інструктаж звільненого співробітника про правила його поведінки після звільнення (переведення на іншу роботу) і недопущення згадки конфіденційних відомостей в ході спілкування з представниками інших підприємств та організацій. Особливу увагу в ході інструктажу приділяється необхідності збереження в таємниці конфіденційної інформації при спілкуванні з іноземними громадянами (при взаємодії в процесі майбутньої роботи з іноземними організаціями).

Перед остаточним звільненням (переведенням на роботу, не пов’язану з конфіденційною інформацією) співробітник зобов’язаний повернути в службу безпеки (або режимно-секретний підрозділ) отримані раніше носії конфіденційної інформації, печатки, ключі від сейфів і сховищ тощо. Факт повернення підтверджується підписами відповідальних посадових осіб в обхідному листі особи, що звільняється.

Після заповнення обхідного листа співробітникові видається оформлена трудова книжка та інші документи про звільнення. Провівши повний розрахунок з підприємством, звільнена особа повертає в бюро перепусток (на контрольно-пропускний пункт) пропуск для проходу на територію і об’єкти підприємства [27].

Загалом процес звільнення працівника, що мав доступ до конфіденційної інформації, можна подати у вигляді схеми (Рис. 2.4.).

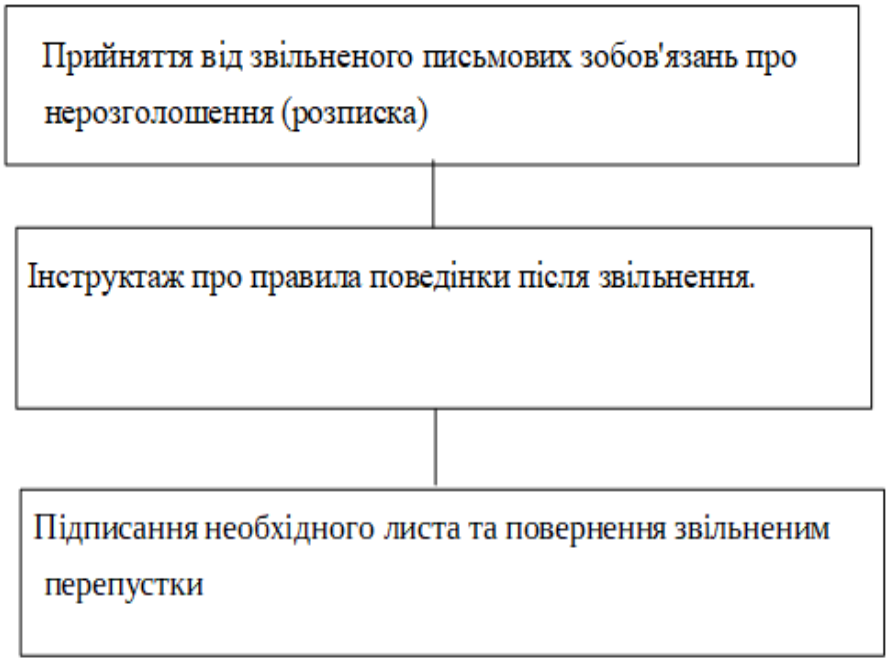

Рис. 2.4. Етапи процесу звільнення персоналу у сфері інформаційної безпеки.

На думку фахівців, через три місяці після звільнення доцільно направити колишньому співробітнику лист-нагадування про необхідність збереження таємниці підприємства. У випадку виявлення фактів несанкціонованого використання колишнім працівником конфіденційних відомостей,

підприємство може звернутися до суду з метою розгляду виявлених фактів і встановлення відповідальності за розголошення інформації обмеженого доступу підприємства.

Дотримання зазначених вище вимог до процедури звільнення персоналу, пов'язаного конфіденційною інформацією, сприятиме не тільки підвищенню відповідальності діючих працівників підприємства за збереження довірених відомостей, а й запобігатиме випадкам викрадення особами, що звільняються, цінної корпоративної інформації, буде обмежено можливості несанкціонованого її використання компаніями-конкурентами.

2.3. Контроль та оцінювання праці персоналу у сфері інформаційної безпеки

Метод контролю у роботі з персоналом підприємства спрямований на оцінку фахової діяльності кожного співробітника щодо забезпечення захисту конфіденційної інформації, використання сукупності корпоративних сил і засобів. Заходи контролю бувають періодичними (плановими) і раптовими. Їх проводять працівники штатних підрозділів підприємства, які вирішують завдання з організації захисту інформації та інформаційної безпеки [27].

Основними формами контролю якості роботи й підвищення професіоналізму співробітників у сфері захисту конфіденційної інформації є:

- перевірки дотримання співробітниками вимог нормативно-методичних документів із захисту інформації, які проводять керівники підприємства або служба безпеки (режимно-секретний підрозділ);

- звіти та доповіді про результати роботи підлеглих співробітників, які готують керівники структурних підрозділів;

- періодична атестація співробітників, допущених до конфіденційної інформації;

- самоконтроль персоналу у сфері захисту конфіденційної інформації (Рис.2.5.).

Рис. 2.5. Форми контролю й оцінювання праці персоналу, задіяного у сфері інформаційної безпеки.

У нинішніх умовах якість праці стає однією з найважливіших категорій, яка впливає на стійкість і ефективність функціонування підприємства. Адже завдяки якості праці, її операційному наповненню можна добитися підвищення продуктивності праці без додаткових часових і матеріальних витрат [25].

З якістю праці тісно пов’язана категорія продуктивності праці, під якою мають на увазі кількісну характеристика роботи, яку виконує персонал. Тобто, підвищення продуктивності праці, за незмінної або покращеної якості, говорить про підвищення ефективності праці. Одним із чинником зростання ефективності праці є атестація працівників. Крім того, атестація персоналу відіграє важливу роль у забезпеченні інформаційної безпеки, зокрема й у контексті протидії внутрішнім загрозам.

Атестаційне оцінювання персоналу є основою для прийняття управлінських рішень щодо внутрішніх переміщень, зарахування в резерв на вищу посаду, підготовки та підвищення кваліфікації, контролю, матеріального та морального заохочення, застосування покарань, звільнення, вдосконалення організації, прийомів і методів управлінської праці, оптимізації структури чисельності апарату. Під оцінюванням розуміють діяльність уповноважених посадовців (представників адміністрації, колективу, кадрових служб, спеціалізованих зовнішніх організацій) щодо визначення ступеня придатності особи до виконання покладених на неї функцій, рівня досягнутих успіхів, наявності необхідних для роботи якостей.

Атестація (атестаційне оцінювання) персоналу – це постійні або періодичні формалізовані заходи, під час яких оцінюють працівника, його діяльність та її результати. Атестаційна оцінка узагальнює результати роботи конкретного працівника за певний період шляхом зіставлення зі стандартом роботи.

Система атестаційного оцінювання персоналу включає три групи даних:

- об’єкти оцінювання (результати, поведінка, успіхи);
- процедури оцінювання;
- методи оцінювання.

Процедури та методи оцінювання персоналу, які розробляють кадрові служби, дозволяють вирішити проблему вибору істотних і другорядних професійних якостей та меж їх прийнятності. При розробці нормативних методичних матеріалів та обробці інформації щодо оцінювання праці персоналу суттєвим моментом є використання загальних принципів управління персоналом.

На підставі атестаційної оцінки вирішують такі кадрові завдання як оцінювання потенціалу для просування по службі і зниження ризику росту малокомпетентних працівників; зниження витрат на навчання; підтримання в персоналу почуття справедливості й підвищення трудової мотивації; організація зворотного зв’язку з працівниками (інформування їх про якість їхньої роботи); розробка кадрових програм навчання і розвитку персоналу.

Для організації ефективної системи оцінювання продуктивності та якості праці необхідно:

- встановити стандарти результативності праці для кожного робочого місця або посади та критерії її оцінювання;
- виробити політику проведення оцінювання результативності праці (коли, як часто і кому проводити оцінювання);
- зобов’язати відповідальних осіб здійснювати оцінювання результативності праці на основі зібраних даних про результативність праці;
- обговорювати атестаційну оцінку з працівником;

- приймати формалізоване рішення щодо ефективності праці особи і задокументувати оцінку.

Алгоритм оцінювання, зокрема, передбачає: виявлення успіхів і проблем працівника; визначення сильних і слабких сторін, якостей (знань, навичок, здібностей, типу поведінки) фахівця, які впливають на виконання ним службових обов'язків, і ступеня їх відповідності вимогам посади чи робочого місця; надання рекомендацій для подолання наявних проблем, способів заохочення (покарання), бажаних посадових переміщень, підвищення кваліфікації і професійного розвитку.

Основними принципами оцінювання персоналу вважають принципи об'єктивності, справедливості, ясності, науковості, систематичності і всебічності. Важливим при атестації дотримуватися таких вимог як об'єктивність (незалежність від приватної думки); надійність (незалежність від впливу ситуації і суб'єктивних факторів), справедливість підходу, відсутність зовнішнього тиску; достовірність результату; орієнтованість на перспективу; комплексність; доступність інформації про критерії і результати; врахування особливостей проведеної кадрової політики [25].

Говорячи про роль позитивної оцінки для працівника, варто відзначити, що схвальне оцінювання з боку керівництва та колег означає для працівника ознакою його соціальної значущості, а з боку споживачів (клієнтів) говорить про результативність діяльності. Загальна позитивна оцінка персоналу сприяє результативності їх праці. Водночас, вона не дає поштовху до вдосконалення виконавця.

Загальна негативна оцінка породжує в працівника невпевненість у собі. Орієнтація на негативну оцінку може припускати відмову від оцінювання при позитивних результатах – в цьому випадку активність суб'єкта падає; замовчування переваг і акцентування на недоліках, що часто викликає протест або навіть провокує озлоблення (у разі системних оцінок); негативне ставлення до будь-якого результату, що веде до втрати ініціативи і бажання контактувати з керівником, байдужості до своїх обов'язків.

Тому більш доречною є оцінка конкретних дій, де якісна орієнтація може бути переважно позитивною (оцінюються лише найбільш яскраві позитивні риси чи досягнення, і підходить для оцінки працівників, діяльність яких дійсно позитивна), або переважно негативною.

Одна з цілей атестації персоналу – виявлення серед персоналу підприємства осіб у стані внутрішніх конфліктів, оскільки у процесі професійного розвитку у працівника періодично може виникати внутрішній конфлікт щодо відповідності його самооцінки й соціальної ролі.

Кожне із завдань атестації безпосередньо пов’язане з процесом забезпечення корпоративної безпеки.

Працівники, які в результаті атестації були оцінені як такі, що повністю відповідають займаній посаді, проходять планові навчальні заняття і тренування. Якщо фахівець показав нижчий від необхідного рівень знань, умінь і навичок, ризик виникнення внутрішніх загроз інформаційній безпеці підприємства можна істотно, залучивши його до участі в корпоративному або зовнішньому навчанні, чи перерозподіливши обов’язки з метою зниження його навантаження.

Особи, віднесені до групи неповної відповідності посаді, мають пройти додатковий цикл навчальних занять у залежності від того, якого компонента в їх досвіді (знань, умінь, навичок) бракує.

Найбільшу небезпеку безпеці підприємства становлять працівники, рівень розвитку професійних навичок яких перевищує необхідний для посади. Надмірний професійний досвід породжує самовпевненість, зниження пильності, внаслідок чого зменшується надійність співробітника.

Надкваліфікований співробітник може не виконувати належним чином свою роботу під впливом демотивуючих факторів: жорсткої субординації, обмежених можливостей самореалізації, низького соціального статусу тощо. Тому таких осіб варто внести до резерву на висування або перевести на ділянку з ширшим колом завдань.

Умовою гармонійного функціонування персоналу є збалансована взаємодія процесів особистісного розвитку, кар'єрного просування і напрацювання соціального авторитету. Особистісний розвиток передбачає професійне зростання через примноження знань і навичок, підвищення авторитету в колективі, покращення добробуту. Кар'єрне просування супроводжується, наприклад, рухом за посадовими позиціями, статусним рангом, рівнем матеріальної винагороди. У випадку розбіжності цих процесів розвивається внутрішній конфлікт, ознаками якого є зниження інтересу до роботи, підвищення тривожності й конфліктності. Усі зазначені чинники негативно впливають на виконання службових обов'язків і призводять до зниження надійності всієї системи [18].

Атестація співробітників служби безпеки є обов'язковою, оскільки її мета полягає в оцінюванні поточного стану сил і засобів, а також пошуку ресурсів для підвищення надійності системи. При проведенні атестації фахівців служби безпеки необхідно використовувати засоби психологічного тестування, що дасть можливість виявити осіб підвищеного ризику. Ситуативними ознаками, за якими співробітники можуть бути віднесені до групи ризику, є тривожність, депресивні прояви або інші психологічні характеристики, що знижують їх надійність. Робота в сфері інформаційної безпеки пов'язана з підвищеними психоемоційними навантаженнями, що може призвести до негативних особистісних змін.

З метою виявлення випадків, пов'язаних з професійним «вигоранням», у процесі атестації варто звертати особливу увагу на несприятливі індивідуально-психологічні особливості фахівців: риси слабкого типу вищої нервової діяльності; сугестивність і схильність до самонавіювання; конфліктність; наявність невротичних станів; егоцентрична спрямованість особистісних інтересів; емоційна нестійкість та надмірна вразливість; нестабільність інтересів; некритичне ставлення до себе і своїх вчинків тощо.

При оцінюванні інтелектуальних здібностей та ділових якостей фахівця з інформаційної безпеки несприятливими показниками є такі:

- відсутність системності у викладі матеріалу з обговорюваної проблеми;
- поверхневі судження, неадекватний аналіз чинників проблеми;
- необґрунтовані, логічно не пов’язані уточнення;
- виражена примітивність або абсурдність висновків;
- суперечливість, подвійність міркувань;
- необґрунтовано категоричні міркування, класифікація та узагальнення;
- нерозуміння деяких проблем професійного значення;
- гарячковість, порушення такту і поведінкових норм, сумнівні та недоречні жарти тощо [27].

У ході атестації хороший результат дає підхід, коли фахівець з інформаційної безпеки, який атестується, кілька робочих змін працює спільно з інструктором або керівником, який не тільки визначає рівень професійної підготовки атестованого, але й навчає його за потреби.

Висновки до другого розділу

З’ясовано, що внутрішніми загрозами інформаційній безпеці підприємства, тобто загрозами з вини персоналу є дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків, втрата інформаційних ресурсів, підрив ділового іміджу підприємства, виникнення проблем у відносинах з реальними чи потенційними партнерами тощо.

Внутрішні загрози об’єктам інформаційної безпеки підприємства за способом впливу можуть бути об’єднані в п’ять груп: власне інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні. Джерела загроз інформаційній безпеці підприємства з вини персоналу умовно можна поділити на навмисні та ненавмисні.

Оскільки персонал підприємства створює найбільше загроз інформаційній безпеці, з метою їх протидії доцільно, насамперед, проводити відбір

потенційних кандидатів на посади, що одержує доступ до конфіденційної інформації, за спеціальною процедурою, яка включає різні форми і методи оцінювання кандидатів при прийомі; документування добровільної згоди особи не розголошувати конфіденційні відомості та дотримуватися вимог інформаційної безпеки; інструктування і навчання працівників практичним діям із захисту інформації.

Контроль якості праці персоналу та її оцінювання, який є одним із засобів запобігання порушенням інформаційної безпеки з боку персоналу, має на меті оцінити ефективність роботи кожного працівника щодо забезпечення інформаційної безпеки, використання сукупності сил і засобів підприємства у цій сфері. Основними формами контролю якості роботи персоналу у сфері захисту інформації є: перевірки дотримання співробітниками положень нормативно-методичних документів з інформаційної безпеки; звіти та доповіді керівників структурних підрозділів про результати роботи підлеглих; періодична атестація співробітників, допущених до конфіденційної інформації; самоконтроль персоналу.

РОЗДІЛ 3
ТЕХНІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ У ПРОТИДІЇ ЗАГРОЗАМ З ВИНИ ПЕРСОНАЛУ

На сьогоднішній день існує великий арсенал технічних засобів забезпечення безпеки інформаційних ресурсів та інфраструктури, серед яких:

– засоби ідентифікації й автентифікації користувачів;

– ПЗ для шифрування інформації, що обробляється в ІТКС;

– віртуальні приватні мережі;

– інструменти контентної фільтрації;

– міжмережеві екрани;

– засоби перевірки цілісності вмісту дисків;

– засоби антивірусного захисту;

– системи виявлення вразливостей мереж і аналізатори мережевих атак та інші.

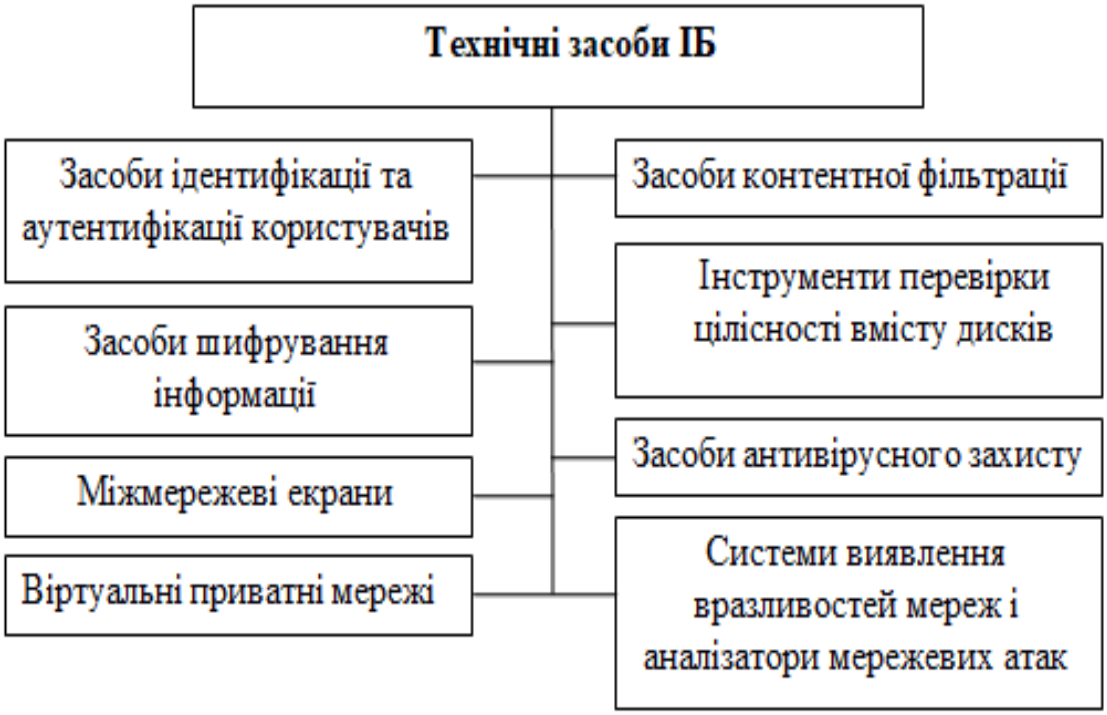

Рис 3.1. Технічні засоби забезпечення інформаційної безпеки.

3.1. Ідентифікація та автентифікація користувачів

Ідентифікацію і автентифікацію вважають основою технічного захисту інформаційних активів, оскільки інші сервіси діють у ході обслуговування авторизованих суб'єктів. Ідентифікація та автентифікація є взаємопов'язаними процедурами і першою «лінією оборони» інформаційного простору підприємства.

Саме ідентифікація і автентифікація відіграють особливо важливу роль у протидії внутрішнім загрозам інформаційної безпеки. Згідно з даними огляду комп'ютерної злочинності CSI/FBI на другому і третьому місцях за розміром збитку підприємств у США знаходяться неавторизований доступ до даних і крадіжка конфіденційних даних. Щоб знизити подібні втрати, необхідно приділяти більше уваги вирішенню завдань автентифікації і управління доступом користувачів [35].

Ідентифікація – це процедура розпізнавання суб'єкта за його унікальним ідентифікатором, наданим йому раніше і занесеним у базу даних в момент реєстрації суб'єкта як легального користувача системи. У процесі ідентифікації суб'єкт (користувач або процес, який діє від імені користувача, чи іншого програмно-апаратного елемента) називає себе (повідомляє своє ім'я).

Автентифікація - процедура перевірки автентичності суб'єкта, який пред'явив свій ідентифікатор, входячи в систему. У більшості випадків вона становить процедуру обміну між користувачем, який входить у систему, і ресурсом, який схвалює чи відмовляє в доступі. За допомогою автентифікації інша сторона бачить і може переконатися, що вказаний суб'єкт дійсно той, за кого він себе видає. [33].

Прикладом автентифікації може бути порівняння пароля, введеного користувачем, з паролем, який збережений в базі даних сервера. Таким чином, ідентифікація і автентифікація є взаємопов'язаними процесами розпізнавання і перевірки автентичності користувачів.

Автентифікація може бути односторонньою (коли клієнт доводить свою справжність серверу) і двосторонньою. Прикладом односторонньої автентифікації є процедура входу користувача в систему.

У мережевому середовищі, де користувач і сервер можуть знаходитися віддалено, ідентифікація й автентифікація мають два основні аспекти: вони використовуються для підтвердження автентичності суб'єкта і забезпечують організований і захищений обмін даними щодо повідомлення та підтвердження автентичності користувача.

У контексті забезпечення безпеки інформації часто використовують багатофакторну автентифікацію, яка передбачає надання більш ніж одного «доказу» способу автентифікації для доступу до даних. Так, користувач може підтвердити автентичність, пред'явивши один або кілька з таких елементів:

- відомості, які він знає (пароль, пін-код, особистий ідентифікаційний номер, криптографічний ключ тощо);
- речі, якими він володіє (особисту картку, флеш-пам'ять, електронний пропуск, магнітну банківську картку, токен тощо);
- ознаки, які належать (притаманні і невід'ємні) тільки йому, наприклад біометричні характеристики або персональні відмінності: голос, відбитки пальців, малюнок сітківки ока, форма обличчя [33].

Одним із різновидів багатофакторної автентифікації є двофакторна або двоетапна. Такий спосіб включає перевірку даних користувача на підставі двох відмінних один від одного компонентів.

Прикладом двофакторної автентифікації є сервіси від Google і Microsoft, в яких авторизуючись з нового пристрою, користувач крім логіна і пароля, має також ввести код з шести або восьми знаків. Код можна отримати тільки одним із зазначених способів: SMS-повідомлення на мобільний телефон; голосовий виклик на телефон; реєстр одноразових кодів; програма-автентифікатор для мобільного або ПК.

Подвійна автентифікація має низку важливих переваг, зокрема зручність (смартфон завжди під рукою) і безпеку (постійна зміна коду підтвердження).

Водночас, цей метод також має певні недоліки: код підтвердження, а саме смс-повідомлення, який передається в бездротовій локальній мережі, може бути перехоплений зловмисниками; можливою є певна затримка при отриманні SMS, яка пов'язана з процедурою перевірки автентичності. Тим не менше, двофакторна автентифікація сьогодні широко використовується багатьма відомими сервісами, такими як Facebook, Web Money, Yandex, Microsoft, Google та іншими.

Загалом в ході ідентифікації й автентифікації у відкритому мережевому середовищі дані, передані суб'єктом, можуть не збігатися з даними, отриманими і використаними для перевірки автентичності. Важливим є забезпечення захисту від пасивного й активного прослуховування (несанкціонованих перехоплення, зміни або відтворення даних). Для цього не підходить передача паролів у відкритому вигляді, шифрування паролів також не забезпечує захист від недозволеного відтворення. Отже, є необхідність у більш складних протоколах автентифікації.

Перешкодами для надійної ідентифікації є не тільки мережеві загрози, але й інші, зокрема майже всі автентифікаційні сутності можна дізнатися, вкрасти або підробити. Крім того, наявні протиріччя між надійністю автентифікації і зручностями користувача і системного адміністратора. Для підвищення рівня безпеки бажаним було б, щоб користувач з певним інтервалом повторно вводив автентифікаційні дані (оскільки упродовж довгого проміжку часу його могла змінити інша людина), а це підвищує ймовірність загроза, що хтось підгляне за введенням даних, та й користувачеві не дуже зручно переривати основну діяльність в системі. І, нарешті, засоби високого рівня захисту коштують не дешево і навпаки. Отже, все упирається в ресурси, які завжди обмежені [37].

Сучасні засоби ідентифікації й автентифікації мають забезпечувати єдиний вхід у систему. Це, в першу чергу, зручно для користувача. За умови, що в мережі багато інформаційних сервісів, скористатися якими можна

незалежно один від одного, то багаторазова процедура ідентифікації та автентифікації стає занадто обтяжливою.

Отже, виникає необхідність шукати компроміс між доступністю, надійністю і вартістю послуги, а також зручністю використання й адміністрування засобів ідентифікації й автентифікації.

Варто відзначити, що сервіс ідентифікації й автентифікації цілком може стати об'єктом атак на доступність. Так, зловмисник може зупинити роботу авторизованого користувача в системі, якщо остання налаштована таким чином, що після певної кількості невдалих спроб пристрій введення ідентифікаційної інформації, наприклад, термінал, блокується. Якщо в мережі не зберігаються конфіденційні дані, то для доступу до ресурсів цілком достатньо введення логіна і пароля. Управління такими системами зазвичай не представляє складнощів.

Оцінюючи тенденції останніх років, варто відзначити, що засоби електронної ідентифікації інтенсивно розвиваються і спрямовані на зменшення участі людини у зборі інформації. Це викликано тим, що оператор може помилитися, вводячи дані, наприклад, з використанням клавіатури комп'ютера. Найбільш повно вимогам комп'ютерних систем і систем управління відповідають технології автоматичної ідентифікації, де потрібно чітко розпізнавати об'єкти в реальному масштабі часу.

Розглянемо детальніше основні технології автоматичної ідентифікації (Рис. 3.2.), які на практиці часто використовуються у поєднанні.

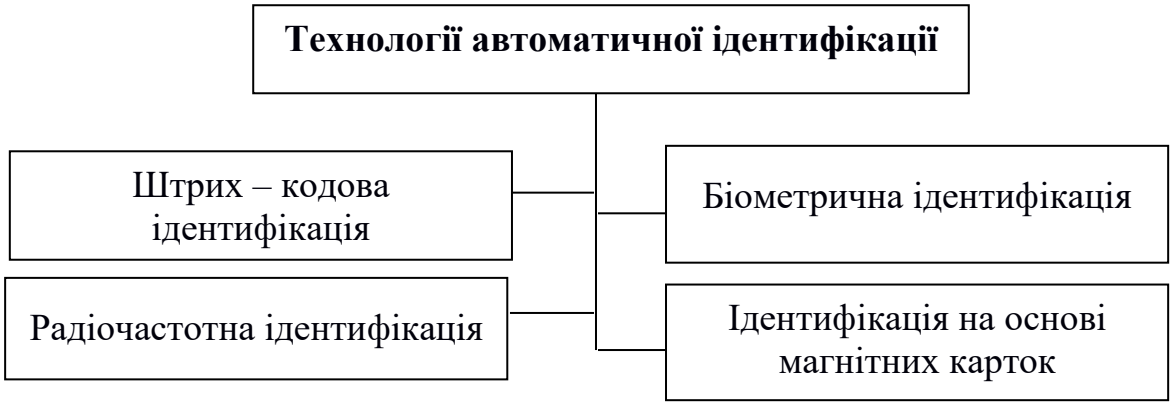

Рис. 3.2. Технології автоматичної ідентифікації.

Штрих - кодова ідентифікація

Штрих-коди використовують переважно для автоматизації руху товару його виробники. Зараз штрих-коди EAN/UPC є в основі всесвітньої багатогалузевої комунікаційної системи, яку розвивають найбільші спеціалізовані міжнародні компанії: EAN International і AIM International.

До переваг штрих-кодової ідентифікації відносять:

– мінімізація паперового документообігу і зменшення числа помилок при введенні інформації;

– пришвидшення процесу обслуговування клієнтів;

– автоматизація основних технологічних процесів руху товарів, починаючи з виробництва і закінчуючи продажами кінцевому покупцю.

Серед основних недоліків штрих-кодової ідентифікації виділяють: відсутність можливості доповнення даних ідентифікаційної мітки, оскільки штрих-код записується тільки один раз у момент його друкування; невеликий обсяг даних (не більше 50 байт); повільне нанесення даних на мітку; представлення даних на мітці у відкритому вигляді, внаслідок чого товари не є захищеними від підробок і крадіжок; недовговічність штрих-кодів внаслідок впливу пилу, вогкості, бруду, механічних пошкоджень [35].

Радіочастотна ідентифікація

Штрих-кодова ідентифікація знайшла свій розвиток у засобах радіочастотної ідентифікації (RFID - Radio Frequency Identification Device), розробники якої використали всі переваги попередньої системи і подолали практично всі недоліки і обмеження. RFID дозволяє отримувати інформацію про предмет без прямого контакту. Дистанції, на яких може відбуватися зчитування і запис інформації, можуть становити від декількох міліметрів до декількох метрів (головним чином, від несучої частоти, що знаходиться в межах від 125 кГц до 5,8 ГГц). Більшість смарт-карт, які застосовуються для ідентифікації співробітників корпорацій, належать до продукції виробництва Ангстрем, HID, Atmel, Mifare, EM Microelectronic Marin, Microchip та інших компаній. Найчастіше використовують несучі частоти 125 кГц або 13,56 МГц.

Біометрична ідентифікація

Зазначена технологія заснована на застосуванні статистичного аналізу біологічних спостережень і явищ. Біометрична характеристика - це вимірна фізіологічна або поведінкова риса людини.

Як зазначалося вище, біометричні характеристики людини поділяють на дві групи:

– фізіологічні біометричні характеристики (так звані статичні) - дані, отримані шляхом вимірювання анатомічних даних людини (відбитки пальців, форма обличчя, кисті, структура сітківки ока тощо) та

– поведінкові біометричні характеристики (так звані динамічні) - біометричні дані, отримані шляхом вимірювання дій людини. Типовою рисою для поведінкових характеристик є їх протяжність, наприклад голос, підпис.

Біометричні системи є різноманітними у відповідності до об'єктів і способів вимірювань. Особа за допомогою фіксуючого пристрою (наприклад, сканера або камери) надає системі зразок - впізнаване, необроблене зображення або запис фізіологічної або поведінкової якості. Біометричний зразок технологічно обробляється, внаслідок чого виходить ЗІП (еталонний ідентифікатор користувача або зразок для перевірки). ЗІП є послідовністю чисел. При цьому сам зразок неможливо відновити з використанням еталона. Знята в процесі ідентифікації характеристика порівнюється з електронними вимірювальними пристроями. Оскільки дані, отримані під час спроби доступу і надані електронними вимірювальними пристроями, повністю ніколи не співпадають, то для отримання дозволу ступінь збігу має перевищувати встановлене порогове значення. При цьому біометричним системам притаманний певний відсоток помилкових відмов і підтверджень.

Ідентифікація з використанням магнітних карток

Карти з магнітною стрічкою вже понад двадцять років використовують в системах контролю фізичного доступу. З метою збереження інформації від випадкового розмагнічування магнітні стрічки роблять з матеріалів, що

потребують сильних магнітних полів для запису і знищення інформації. Магнітні картки спрацьовують при проведенні через зчитувач.

Істотною перевагою магнітних карт є їх низька вартість. Водночас, до основних недоліків цієї технології відносять: обмеження за обсягом інформації, яка може бути записана на магнітну стрічку; слабка захищеність від копіювання; чутливість до забруднення, вологи та механічних пошкоджень; відносно короткий термін служби [35].

3.2. Міжмережеві екрани та віртуальні приватні мережі

Міжмережевим екраном називається програмно-апаратний або програмний елемент, який відповідно до встановлених параметрів контролює і, за потреби, фільтрує мережевий трафік. Інші назви зазначеного засобу - файєрвол або брандмауер. Міжмережевий екран призначений для захисту пристроїв локальної мережі від атак ззовні. Він також сприяє запобіганню випадковим або навмисним діям працівників підприємства, які можуть спровокувати зараження окремого комп'ютера або навіть усієї системи.

Мережевий екран використовують для захисту окремих сегментів мережі або хостів від потенційного несанкціонованого проникнення через уразливості програмного забезпечення системи або протоколів мережі. Робота брандмауера полягає в порівнянні характеристик трафіку, що проходить крізь нього, з шаблонами вже відомого шкідливого коду [41].

Міжмережеві екрани володіють набором стандартних можливостей, зокрема:

– фільтрують трафік, блокують процеси, які намагаються отримати доступ до системних або незахищених служб;

– запобігають спробам несанкціонованого доступу до конфіденційної інформації і блокують нелегітимні спроби її передачі;

– контролюють доступ до мережевих пристроїв і портів;

– фіксують усі мережеві активності і події, ведуть статистику;

– видають повідомлення у випадку виявлення підозрілих активностей або мережевих атак.

Варто відзначити, що міжмережевий екран самостійно не може забезпечити цілковитий захист системи від вірусів. Ефективна робота брандмауера буде забезпечена у комплексі з іншим захисним програмним забезпеченням - антивірусом. Принципи роботи стандартного брандмауера й антивіруса в корені відрізняються: перший запобігає потраплянню вірусів в локальну мережу або на окремий ПК, а інший - знаходить і видаляє вже Незважаючи на те, що сьогодні не існує єдиної і загальновизнаної класифікації міжмережевих екранів, виділяють такі їх класи: фільтруючі маршрутизатори; шлюзи сеансового рівня; шлюзи рівня додатків.

Фактично, лише невелика кількість наявних зараз міжмережевих екранів містять один з перерахованих елементів, решта включають їх як базові компоненти.

Розглянемо характеристики кожного із перелічених видів брандмауерів.

Фільтруючі маршрутизатори – це маршрутизатори або серверні програми, розташовані між мережею, що захищається, та Інтернетом. Вони сконфігуровані таким чином, щоб фільтрувати вхідні і вихідні пакети на основі інформації, що міститься в TCP- і IP-заголовках пакетів (IP-адреси й порти відправника й одержувача).

Фільтруючий міжмережевий екран є найбільш поширеним і простим в реалізації.

Шлюзи сеансового рівня є, по суті, транслятором TCP-з'єднання, який отримує запит авторизованого користувача на конкретні послуги і після перевірки допустимості бажаного сеансу встановлює з'єднання з зовнішнім хостом. Після цього шлюз копіює пакети в обох напрямках, не здійснюючи їх фільтрації.

Шлюзи рівня додатків. Для захисту властивих фільтруючим маршрутизаторам вразливих місць міжмережеві екрани використовують прикладні програми для фільтрації з'єднань з такими сервісами, як Telnet і

FTP. Зазначений додаток називають proxy-сервісом, а хост, на якому спрацює такий сервіс, - шлюзом рівня додатків. Такий шлюз не забезпечує пряму взаємодію між авторизованим клієнтом і зовнішнім хостом, а фільтрує всі вхідні і вихідні пакети на прикладному рівні [20].

Однак, брандмауери не в змозі вирішити всі проблеми безпеки корпоративної мережі. У використанні ці пристрої мають ряд обмежень, а також є загрози безпеки, від яких міжмережеві екрани не можуть захистити. Отже, міжмережеві екрани не захищають від чорних входів (люків) в мережі; недостатньо ефективні у захисті від атак співробітників компанії; мають обмеження в доступі до потрібних сервісів і можуть блокувати ряд сервісів, які застосовують користувачі, наприклад Telnet, FTP тощо, вимагають концентрації різних засобів забезпечення безпеки в одному місці; володіють обмеженою пропускною здатністю.

Для вирішення подібних проблем потрібне проведення добре продуманої політики безпеки, в якій буде дотримуватися баланс між вимогами безпеки і потребами користувачів.

Говорячи про найбільш поширені марки файєрволів, варто скористатися дослідженням відомого аналітичного агентства Gartner, відповідно до якого в категорії Enterprise Firewalls (міжмережеві екрани для підприємства) лідерами є такі виробники як: Palo Alto Networks, Check Point, Fortinet. У категорії переслідувачів провідні позиції займають компанії Cisco і Huawei [40].

Міжмережеві екрани використовуються при організації захищених віртуальних приватних мереж, коли кілька локальних мереж, підключених до глобальної, об'єднуються в одну захищену віртуальну приватну мережу.

Отже, віртуальна приватна мережа (Virtual Private Network, VPN) створюється на базі мережі Інтернет. На відміну від зв’язку через Інтернет, де є велика вірогідність порушень захисту та конфіденційності, VPN можуть гарантувати, що отриманий через Інтернет трафік захищений настільки ж добре, як і трафік всередині локальної мережі. Крім того, віртуальні мережі забезпечують значну економію витрат [41].

VPN – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Забезпечення захисту передавання пакетів через загальнодоступні мережі реалізується у VPN через використання засобів шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати кілька територіально віддалених мереж в єдину мережу підприємства з використанням непідконтрольних каналів для зв'язку між ними.

Віртуальні канали зв'язку, які створюються через загальнодоступні мережі в рамках технології VPN, називають VPN-тунелями. Оскільки трафік, що проходить через тунелі і з'єднує віддалені філії, шифрується, зловмисник, навіть перехопивши інформацію, не може її переглянути.

Найчастіше для створення VPN використовують інкапсуляцію протоколу PPP в будь-який інший протокол – IP (такий спосіб використовує реалізація PPTP – Point-to-Point Tunneling Protocol) або Ethernet (PPPoE). Останнім часом технології VPN використовують не тільки для створення власне приватних мереж, але і для надання виходу в Інтернет з «внутрішньої» (підконтрольної) мережі, яких може бути кілька, і «зовнішньої» мережі (зазвичай це Інтернет), якою проходить інкапсульоване з'єднання. Підключення окремого комп'ютера до віртуальної мережі також є можливим.

Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, підключеного одночасно до внутрішньої і зовнішньої мережі. Підключаючи віддаленого користувача (або встановлюючи з'єднання з іншою захищеною мережею), сервер доступу вимагає проходження процесу ідентифікації й автентифікації. Після підтвердження справжності віддалені користувач або локальна мережа отримують повноваження для роботи в мережі, тобто відбувається авторизація.

VPN-рішення класифікують за такими основними параметрами: типом середовища, що використовується, і способом реалізації рішення (Рис.3.3.).

Рис. 3.3. Класифікація VPN.

За типом використовуваного середовища VPN поділяють на захищені і довірчі.

Захищені VPN є найбільш поширеним варіантом віртуальних приватних мереж, за допомогою яких створюють надійну і захищену підмережу на основі неконтрольованої мережі, переважно Інтернету. Прикладом захищених VPN є: IPSec, OpenVPN і PPTP [47].

Довірчі VPN використовують у випадках, коли середовище передачі інформації вважають достатньо надійним, а основним завданням є створення віртуальної підмережі в рамках більшої мережі. Тоді питання безпеки стає неактуальним. Прикладами подібних VPN-рішень є: Multi-protocol label switching (MPLS) і L2TP (Layer 2 Tunneling Protocol).

За способом реалізації VPN бувають у вигляді:

– спеціального комплексу програмно-апаратних засобів. Завдяки такій реалізації забезпечується висока продуктивність і достатній ступінь захисту;

– програмного забезпечення з використанням персонального комп’ютера, який забезпечує функціональність VPN.

– інтегрованого рішення, коли функціональність VPN забезпечує комплекс, який виконує також завдання фільтрації зв’язку, організації мережевого екрану і забезпечення якості обслуговування.

Отже, серед переваг VPN як засобу захисту процесів передачі даних, виділяють такі: створення захищених каналів зв’язку за ціною доступу в Інтернет, що в рази дешевше виділених ліній; відсутність потреби при установці VPN змінювати топологію мереж, переписувати програми, навчати користувачів, що призводить до значної економії; незалежність від криптографії і можливість застосовувати криптографічні модулі різних виробників згідно з діючими в країні стандартами; наявність відкритих інтерфейсів, які дозволяють інтегрувати окрему мережу з іншими програмними продуктами та бізнес-додатками.

До недоліків VPN відносять, насамперед, порівняно низьку надійність [45].

У порівнянні з виділеними лініями та мережами на основі Frame relay віртуальні приватні мережі менш надійні, проте в 5-10, а іноді і в 20 разів дешевше [34] Тому, на думку аналітиків, це не зупинить VPN, оскільки це не суттєво для більшості користувачів.

Особливо ця теза є актуальною в умовах наявності багатьох варіантів безкоштовних VPN. В Україні найкращими варіантами таких сервісів є NordVPN, Hotspot Shield, Windscribe, hide.me, Proton, Opera, TunnelBear. Кожна з представлених VPN має свою специфіку і може бути ідеальним засобом для перегляду потокового контенту, завантаження торрентів, використання під час подорожі тощо [23].

3.3. Засоби захисту від комп’ютерних вірусів та їх особливості

Комп’ютерні віруси є одними з найбільш поширених загроз інформаційним та телекомунікаційним системам. Часто власне персонал підприємства стає джерелом зараження корпоративних інформаційних ресурсів та інфраструктури внаслідок своєї некомпетентності або халатності.

Найбільш поширеними заходами запобігання інфікуванню шкідливим програмним забезпеченням є такі:

- використання надійних джерел програмного забезпечення;
- обмеження доступу до комп'ютера сторонніх осіб;
- встановлення захисту від запису на змінних дисках з файлами, у тому числі, за рахунок системного адміністрування;
- регулярне створення резервних копій;
- перевірка інформації, що надходить ззовні, і поточного стану ПК за допомогою антивірусних програм.

Антивірусне програмне забезпечення

Для захисту від різноманітних вірусів існує декілька видів антивірусних програм, які за призначенням поділяють на детектори, фаги, ревізори, фільтри та вакцини. Схема видів антивірусів подано на Рис. 3.4.

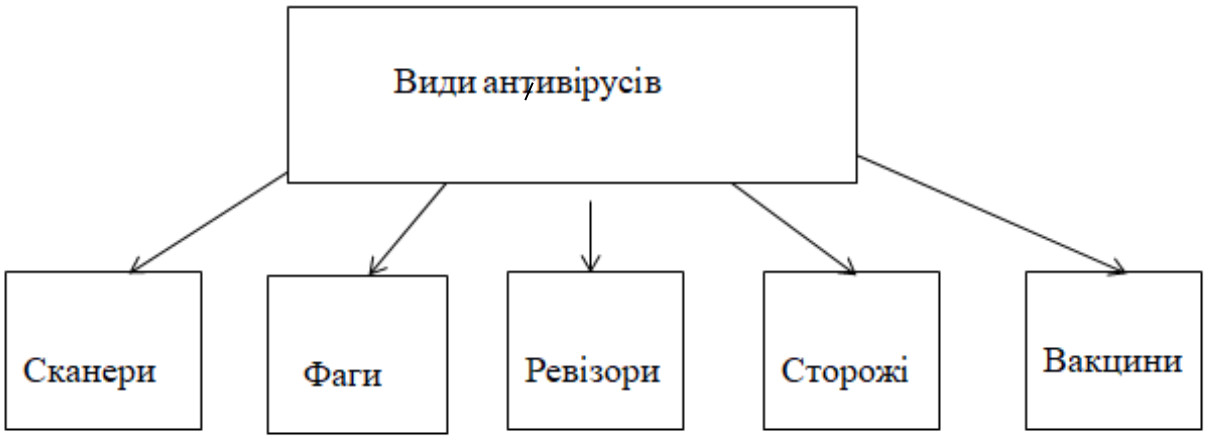

Рис. 3.4. Види антивірусів.

Розглянемо їх характеристики більш докладно.

Детектори (сканери) – програмне забезпечення, завданням якого є перевірка на наявність вірусу оперативної або зовнішньої пам'яті за допомогою розрахованої контрольної суми або сигнатури і складення списку пошкоджених програм. Резидентний детектор вірусів перевіряє програму, і вона активується тільки за умови відсутності вірусів.

Недоліком таких антивірусних програм є те, що вони можуть знаходити тільки відомі розробникам віруси. Прикладом такого детектора є, наприклад, програма MS AntiVirus.

Фаги або програми-лікарі не тільки виявляють, але і знешкоджують вірус (фаг) або кілька вірусів. Програми-доктори, призначені для пошуку і знищення великої кількості вірусів, називають поліфагами. Сучасні версії поліфагів, як правило, можуть досліджувати файл на наявність коду, характерного для вірусу (додання частини однієї програми в іншу, шифрування коду тощо). Фагами є, наприклад, програми Aidstest, DrWeb.

Дуже часто функції детектора і фага поєднані в одній програмі, а вибір режиму роботи здійснюється через встановлення певних параметрів. На зорі вірусної ери кожен новий вірус визначався та лікувався окремою програмою, а для лікування від деяких таких вірусів було створено не менше десятка антивірусних програм. Згодом були розроблені програми, які могли виявляти й лікувати декілька типів вірусів, тому їх стали називати відповідно полідетекторами та поліфагами.

Сучасні антивірусні програми знаходять і знешкоджують тисячі різновидів вірусів. Найбільш популярними детекторами й фагами є програми Aidstest, DrWeb (фірма «ДиалогНаука», Росія), Scan, Clean (фірма McAfee Associates, США), Norton AntiVirus (фірма Symantec Corporation, США).

З огляду на те, що постійно з'являються нові віруси, програми-детектори і програми-фаги швидко застарівають, і потребують регулярного оновлення. Тільки постійне оновлення таких програм дозволяє користувачу боротися з новими вірусами.

Ревізори – програми, що контролюють можливі засоби зараження комп’ютера. Саме такі програми відносять до найнадійніших засобів захисту від вірусів, оскільки вони можуть виявити вірус, невідомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT-таблиці, атрибути файлів. Ревізори запам'ятовують вихідний (неінфікований) стан програм, каталогів і системних областей диска, а потім періодично або за бажанням користувача

порівнюють поточний стан з вихідним. У ході порівнянні ревізори перевіряють довжину файла, код циклічного контролю (контрольна сума файла), дату й час модифікації, інші параметри. Нескладний аналіз встановлених змін дозволяє надійно визначити факт зараження комп’ютера вірусами.

Програми-ревізори мають достатньо розвинені алгоритми, виявляють стелс-віруси і можуть навіть відрізнити зміни версії програми від змін, внесених вірусом. До числа програм-ревізорів належить широко поширена в Росії програма Adinf фірми "Діалог-Наука" [30].

Програми-фільтри. На попередньому етапі розвитку антивірусних засобів, коли надійність існуючих антивірусних програм була низькою, широкого поширення набули так звані фільтри. Програми-фільтри – це невеликі резидентні програми, призначені для виявлення підозрілих і характерних для вірусів дій під час роботи комп'ютера. Такими діями можуть бути: спроби модифікації файлів з розширеннями COM і EXE; зміна атрибутів файлів; прямий запис на диск за абсолютною адресою; запис в BOOT-сектори диска; завантаження резидентної програми.

Ці антивірусні програми блокують операцію записування на диск і виконують її тільки з дозволу користувача. При цьому легко встановити ініціатора команди на запис: чи це авторизований користувач, чи вірусна програма. Серед широко відомих програм-фільтрів програми VirBlk, FluShot та інші. Оскільки такі програми забирають багато часу для зайвої комунікації і не завжди виявляють віруси, зараз їх майже не використовують.

Сторожами називають резидентні програми, які постійно зберігаються у пам’яті комп’ютера й у визначений користувачем час перевіряють оперативну пам’ять комп’ютера, файли, BOOT-сектор, FAT-таблицю. Сторожем є, наприклад, програма AVP.

Вакцини або імунізатори - це резидентні програми, що запобігають зараженню файлів. Вакцини використовують для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів. Однак,

вакцинація можлива тільки від відомих вірусів. Вакцина модифікує програму або диск таким чином, щоб це не відбивалося на їх роботі, а вірус буде сприймати їх зараженими і тому не впровадити. У сучасних умовах програми-вакцини використовують в обмежених обсягах [42].

Підсумовуючи, відзначимо, що антивірусні програми, які ефективно захищатимуть інформацію підприємства, мають відповідати низці вимог.

Зокрема антивірусна програма має виконувати такі функції:

Здійснювати оперативну перевірку з метою запобігти інфікування файлів на комп'ютері або зразу виявити інфікований файл, що потрапив на нього, до того як вірус нанесе реальний збиток.

Проводити повну перевірку системи, тобто перевіряти на віруси весь вміст жорсткого диску для виявлення будь-якого інфікованого файлу, який міг «обійти» захист.

Перевіряти електронну пошту, оскільки часто віруси розповсюджуються саме в такий спосіб. Антивірус, перебуваючи між поштовим сервером і програмою електронної пошти на комп'ютері, має перехоплювати будь-які потенційно загрозливі повідомлення, перш ніж вони потраплять у поштову скриньку чи будуть відправлені.

Перевіряти макросценарії, тому що віруси використовують беззахисність макромов типу JavaScript, які використовуються для створення додаткових функцій і інтерактивних елементів для веб-сторінок.

Здійснювати перевірку архівів, адже багато вірусів ховаються, створюючи файл архіву типу .zip.

Контролювати підозрілі процеси, який може вказувати на роботу вірусу. Цю функція антивірусної програми називають евристичним аналізом.

Інтегруватися з Microsoft Office, оскільки через наявність численних вразливостей багато вірусів розповсюджуються через документи Microsoft Office.

Підтримувати миттєві повідомлення, через які також можливе зараження шкідливим програмним кодом. Таким чином можна перешкодити

збереженню або виконанню будь-якого інфікованого файлу, отриманого через миттєве повідомлення.

Виконувати функції завантажувального диску, оскільки деякі з найбільш небезпечних вірусів можуть провокувати відмову в завантаженні операційної системи. Завдяки цій функції антивірус може завантажити заблокований комп’ютер і видалити вірус [44.].

Антивірусні програмно-апаратні засоби

На думку багатьох фахівців, найбільш надійним методом захисту від вірусів є апаратно-програмні антивірусні засоби, зокрема спеціальні контролери та їх програмне забезпечення. Контролер установлюється в роз’єм розширення, отримуючи доступ до загальної шини. Таким чином пристрій контролює всі звернення до дискової системи. У програмному забезпеченні контролера запам'ятовуються області на дисках, зміна яких у звичайних режимах роботи неприйнятна. Так можна встановити захист і запобігти зміні головного завантажувального запису, завантажувальних секторів, виконуваних файлів та файлів конфігурації. При виконанні заборонених дій будь-якою програмою контролер видає відповідне повідомлення користувачеві і блокує роботу інформаційної системи.

Серед переваг апаратно-програмних антивірусних засобів у порівнянні з програмними виділяють: здатність працювати постійно, виявляти всі віруси, незалежно від механізму їх дії, блокувати несанкціоновані дії, які можуть бути ознакою роботи вірусу або некваліфікованого користувача. Водночас основний недолік апаратно-програмних засобів антивірусного захисту – це залежність від апаратних засобів, зміна яких призводить до необхідності заміни контролера. Прикладом апаратно-програмного захисту від вірусів може служити комплекс Sheriff [9].

Резервне копіювання даних

Важливим засобом захисту інформації від деструктивного впливу вірусів є резервне копіювання найцінніших даних. У разі втрати інформації внаслідок зараження шкідливим програмним кодом, жорсткий диск

форматують, готуючи таким чином до нового етапу експлуатації. На «чистий» диск установлюють операційну систему з дистрибутивного компакт-диска, потім решта необхідного програмного забезпечення, яке теж беруть з дистрибутивних носіїв. Відновлення комп’ютера завершують відновленням даних шляхом повернення даних, збережених на резервних носіях [5].

Одним із основних принципів резервного копіювання є принцип зберігання резервних копій окремо від основного комп’ютера. Створення резервних копій даних на окремому жорсткому дискові того самого комп'ютера є недоцільним, оскільки у випадку виведення основного комп’ютера з ладу, будуть знищені й основні документи і їх резервні копії. Відносно новим і досить надійним методом зберігання даних є зберігання їх на віддалених серверах в Інтернеті. Сьогодні можна отримати простір у хмарі для зберігання даних користувача як платно, так і безкоштовно.

Загалом варто відзначити, що ефективний захист від комп’ютерних вірусів забезпечує комплексна система антивірусного захисту, яка складається з чотирьох антивірусних рівнів і передбачає встановлення антивірусного ПЗ на об’єкти в зоні найбільшого ризику вірусного зараження.

На першому рівні антивірусного захисту встановлюють первинний антивірусний шлюз і перевіряють усі операції взаємодії з глобальними мережами і, зокрема, Інтернетом, що має на меті захист інформаційно-обчислювальної мережі.

На другому рівні антивірусного захисту встановлюють на сервери електронної пошти антивірусне програмне забезпечення, яке в режимі реального часу перевіряє вхідні та вихідні поштові повідомлення і, таким чином захищає сервери від вірусних загроз.

На третьому рівні антивірусного захисту встановлюють антивірусне програмне забезпечення на файлові сервери інформаційно-обчислювальної мережі: файлові, баз даних, та, за потреби, технологічні сервери й сервери розробників програмного забезпечення, з метою виявлення спроб запису на них заражених та підозрюваних файлів.

На четвертому рівні антивірусного захисту захищають АРМ (автоматизовані робочі місця) користувачів та комп’ютери, які не під’єднані до мережі, шляхом встановлення антивірусних монітора і сканера.

Засобом адміністрування системи антивірусного захисту є Symantec System Center, яка власне і дає можливість регулювання корпоративної антивірусної політики через налаштування, перегляд і блокування конфігурацій на комп’ютерах-клієнтах і серверах, що дозволяє уникнути втручання користувачів у політику захисту інформації [11].

Висновки до третього розділу

Встановлено, що на сьогоднішній день існує великий арсенал технічних засобів забезпечення інформаційної безпеки, котрі також є і інструментами запобігання внутрішнім загрозам. Серед них засоби ідентифікації і аутентифікації користувачів; засоби шифрування інформації, що зберігається на комп'ютерах і що передається по мережах; міжмережеві екрани; віртуальні приватні мережі; засоби контентної фільтрації; інструменти перевірки цілісності вмісту дисків; засоби антивірусного захисту; системи виявлення вразливостей мереж і аналізатори мережевих атак.

Ідентифікацію і автентифікацію вважають основою технічного захисту інформаційних активів. З огляду на те, що неавторизований доступ до конфіденційних даних є одним із найбільш збиткових порушень інформаційної безпеки, саме ідентифікація й автентифікація відіграють особливо важливу роль у протидії внутрішнім загрозам інформаційної безпеки. Найбільш повно вимогам комп'ютерних систем відповідають технології автоматичної ідентифікації, серед яких штрих – кодова, радіочастотна, біометрична та ідентифікація з використанням магнітних карток. У контексті забезпечення безпеки інформації найбільш виправданою є багатофакторна автентифікація.

Міжмережевий екран (брандмауер), який призначений для захисту пристроїв локальної мережі від атак ззовні, сприяє запобіганню випадковим або навмисним діям працівників підприємства, які можуть спровокувати зараження окремого комп'ютера або навіть усієї системи. Незважаючи на те, що сьогодні не існує єдиної і загальновизнаної класифікації брандмауерів, виділяють такі їх класи: фільтруючі маршрутизатори, шлюзи сеансового рівня і рівня додатків. Сьогодні більшість міжмережевих екранів включають перераховані елементи як базові.

З метою зменшення ризиків зараження інформаційної системи через Інтернет внаслідок некваліфікованих або навмисних дій персоналу широко використовують віртуальні приватні мережі (VPN). VPN є логічною мережею, яка створюється на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет) і гарантує захищену передачу даних шляхом використання засобів шифрування. VPN-рішення класифікують за такими основними параметрами: типом середовища, що використовується (захищені і довірчі), і способом реалізації рішення (комплекс програмно-апаратних засобів; програмне забезпечення; інтегроване рішення, в межах якого вирішуються завдання фільтрації зв’язку, організації мережевого екрану і забезпечення якості обслуговування).

Найбільш поширеним засобом запобігання інфікуванню інформаційних систем шкідливим програмним кодом є використання антивірусних програм, які за призначенням поділяють на детектори, фаги, ревізори, фільтри та вакцини. На думку багатьох фахівців, більш надійним методом захисту від вірусів є апаратно-програмні антивірусні засоби. Важливим кроком щодо захисту конфіденційної інформації є створення резервних копій важливих документів. Загалом варто відзначити, що ефективний захист від комп’ютерних вірусів забезпечує комплексна система антивірусного захисту, яка завдяки засобам адміністрування, серед іншого, дає можливість уникнути втручання користувачів у політику захисту інформації.

ВИСНОВКИ

Встановлено, що забезпечення інформаційної безпеки підприємства – це цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища підприємства, що забезпечує її нормальне функціонування і динамічний розвиток. Структура системи забезпечення інформаційної безпеки підприємства включає такі рівні: нормативно-правовий, організаційний, процедурний (операційний) та контрольний.

Безпосереднім об’єктом правопорушень у сфері інформаційної безпеки насамперед є інформація (дані). Підприємство має захищати дані, відомості, якими володіє або розпоряджається з дозволу законного володільця, насамперед комерційну таємницю та персональні дані.

Під загрозою інформаційній безпеці підприємства розуміють явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію власних інтересів підприємства в інформаційній сфері та створюють небезпеку для її інформації.

З′ясовано, що внутрішніми загрозами інформаційній безпеці підприємства, тобто загрозами з вини персоналу є дії чи бездіяльність (навмисні чи не навмисні) співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення матеріальних, економічних, репутаційних та інших збитків. Внутрішні загрози об’єктам інформаційної безпеки підприємства поділяють на інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні.

Оскільки персонал підприємства створює найбільше загроз інформаційній безпеці, з метою їх протидії доцільно, насамперед, проводити відбір потенційних кандидатів на посади, що передбачають доступ до конфіденційної інформації, за спеціальною процедурою, а також здійснювати контроль ефективності праці персоналу щодо забезпечення інформаційної безпеки.

Сьогодні існує великий арсенал технічних засобів забезпечення інформаційної безпеки, котрі також є й інструментами запобігання внутрішнім загрозам. Серед них засоби ідентифікації і автентифікації користувачів, які відіграють особливо важливу роль у протидії загрозам з вини персоналу, оскільки неавторизований доступ є найбільш збитковим для підприємства порушенням інформаційної безпеки.

Запобіганню випадковим або навмисним діям працівників підприємства, які можуть спровокувати зараження окремого комп'ютера або навіть усієї системи, сприяє використання міжмережевих екранів, призначених для захисту пристроїв локальної мережі від атак ззовні, та віртуальних приватних мереж (VPN), які гарантують захищену передачу даних шляхом використання засобів шифрування.

Найбільш поширеними засобами протидії шкідливому програмному коду є антивірусні програмні й апаратно-програмні засоби. Важливим для захисту конфіденційної інформації є резервне копіювання. Загалом ефективний захист від комп’ютерних вірусів забезпечує комплексна система антивірусного захисту, яка завдяки засобам адміністрування, серед іншого, дає можливість уникнути втручання користувачів у політику захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Будник М. М., Тимофєєв Д. С. Внутрішні загрози інформаційної безпеки та заходи по їх мінімізації. Інформаційні технології. Безпека та зв'язок : матеріали IV всеукраїнської науково-практичної конференції (29 листопада 2012 р., м. Дніпропетровськ). Д. : Державний ВНЗ «Національний гірничий університет», 2012. 51 с.

2. Бурячок В.Л., Киричок Р.В., Складанний П. М. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. К. 2018. 320 с.

3. Васильєв Ю. Класифікація та аналіз загроз інформаційній безпеці в ключових системах інформаційної інфраструктури Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. 2015. Вип. 1 (29). С.56-61.

4. Герасименко О. В. Інформаційна безпека підприємства: поняття та методи її забезпечення. URL: http://intkonf.org/ken-gerasimenko-ov-kozak-avinformatsiyna-bezpeka-pidpriemstva-ponyattyata-metodi-yiyi-zabezpechennya (дата звернення: 28.05.2020)

5. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. К., 2009. 608 с.

6. ДСТУ ISO 19011:2012 Настанови щодо здійснення аудитів систем управління (ISO 19011:2011, IDT). К.: Мінекономрозвитку України, 2013. 34 с.

7. Єжова Л.Ф., Корченко А.О., Мачалін І.О., Скачек Л.М., Хорошко В.О. Управління інформаційною безпекою. В 2-х томах. Видання друге, доповнене та перероблене. Том 2. К. 2012. 347 с.

8. Желіховський В.М., Ліпкан В.А., Максименко Ю.Є. Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ. 2006. 280 с.

9. Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. М.: Логос; ПБОЮЛ Н.А. Егоров. 2001. 264 с.

10. Загорецька О. Загальне діловодство на підприємствах різних форм власності. Секретарь-референт. 2013. № 03. ч. 2. URL: undiasd.archives.gov.ua/doc/zmi/SR_04_2013_kurs.pdf (дата звернення: 28.05.2020)

11. Захарченко М.В., Кононович В.Г., Кільдішев В.Й., Голев Д.В. Інформаційна безпека інформаційно-комунікаційних систем. Лабораторний практикум. Частина 1. Комплекси засобів захисту інформації від НСД: навч. посіб. За ред. ак. МАІ М.В. Захарченка. Одеса: ОНАЗ ім. О.С. Попова, 2011. 168 с.

12. Інформаційна безпека підприємства. Основні положення та ввідні поняття. URL: http://stud.com.ua/21678/ekonomika/informatsiyna_bezpeka_pidpriyemstva (дата звернення: 28.05.2020)

13. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Монографія. Запоріжжя, 2001. 115 с.

14. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD). ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. К.: Національний банк України. 2010. 163 с.

15. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. К.: Національний банк України. 2010. 49 с.

16. Кавун С.В., Носов В.В., Мажай О.В. Інформаційна безпека. Навчальний посібник. Ч.1. Харків: Вид. ХНЕУ. 2008. 352 с.

17. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості. 2010. № 3. С. 123-129.

18. Колот А. М. Мотивація персоналу : підручник. 2-ге вид., без змін. К. : КНЕУ, 2006. 340 с.

19. Легомінова С.В. Теоретичні засади інформаційної безпеки підприємства. Економіка. Менеджмент. Бізнес. 2015. № 3. С. 87–92.

20. Максимов В. Межсетевые экраны. Способы организации защиты URL: https://compress.ru/article.aspx?id=10145 (дата звернення: 28.05.2020)

21. Марущак А. І. Інформаційно-правові напрями дослідження проблем інформаційної безпеки. Державна безпека України. 2011. № 21. С. 92-95.

22. Матиев Д. Средства защиты информации: проблема выбора и соответствия. URL: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-isootvetstviya-5386161 (дата звернення: 28.05.2020)

23. Матюшко Д. Топ-7 Безкоштовних VPN (100% захищених) для України у 2020 році. URL: https://uk.vpnmentor.com/ (дата звернення: 28.05.2020)

24. Мельник С., Цуп М. Інформаційна безпека як складова економічної безпеки підприємства. URL: http://nauka.kushnir.mk.ua/?p=66146 (дата звернення: 28.05.2020)

25. Менеджмент персоналу : навч. посіб. Данюк В.М., Петюх В.М., Цимбалюк С.О. та ін.; за заг. ред. В. М. Данюка, В. М. Петюха. К. : КНЕУ. 2004. 398 с.

26. Обеспечение информационной безопасности бизнеса. В.В. Андриянов, С.Л. Зефиров, В.Б. Голованов, Н.А. Голдуев, ред.: А.П. Курило, Центр исслед. платежных систем и расчетов. 2-е изд., перераб. и доп. М. : Альпина Паблишерз, 2011. 373 с.

27. Ожиганова М.І., Хорошко В.О., Яремчук Ю.Є. та ін. Управління персоналом : навч. посіб. Вінниця : ВНТУ, 2014. 187 с.

28. Ортинський В.Л., Керницький І.С., Живко З.Б. та ін. Контроль персоналу. Економічна безпека підприємств організацій та установ : навч. посіб. К. : Правова єдність, 2009. 544 с.

29. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації : міжнар. зб. наук. праць. 2014. Вип. 2. С. 165-168.

30. Поняття і види антивірусних програм. URL: http://litr.at.ua/publ/komp_juterni_tekhnologiji_v_juridichnij_dijalnosti/tema_3/3_15_ponjattja_i_vidi_antivirusnikh_program/10-1-0-52 (дата звернення: 28.05.2020)

31. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI / Верховна Рада України. Відомості Верховної Ради України. 2010. № 34, ст. 481

32. Про інформацію : Закон України від 02.10.1992 № 2657-XII / Верховна Рада України. Відомості Верховної Ради України. 1992. № 48. Ст. 650.

33. Програмні засоби захисту від комп'ютерних вірусів. URL: https://sites.google.com/site/siteallaboutviruses/programni-zasobi-zahistu-vid-komp-uternih-virusiv (дата звернення: 28.05.2020)

34. Рощін А.О. Дослідження технології VPN з метою організації високопродуктивного та надійного транспортного середовища. URL: https://biblio.onat.edu.ua/bitstream/handle/123456789/2991/Roshchin_Bubentsova.pdf?sequence=1&isAllowed=y (дата звернення: 28.05.2020)

35. Сабанов А. Обзор технологий идентификации и аутентификации URL: http://www.infosecurity.ru/cgi-bin/mart/arts.pl?a=_060920 (дата звернення: 28.05.2020)

36. Санникова И.Н., Приходько Е.А. Экономическая безопасность: учебное пособие. Новосибирс: Из-во НГТУ, 2018. 103 с.

37. Скляренко А.К. Загрози витоку інформації через персонал. Автоматизированный информационный анализ URL: http://analiz.at.ua/publ/informacija/zakhist_informaciji/zagrozi_vitoku_informaciji_ cherez_personal/3-1-0-32 (дата звернення: 28.05.2020)

38. Сліпачук С. Комерційна таємниця на підприємстві. Справочник экономиста. 2005. №7. С.67

39. Степанов Е.А., Корнеев И.К. Информационная безопасность и защита информации. М.: ИНФРА-М, 2001. 304 с.

40. Талтаев Ч. Какой firewall лучше всех? Лидеры среди UTM и Enterprise Firewalls (Gartner 2017) URL: https://habr.com/ru/company/tssolution/blog/333338/ (дата звернення: 28.05.2020)

41. Трофимов В. В. Информационные системы и технологии в экономике и управлении: учебник / [В. В. Трофимов и др.]; под ред. В. В. Трофимова; С.-Петерб. гос. ун-т экономики и финансов (СПбГУЭФ). М.: ЮРАЙТ, 2011. 521 с.

42. Характеристика антивирусных программ URL: http://www.univer.omsk.su/omsk/Edu/infpro/1/13/virys2.html (дата звернення: 28.05.2020)

43. Цивільний кодекс України : Закон України від // Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356.

44. Черкун О.М.. Сучасні технології комп'ютерної безпеки. Монографія. Науковий керівник Р.М.Літнарович. МЕГУ, Рівне, 2012. 90с.

45. Чунарьова А.В., Власенко А.Ю. Методи та засоби захисту VPN мереж. URL: http://www.rusnauka.com/12_KPSN_2014/Informatica/4_166665.doc.htm (дата звернення: 28.05.2020)

46. Шадська У. ТОП-10 питань у сфері захисту персональних даних/ URL: https://www.prostir.ua/?library=top-10-pytan-u-sferi-zahystu-personalnyh-danyh (дата звернення: 28.05.2020)

47. VPN – що це, як створити підключення до безкоштовного віртуального сервера і налаштувати підключення.
URL: http://radka.in.ua/poradi/vpn-sho-ce-iak-stvoriti-pidkluchenn.html (дата звернення: 28.05.2020)