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

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

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

ДИПЛОМНА РОБОТА

на тему:

ОРГАНІЗАЦІЙНО-ТЕХНІЧНІ АСПЕКТИ ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ З ВИНИ ПЕРСОНАЛУ

СТУДЕНТ: Жовтюк Андрій Володимирович _____
(підпис)

КЕРІВНИК: Рабчун Дмитро Ігорович _____
(підпис)

Київ – 2022

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Освітньо-кваліфікаційний рівень – магістр

Спеціальність «Кібербезпека»

Спеціалізація «Управління інформаційною безпекою»

«ЗАТВЕРДЖУЮ»
Завідувач кафедри УІКБ
_____ С.В. Легомінова
«___»_____20__ р.

ЗАВДАННЯ

на дипломну роботу

студенту Жовтюку Андрію Володимировичу

1. Тема роботи «Організаційно-технічні аспекти протидії загрозам інформаційної безпеки з вини персоналу», затверджена наказом по університету № від «___»_____20__ р.

2. Термін здачі студентом оформленої роботи «___»_____20__ р.

3. Об'єкт дослідження: протидії загрозам інформаційної безпеки з вини персоналу.

4. Предмет дослідження: особливості протидії загрозам інформаційної безпеки з вини персоналу.

5. Мета дослідження: вивчення організаційно-технічних аспектів протидії загрозам інформаційної безпеки з вини персоналу.

6. Перелік питань, які мають бути розроблені:

1. Визначити сутність інформаційної безпеки підприємства, загрози, їх види та класифікація.

2. Дослідити особливості відбору та звільнення співробітників, які працюють з конфіденційною інформацією, визначити методи навчання персоналу з питань інформаційної безпеки.

3. Визначити напрями та методи захисту від комп'ютерних вірусів та надати рекомендації щодо забезпечення інформаційної безпеки на підприємстві відповідно до запропонованої класифікації загроз.

7. Дата видачі завдання «___»_____20__ р.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

студентом Жовтюком Андрієм Володимировичем

Дата видачі завдання «___»_____20__ р.

№ з/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, мети та завдань дослідження.	11.10.2021	
2.	Підбір наукової літератури.	13.11.2021	
3.	Визначення сутності інформаційної безпеки підприємства, загрози, їх види та класифікація	20.11.2021	
4.	Дослідження особливостей відбору та звільнення співробітників, які працюють з конфіденційною інформацією	24.11.2021	
5.	Визначення напрямів та методів захисту від комп’ютерних вірусів та надання рекомендацій щодо забезпечення інформаційної безпеки на підприємстві	06.01.2022	
6.	Формулювання висновків за результатами проведеного дослідження.	10.01.2022	
7.	Оформлення роботи.	12.01.2022	
8.	Оформлення презентації.	13.01.2022	
9.	Отримання рецензії на роботу.	15.01.2022	
10.	Захист в ДЕК.	19.01.2022	

Студент: Жовтюк Андрій Володимирович _____
(підпис)

Науковий керівник: Рабчун Дмитро Ігорович _____
(підпис)

РЕФЕРАТ

Дана робота присвячена дослідженню організаційно-технічних аспектів протидії загрозам інформаційної безпеки з вини персоналу. Робота складається зі вступу, трьох розділів, що містять 6 рисунків та 3 таблиці, висновків, списку використаних джерел із 44 найменувань. Загальний обсяг роботи становить 97 аркушів, з яких 6 аркушів займає список використаних джерел.

Розглянуто теорію і практику організаційно-технічних аспектів, поняття загроз а також їх видів. Проаналізовані можливі загрози з вини персоналу та запропоновані відповідні рекомендації щодо їх мінімізації на підприємстві.

Вступ - актуальність даної теми згідно статистики у сфері інформаційної безпеки свідчить, що близько 80% зловмисників належить до інсайдерів У компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових втрат. Таким чином, з огляду на значні обсяги втрат та шкоди підприємству внаслідок загрозливих дій персоналу, а також відсутність достатніх заходів для захисту від дій інсайдерів, необхідним є вивчення значень та видів загроз інформаційній безпеці підприємства з вини його працівників.

З огляду на зазначене, тема є актуальною в наш час, а використання її результатів сприятиме підвищенню рівня інформаційної безпеки на підприємстві,включаючи до тримання персоналом вимог щодо її забезпечення.

Об’єкт дослідження – процеси протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Предмет дослідження – методи організаційно-технічної протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Мета роботи – полягає у дослідженні організаційно-технічних аспектів протидії загрозам інформаційної безпеки підприємства з вини персоналу підприємства.

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

Для досягнення цієї мети в роботі необхідно виконати наступні пункти:

1. З’ясувати зміст та види загроз інформаційній безпеці підприємства, в тому числі з вини персоналу.

2. Дослідити організаційні засади протидії загрозам інформаційній безпеці підприємства з вини персоналу.

3. Визначити технічні аспекти забезпечення інформаційної безпеки, та внести необхідні рекомендації щоб мінімізувати ризики втрати інформації в тому числі і 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 методи протидії загрозам інформаційній безпеці.

Галузь використання - підходи можуть бути використані при плануванні та реалізації заходів менеджменту персоналу у рамках системи управління інформаційною безпекою підприємства.

Ключові слова: ПЕРСОНАЛ, ВИНА ПЕРСОНАЛУ, ЗАГРОЗИ, ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, МЕТОДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

ВСТУП

В світі інформатизованих систем, враховуючи бурхливий розвиток технологій технології, постійно вдосконалюються загрози в вигляді вірусів та інших проявів, які можуть нашкодити підприємству і це призведе до великих збитків. Відповідно треба розробляти способи протидії загрозам задля забезпечення безпеки підприємства.

У сфері інформаційної безпеки близько 80% зловмисників належить до інсайдерів. У компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових втрат. Таким чином, з огляду на значні втрати та нанесення шкоди підприємству внаслідок загрозливих дій персоналу, а також відсутність достатніх заходів для захисту від дій інсайдерів, необхідним є вивчення типів загроз інформаційній безпеці підприємства з вини працівників.

Тому політика забезпечення інформаційної безпеки підприємства має буде побудована таким чином, щоб урахувати всі потреби та протидіяти загрозам, що виникають з вини персоналу, а також захищати важливу інформацію.

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

Мета роботи полягає у формуванні організаційно-технічних основ протидії загрозам інформаційної безпеки підприємства з вини персоналу підприємства.

Для досягнення цієї мети необхідно виконати наступні завдання:

1. Розкрити сутність загроз інформаційній безпеці підприємства, в тому числі і з вини персоналу.
2. Дослідити організаційні засади протидії загрозам інформаційній безпеці підприємства з вини персоналу.
3. Визначити технічні аспекти забезпечення інформаційної безпеки підприємства у контексті протидії людському фактору.
4. Всобливості відбору та звільнення співробітників, які працюють з конфіденційною інформацією

5. Дослідити основні методи навчання персоналу з питань інформаційної безпеки

6. Визначити контроль та оцінювання якості праці персоналу у сфері інформаційної безпеки

7. Розкрити поняття ідентифікації та автентифікації користувачів

8. Між мережеві екрани та віртуальні приватні мережі

9. Визначити засоби контентної фільтрації

10. Перерахувати засоби захисту від комп'ютерних вірусів

11. Надати рекомендації щодо забезпечення інформаційної безпеки на підприємстві

Об'єкт дослідження – організаційно-технічні способи та методи протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Предмет дослідження – засоби забезпечення інформаційної безпеки підприємства протидії загрозам інформаційній безпеці підприємства з вини персоналу.

Методи дослідження.

Для вирішення зазначеного наукового завдання в роботі використані методи аналізу та управління персоналом, теорії інформаційної безпеки та технічного захисту інформації.

Наукова новизна одержаних результатів.

Надані рекомендації щодо забезпечення інформаційної безпеки можуть бути використані при плануванні та реалізації заходів забезпечення інформаційної безпеки підприємства у контексті протидії загрозам з вини персоналу.

Практичне значення одержаних результатів.

Застосування даних рекомендацій дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, якісний і правильний підбір персоналу, що працюватимуть з конфіденціною інформацією, а також проведення курсів для навчання та стимулювання персоналу до роботи.

Апробація результатів кваліфікаційної дипломної роботи. Результати досліджень, викладені в кваліфікаційній дипломній роботі , були представлені у вигляді доповіді на Всеукраїнській науково-практичній конференції: «Цифрова трансформація кібербезпеки».

Розділ 1

ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА ЗМІСТ ТА ВИДИ

1.1 Основні підходи до розуміння сутності інформаційної безпеки підприємства

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

В. Цимбалюк характеризує інформаційну безпеку як стан інформації в якому забезпечується збереження визначених політикою безпеки властивостей інформації [5, с.3].

В. Фурашев вважає що інформаційна безпека – це вид інформаційних правовідносин щодо створення підтримки, охорони та захисту бажаних для людини і держави безпечних умов життєдіяльності [1, с.48].

О. Сороківська визначає інформаційну безпеку підприємства як суспільні відносини щодо створення і підтримання на належному рівні життєдіяльності інформаційної системи господарської діяльності [1].

Доступність – це властивість бути придатним до використання авторизованим користувачам.

Цілісність – це властивість захищеності та повноти даних.

Конфіденційність – це властивість захищеності інформації від неавторизованого використання фіз. особами та процесами.

Інформаційні активи – це знання чи дані, які мають цінність для організації.

На думку С. Легомінової під інформаційною безпекою розуміється захищеність інформації ті підтримуючої інфраструктури від будь – яких

випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації її власникам або підтримуючій інфраструктурі.

Погоджуюсь, 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 організації, що забезпечує її нормальне функціонування і динамічний розвиток [1, с. 94].

В 21 столітті, пріоритетним напрямом у процесі забезпечення інформаційної безпеки підприємства є збереження в таємниці комерційно важливої інформації, що дозволяє успішно конкурувати на ринку виробництва та збуту товарів і послуг [1, с. 35].

Підприємницька діяльність тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітних інформаційних потоків. Захисту підлягає не вся інформація, а тільки та, яка представляє цінність для підприємця. При визначенні цінності підприємницької інформації необхідно керуватися критеріями, як корисність, своєчасність і достовірність надійшли відомостей.

Успіх підприємницької діяльності в чималому ступені залежить від уміння розпоряджатися таким найціннішим товаром, як інформація, але вигідно використовувати можна лише ту інформацію, яка потрібна ринку, але невідома йому. В умовах посилення конкуренції успіх підприємництва, гарантія отримання прибутку все більшою мірою залежить від збереження в таємниці секретів виробництва, що спираються на певний інтелектуальний потенціал і технологію.

Розробку заходів щодо забезпечення інформаційної безпеки підприємства слід здійснювати, дотримуючись принцип комплексного перекриття можливих каналів витоку інформації та забезпечення рівнозначної надійності захисту всіх її носіїв.

Суб'єкти впливу на інформаційну систему підприємства поділяються на дві групи: зовнішні (злочинці, хакери) та внутрішні (персонал, який має доступ до інформаційних систем).

Зазначу, що на стан інформаційних систем можуть вплинути так звані «природні» фактори, тобто ті, що не зумовлені несанкціонованими діями суб'єктів.

Методи забезпечення інформаційної безпеки підприємства можна об'єднати у три групи: правові, організаційні та програмно-технічні.

Правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства.

Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення.

Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту [2, с. 4].

Аніловська Г. Я. одним із методів забезпечення інформаційної безпеки підприємства називає стандартизацію інформаційної структури інформаційної системи, елементами якої є форми існування і подання інформації у цілому, а зв'язками - операції перетворення інформації в системі [2, с.1].

Незважаючи на використання вищезазначених методів, забезпечення інформаційної безпеки підприємства на належному рівні можливе лише тоді, коли інформаційна безпека розглядатиметься як невід'ємний елемент процесу управління підприємством [2, с. 5].

Забезпечення незмінності існуючого порядку функціонування інформаційних систем має відбуватися на трьох рівнях:

– адміністративному - за допомогою політики безпеки організації;

– локальному - шляхом формування специфічних правил для персонала;

– об'єктному - використання сертифікованих, легальних засобів програмного та апаратного забезпечення.

Об’єктом правопорушень у сфері інформаційної безпеки перш за все, є інформація. Правопорушник отримує доступ до інформації, що охороняється, без дозволу її власника, або з порушенням порядку доступу.

До конфіденційної інформації відносять відомості, що містять планово-аналітичні матеріали та звіти за період часу, та інша інформація про діяльність установи, розголошення яких може призвести до зниження ефективності функціонування однієї з систем, що забезпечують розвиток установи.

До такої інформації можна віднести:

– Результати вивчення і формування нових напрямків в інвестиційній політиці підприємства;

– Інформацію про пошук нових шляхів у діяльності установи, що підвищують ефективність;

– Матеріали контролю організацій, що працюють за участю банківського капіталу;

– Додаткові угоди, протоколи та інші документи, що оформляються

в депозитарії до договорів [3, с.20].

До комерційної таємниці відносяться відомості стратегічного характеру, розголошення яких може призвести до зриву виконання функцій однієї або декількох систем підприємства.

До таких відомостей можна віднести:

– Головні цілі, завдання установи, програми та шляхи їх реалізації;

– Відомості про помилки та прорахунки в діяльності підрозділів установи;

– Інформацію про причини, що стримують динаміку розвитку установи, обумовлені діями державних органів, конкурентів, внутрішніми причинами;

– Інформацію про негативний характер взаємодії з органами державного регулювання та управління, партнерами установи;

Виділення документів та інших носіїв інформації, які містять конфіденційні відомості, із загального потоку інформації здійснюється присвоєнням їм грифів «Конфіденційно» і «Комерційна таємниця».

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

Відомості про організацію роботи установи:

– Штатний розклад і функціональні обов'язки працівників;

– Схеми, плани розміщення обладнання, службових приміщень та їх закріплення за посадовими особами установи;

– Службова і ділове листування, інформація приватного характеру;

– Персональні дані співробітників установи та його філій.

Відомості про функціонування систем забезпечення безпеки:

– Плани розміщення і технічні характеристики систем і засобів забезпечення безпеки;

– Відомості про розмежування доступу персоналу установи до конфіденційної інформації і повноваження користувачів;

– Закріплення службових автомобілів за посадовими особами установи, маршрути їх руху, місця стоянки;

– Відомості про розміщення сховищ матеріальних цінностей та інформації, обладнанні їх засобами безпеки і порядку доступу до них [3, с. 20]

1.2 Сутність та види загроз інформаційній безпеці підприємства

Змісту поняття «інформаційна безпека» дослідниками приділяється значна увага, у той час як такі поняття, як небезпека і загроза розглядаються дещо спрощено і здебільшого у 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 [4, с.10].

Загрози інформаційній безпеці - це 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 на особистість, суспільство, державу;
- загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси;
- загрози інформаційним правам і свободам особистості право на

виробництво, розповсюдження, пошук, одержання, передавання і використання інформації [4, с 20].

Загроза інформаційній безпеці підприємства - будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та нанесення збитку ІКС. [4, с. 20].

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

Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом, як уразливість.

Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз.

За характером реалізації загрози поділяють на:

- реальні;
- потенційні;
- здійснені;
- уявні;
- повторювані;
- продовжувані.

За сферами походження:

- екзогенні - джерело дестабілізації системи лежить поза її межами;
- ендогенні - алгоритм дестабілізації системи перебуває у самій системі.

За ймовірністю реалізації:

- імовірні - такі загрози, які за виконання певного комплексу умов обов'язково відбудуться. Прикладом може слугувати оголошення атаки інформаційних ресурсів суб'єкта забезпечення національної безпеки, 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 рівнем детермінізму:

– закономірні - такі загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки.

– випадкові - такі загрози, які можуть або трапитися, або не трапитися. До таких загроз належать загрози хакерів дестабілізувати інформаційні системи суб'єктів підприємництва.

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. Так, наприклад, вірус «i love you», спричинив пошкодження комп'ютерних систем у багатьох містах світу, і завдав загального збитку біля 100 мільйонів доларів США.

За структурою впливу загрози:

– системні - загрози, що впливають одразу на всі складові елементи суб'єкта підприємництва. Для суб'єкта підприємництва це може бути вплив шкідливого програмного забезпечення, хакерські атаки, використання методів шпигунства, підкуп працівників, поширення дезінформації щодо підприємства тощо.

– 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 [6, с.2].

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. У даному 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.

За формами закріплення:

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

За джерелами походження:

– природного походження - включають в себе природні явища, що можуть порушити якість зв'язку.

– техногенного походження - транспортні аварії, пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку,

аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів органів державного управління тощо;

– антропогенного походження - вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення об'єкта. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини (це може бути помилковий запуск програми, ненавмисне інсталяція закладок);

– навмисні, що стали результатом навмисних дій людей (наприклад: навмисне інсталяція програм, які передають інформацію на інші комп'ютери, навмисне введення вірусів тощо) [6,с. 10].

Зовнішні загрози можуть бути спрямовані на носії інформації і виражатися, наприклад, в наступному: спроби викрадення документів або зняття копій з документів, знімних носіїв, зняття інформації, що виникає в тракті передачі 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.

Внутрішні загрози становлять найбільшу небезпеку для новосформованих колективів, однак увагу своєчасному розкриттю цих загроз повинна приділятися повсюдно. Не виключена ймовірність того, що окремі співробітники з високим рівнем самооцінки через незадоволення своїх амбіцій. Можуть вживати заходів щодо ініціативної видачу комерційної інформації конкурентам, а також спробувати знищити важливу інформацію або пасивні носії (наприклад, внести комп'ютерний вірус). За оцінками психологов, до 25% всіх службовців фірм, прагнучи заробити кошти будь

якими способами і за всяку ціну, часто на шкоду інтересам своєї фірми очікують зручного випадку для розголошення комерційних секретів.

Вельми важливим видається також відображення питань захисту комерційної таємниці в контракті, що укладається з керівником підприємства при його призначенні на посаду.

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.

До техногенних джерел загроз відносяться:

- неякісні технічні засоби обробки інформації;
- неякісні програмні засоби обробки інформації;
- засоби зв'язку, охорони, сигналізації.

До стихійних джерел загроз відносяться пожежі, землетруси, повені, урагани та інші форс-мажорні обставини. [6, с. 11].

До внутрішньодержавних джерел загроз інформаційній безпеці відносяться:

- недостатня економічна міць держави і недостатнє фінансування заходів щодо забезпечення інформаційної безпеки;
- відставання України від провідних країн світу за рівнем інформатизації більшості сфер життєдіяльності;
- недостатня розробленість нормативної правової бази, що регулює відносини в інформаційній сфері;
- несприятлива кримінальна 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;

– нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком інформаційного ринку в Україні;

– 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 [6, с.15].

1.3 Загрози та джерела загроз інформаційній безпеці підприємства з вини персоналу

Погіршення на підприємстві таких параметрів інформації, як конфіденційність, цілісність, доступність, вірогідність, може призвести до досить негативних наслідків:

– збоїв у функціонуванні систем управління технологічними процесами й іншими критичними системами;

– розголошення відомостей, що становлять комерційну й інші види таємниць;

– порушення вірогідності;

– несанкціонованого доступу до персональних даних фізичних осіб тощо.

Результатом перерахованого можуть стати:

– зриви переговорів, втрата вигідних контрактів;

– невиконання договірних зобов'язань;

– необхідність проведення додаткових ринкових досліджень;

– відмови від рішень, що стали неефективними через розповсюдження інформації, і, як наслідок, – фінансові втрати, пов'язані з новими розробками;

– втрата можливості запатентувати результат науково-технічної діяльності або продати ліцензію;

– зниження цін або обсягів реалізації;

– втрати ділової репутації;

У визначених ситуаціях зневага питаннями захисту інформації може призвести до повного банкрутства, тому питання аналізу загроз і ризиків є визначальним при побудові ефективної системи захисту інформації [8, с. 32]

Однак, за оцінками фахівців, лише не більше 5% підприємств використовують власні методики аналізу ризиків, що дозволяють виконувати кількісний аналіз та оптимізацію системи інформаційної безпеки.

Результати досліджень показують, що більшість підприємств не вживають достатніх заходів для захисту від дій інсайдерів. Статистика у сфері інформаційної безпеки свідчить, що близько 80% зловмисників належить до інсайдерів.

В компаніях телекомунікаційної галузі на їх дії припадає близько 90% фінансових утрат [7, с.20].

Людський фактор завжди був і є одним із найважливіших ризиків будь-якого бізнесу, оскільки більшість інцидентів відбуваються саме з вини співробітників.

Навмисний вплив часто важко відрізнити від ненавмисного, однак це не завжди потрібно, оскільки наслідки для підприємства при будь-якому із цих варіантів можуть бути катастрофічними. Те, що більшість керівників не знають джерел внутрішніх загроз, говорить про те, що в компанії приділяється недостатньо уваги інформаційній безпеці, що, є одним із найважливіших факторів існування підприємства.

Аналіз, проведений на підприємствах середнього бізнесу, показав, що випадкові кібератаки виникають набагато частіше і потенційно можуть нашкодити більше, ніж навмисні атаки інсайдерів.

У результаті дослідження з'ясовано, що більшість підприємств приділяють набагато більше уваги захисту від навмисних зовнішніх атак, ніж від більш частих і потенційно більш руйнівних випадкових внутрішніх інцидентів. Поза увагою залишаються питання потенційних внутрішніх ризиків, що вчиняють співробітники, які мають доступ до критично важливих систем і секретної інформації.

Значною є кількість порушень та випадків несанкціонованого доступу і використання інформації самими співробітниками, що ставить під загрозу основу бізнесу багатьох підприємств.

Із 500 керівників підприємств у сфері IT, що брали участь у дослідженні, більшість відзначили, що вони не знають джерел і причин виникнення внутрішніх загроз.

При цьому підприємства намагаються оцінити потенційний фінансовий збиток від цих загроз та їх вплив на операційну діяльність. Більшість внутрішніх загроз створюється ненавмисно, 20% вважають загрози навмисними, 25%, – що навмисних і ненавмисних загроз приблизно нарівно, 5% утруднилися з відповіддю. У пункті, де пропонувалося перелічити найбільші загрози за їх важливістю, майже 85% респондентів не могли точно сказати, чи були навмисними або випадковими внутрішні інциденти, спровоковані підрядчиками або тимчасовими співробітниками.

Дослідження показало, що приблизно раз на місяць на підприємствах трапляється один інцидент, який можна віднести до одного з 10 можливих типів загроз. Більше за все відбувається випадків ненавмисної втрати даних через недбалість співробітників – таких інцидентів відбувається 15-20 на рік. Внутрішні зловмисні атаки і шпигунство – 10 випадків на рік, зловживання доступом до інформації – 20 випадків на рік.

Результати дослідження свідчать, що універсального рішення для усунення внутрішніх ризиків не існує. Кожне підприємство має виробити власний комплексний підхід з урахуванням структури і специфіки діяльності. Хоча навмисних атак зловмисників стає все більше, практика показує, що випадкові помилки, неуважність до правил безпеки впливають на діяльність підприємства набагато більше, ніж атаки шахраїв [8, с. 32].

Причому, на жаль, слід констатувати, що в нашій країні не на достатньому рівні усвідомлюють небезпеку саме в інформаційній сфері, немає штатних одиниць в органах державного управління по забезпеченню інформаційної безпеки, не проводиться підготовка відповідних фахівців для органів державного управління.

До внутрішніх загроз відносять навмисні чи не навмисні дії співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами тощо. Враховуючи, що значна частина внутрішніх загроз реалізується за участі або сприяння персоналу, можна вважати, що основним джерелом таких загроз є працівники даної організації.

Виходячи з цього внутрішні загрози можуть виникати внаслідок:

– непрофесійних дій працівників;

– низького стану виховної та профілактичної роботи в організації;

– недосконалої системи заробітної плати та стимулювання праці персоналу;

– порушень правил кадрової роботи, невідповідності кадрової політики роботи в організації;

– психологічних та комунікаційних особливостей працівників;

– відсутності нормативної бази організації, яка б установлювала режими їх діяльності та правила поведінки персоналу;

– низького стану трудової та виробничої дисципліни, слабкої вимогливості керівного складу [8, с. 40].

Фахівці компанії фокусують увагу виключно на захисті даних від витоку, модифікації та знищення, і тому їх погляди відрізняються великою глибиною аналізу (Таблиця 1.1) [9, с.3].

Таблиця 1.1

Екосистема внутрішніх порушників компанії InfoWatch.

Тип	**Навмисність**	**Користь**	**Постановка задачі**	**Діїпри неможливості**
Халатний	Ні	Ні	Ні	Повідомлення
Маніпульований	Ні	Ні	Ні	Повідомлення
Скривджений	Так	Ні	Сам	Відмова
Нелояльний	Так	Ні	Сам	Імітація
Підробляючий	Так	Так	Сам/Ззовні	Відмова/Імітація/ Злом
Впроваджений	Так	Так	Ззовні	Злом

До можливих загроз безпеці інформації відносять:

– помилки персоналу під час експлуатації;

– навмисні дії зловмисників і порушників.

Способи неправомірного доступу до комп’ютерної інформації можуть бути різними – крадіжка носія інформації, порушення засобів захисту інформації, використання чужого імені, зміна коду або адреси технічного пристрою, представлення фіктивних документів на право доступу до інформації, установка апаратури запису, що підключається до каналів передачі даних. Також доступ може бути здійснений в приміщеннях підприємства, де зберігаються носії, з комп’ютера на робочому місці, з локальної мережі.

Внутрішні загрози об’єктам інформаційної безпеки підприємства за способом впливу можуть бути об’єднані в п’ять груп:

– інформаційні,

– фізичні,

– організаційно-правові,

– програмно-математичні,

– радіоелектронні.

До інформаційних загроз належать:

– порушення своєчасності інформаційного обміну, протизаконні збір і використання інформації;

– несанкціонований доступ до інформаційних ресурсів;

– маніпулювання інформацією;

– незаконне копіювання інформації в інформаційних системах;

– використання засобів масової інформації з позицій, які суперечать інтересам громадян, організацій чи держави;

– викрадення інформації з бібліотек, архівів, банків і баз даних;

– порушення технології обробки інформації.

До програмно-математичних загроз належать:

– запуск програм-вірусів;

– установка програмних і апаратних закладних пристроїв;

– знищення і модифікація даних в системах.

Фізичні загрози включають:

– знищення, руйнування чи викрадення оригінальних носіїв інформації;

– викрадення програмних чи апаратних ключів і засобів криптографічного захисту інформації;

До організаційно-правових загроз слід віднести:

– купівлю недосконалих або застарілих інформаційних технологій та засобів інформатизації;

– невиконання вимог законодавства та затримку прийняття необхідних нормативно-правових положень в інформаційній сфері;

– неправомірне обмеження доступу, до документів, в яких знаходиться важлива для громадян та організацій інформація [9, с.12]

Способи реалізації внутрішніх загроз поділяють на реалізовані:

– технічними каналами, до яких належать канали побічного електромагнітного випромінювання і наведень, а також акустичні, оптичні, радіотехнічні, хімічн;

– каналами спеціального впливу шляхом формування полів і сигналів із метою руйнування системи захисту;

– шляхом несанкціонованого доступу через підключення до засобів та ліній зв'язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав'язування хибної інформації.

Працівник підприємства, який має безпосередній легальний доступ до автоматизованої системи, може реалізувати такі загрози:

– здійснити крадіжку конфіденційної інформації - користувач може скопіювати інформацію на зовнішні носії, опублікувати її на веб-сайті, відправити за помилковим поштовим індексом. Може реалізовуватися через помилку користувача або через його навмисні дії;

– порушити авторські права на інформацію - здійснення несанкціонованого копіювання авторського документу чи його частини, шифрування документу з власним паролем, підробка реквізитів іншого користувача чи компанії;

– шахрайство - спотворення фінансової документації, перевищення повноважень під час роботи з базами даних, модифікація важливих даних.

– саботаж інформації - реалізується навмисно задля досягнення певної мети чи для помсти [10, с. 2].

Установлено, що джерела загроз ІБ підприємства з вини персоналу умовно можна поділити на навмисні та ненавмисні. До навмисних відносять скривдженість, нелояльність, впроваждженість, недоскональність системи заробітної плати та мотивування персоналу. Серед ненавмисних виділяють 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 та слабкі дії керівного складу [10, с.4].

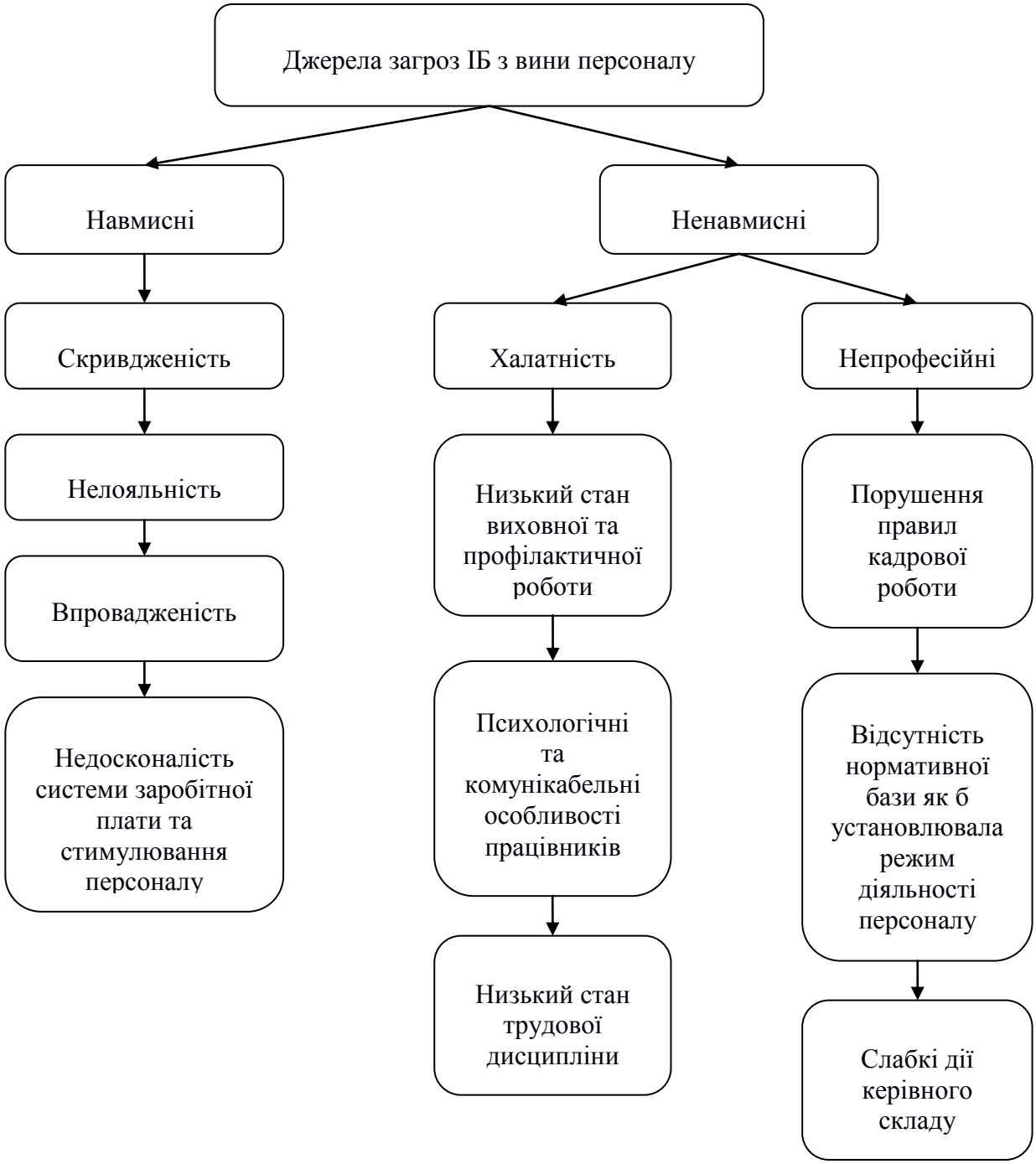

Рис. 1.2 Загрози ІБ з вини персоналу

Висновки до першого розділу

Забезпечення інформаційної безпеки підприємства – 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.

До основних методів забезпечення інформаційної безпеки підприємства відносять: правові, організаційні та програмно-технічні. Правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства. Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення. Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту.

Встановлено, що під загрозою ІБ підприємства розуміють будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та нанесення збитку ІКС.

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.

Серед основних видів загроз ІБ виділяють:

– навмисні - скривдженість, нелояльність, впровадженість, не доскональність системи заробітної плати та мотивування персоналу.

– ненавмисні - 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.

Відповідно до статистики у сфері інформаційної безпеки близько 80% зловмисників належить до інсайдерів, що свідчить про те, що керівництво підприємства не вживає необхідних заїодів для захисту інформації від інсайдерів. Набагато більше уваги приділяється захисту інформації від зовнішніх загроз та зловмисників. Це пов'язано з тим, що більшість керівників не знає внутрішніх джерел загроз, це свідчить про те, що інформаційній безпеці на підприємствах приділяється недостатньо уваги.

Внутрішніми загрозами ІБ підприємства, тобто загрозами з вини персоналу є навмисні чи не навмисні дії співробітників, що протидіють інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, підрив ділового іміджу компанії, виникнення проблем у відносинах з реальними чи потенційними партнерами.

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.

Встановлено, що джерела загроз ІБ підприємства з вини персоналу умовно можна поділити на навмисні та ненавмисні. До навмисних відносять скривдженість, нелояльність, впровадженість, не доскональність системи заробітної плати та мотивування персоналу. Серед ненавмисних виділяють 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

Розділ 2
ОРГАНІЗАЦІЙНІ ЗАСАДИ ПРОДИТІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА З ВИНИ ПЕРСОНАЛУ

2.1 Основна загроза інформаційній безпеці організацій, що виходить із її некомпетентних співробітників

За даними статистики в галузі інформаційної безпеки, близько 80 злочинців належать до інсайдера, це означає, що керівники підприємства не використовують необхідні засоби для захисту інформації від інсайдера. Набагато більше уваги приділяється захисту інформації від загрози зовнішніх осіб та злочинців. Це зумовлено тим, що багато керівників не знають джерел внутрішніх загроз, свідчать про недостатню увагу до інформаційної безпеки на підприємствах.

Внутрішні небезпеки ІБ підприємств, тобто загрози з вини співробітників, - це навмисне чи ненавмисне дію співробітників, які протидіють інтересам підприємства, результатом яких можуть бути економічні збитки компанії, втрати інформаційних засобів, падіння бізнес-іміджу компанії та виникнення конфліктів у відносинах з боку реальних чи потенційних партнерів.

Внутрішні ризики об'єктів інформаційної безпеки підприємств за способом їхнього впливу можна поєднати в 5 груп: інформаційне, фізичне, організаційне, програмне, радіоелектронне. Встановлено, що кримінальні джерела загрози ІБ підприємств із вини співробітників умовно можуть бути поділені на навмисні та не випадкові.

Умисними є образа, несумлінність, використання, недосконаліть системи оплати праці та мотивація співробітників. Ненавмисними є халатність, низький рівень виховання та профілактики, психологічний та комунікаційний стан працівників, низький рівень трудової дисципліни,

непрофесійна дія, порушення правил кадрової діяльності, недостатність нормативних баз, що встановлюють режим роботи персоналу, слабка дія керівного колективу.

Люди завжди були вразливими об'єктами для витоків та втрат інформації. У 2015 році Організація CERT проводила дослідження «E-CrimeWatch Survey», в якому було понад 800 підприємств, а кожна третя компанія, хоч би один раз на рік, постраждала від витоку інформації. Аналітики вважають, що усі інциденти витоку інформації викликані чинними або колишніми співробітниками. Це говорить про те, що проблема наявності несумлінних та некомпетентних співробітників для організації є досить важкою.

Щоб краще зрозуміти можливості витоку інформації, а також визначити способи її запобігання слід розглядати існуючі класифікації самих винуватців та класифікації загроз, що виникають щодо персоналу. Так, існують різні класифікації внутрішніх порушень – інсайдерів організації.

Одним із першочергових кроків із класифікації став міжнародний дослідний інститут IDC, який представив у 2016 році свій підхід до проблеми. За даними IDC, у системі інсайдерів чотири рівні – «громадяни», «порушники», «відступники», «зрадники».

На верхньому рівні перебувають «громадяни» - лояльні працівники, які рідко порушують корпоративні правила та етики, і насамперед не загрожують безпеці. На другому етапі перебувають «порушники», які є великою частиною всіх працівників підприємства. Ці працівники працюють на персональній почті, грають у комп'ютерну гру на роботі та роблять онлайн покупки. Представники даного рівня порушень становлять загрозу інформаційній безпеці, але подібні ситуації є невипадковими.

На наступних рівнях знаходяться «відступники» - працівники, яким більшість часу доводиться робити те, що не потрібно. Ці співробітники

зловживають привілеями доступу до Інтернету. Крім того, подібні працівники можуть надсилати конфіденційні дані компанії зовнішнім адресатам, які зацікавлені в цьому. Тому «відступники» є серйозною загрозою безпеці.

На найнижчих рівнях знаходяться «зрадники». Це співробітники, які навмисно регулярно загрожують конфіденційній інформації компанії. Халатний порушник – найпоширеніший тип внутрішнього порушника. [46, с. 5].

Порушників, що маніпулюють, є співробітники, які штовхають на порушення встановлених правил. Таких співробітників часто не підозрюють, що вони роблять дії, що призвели до втрати персональних даних, а також втрати конфіденційної інформації.

Ображені порушники - це співробітники, які прагнуть завдати компанії шкоди з особистих причин. Найчастіше причиною подібної поведінки можуть стати образи, що виникають через неправильну оцінку ролі їх в компанії, недостатнього розміру матеріальних компенсацій, неправильного розташування у корпоративному співтоваристві, відсутності елементів морального мотиву. Наступним типом є нелояльні злочинці. Це насамперед працівники, які вирішили змінити своє місце роботи, а акціонери вирішили відкрити свій бізнес.

Співробітники які «підробляють» для продажу конфіденційних даних та запровадження внутрішніх порушень є співробітниками, визначальними замовника викрадення даних. Обидва випадки інсайдери намагаються якомога надійніше замаскувати свою діяльність.

Докладно розглянемо зовнішні та внутрішні типи загрози інформаційній безпеці організації, що належать до персоналу. Зовні вважають таку загрозу, яка є джерелом якої є підприємство, проте саме тому,

що необхідно захистити інформацію, і тому, що існує внутрішня загроза. Адже якщо зацікавлених осіб для отримання інформації підприємства не було, то захищати її не варто. Зовнішні загрози можуть бути пов'язані з протиправною діяльністю злочинних структур, контрагентів, фірм, приватних осіб у сфері промислового шпигунства та соціальної інженерії. Внутрішня загроза включає необережну чи навмисну дію персоналу для розголошення інформації та афери від провідних експертів: «відкати», фальсифікація документації підприємства через електронну техніку та інтернет, запровадження «потрібних» змін до документів звіту та ін.

Розглянемо цю загрозу докладніше:

Зовнішня:

Промислове шпигунство. Вперше слово "промисловий шпигун" було сформульовано на початку XX століття на семінарі зі збору інформації для вищих менеджерів, який проводила американська консалтингова компанія Management Investigation Services Західні теоретики розуміють під «промисловий шпигунство» видобуток незаконним і нелегальним шляхом у конкурентних фірм, інформацію чи інформацію у сфері науково-дослідних досліджень, виробництво продукції за найперспективнішими технічними технологіями, та персональні дані з метою використання їх у конкурентних боротьби або в комерційних цілях [46, с. 23].

Метою промислової шпигунства часто є: перевірка бізнес-партнера на його добробут, знищення конкурента або завдання йому серйозних втрат. І якщо в першому випадку не виникає прямої загрози для організації, то в другому випадку, якщо такі агенти потрапляють до рук конфіденційної інформації, це може мати дуже серйозні наслідки для організації, починаючи з банкрутства та ліквідації.

На думку фахівців, людського чинника, тобто. «балакучість» співробітників, що займає до 60% всієї передачі інформації, решту 40 % вдалося перехопити технікою. При цьому за допомогою технічних засобів промисловий шпигун нерідко звертається до співробітників фірми, яка прагне отримати дані. Навіть працівники вищої ланки мають можливість встановити відповідне обладнання передачі інформації. Таким чином, промисловий шпигунство - важлива зовнішня загроза, яку необхідно захищати. Проте промисловий шпигун не зміг би досягти поставленої мети без внутрішніх загроз: необережних чи навмисних дій працівника.

Соціальна інженерія є методом невідкладного доступу до інформації або систем зберігання інформації, не використовуючи технічних засобів. Метод ґрунтується на використанні людської слабкості і є дуже руйнівним. Зломщик отримує дані, наприклад, збираючи персональні дані про співробітників об'єкта нападу, використовуючи звичайний телефонний дзвінок або проникаючи в організацію як її співробітник.

Методи соціального інженерія включають:

Текстування – дія, виконана відповідно до заздалегідь складеного сценарію. Цей тип атак зазвичай використовується на телефоні. У більшості випадків ця техніка включає більше, ніж лише брехня, вимагає якогось попереднього дослідження, наприклад персоналізації, дати народження і суми останніх рахунків для забезпечення довіри людини.

Фішинг – є технікою, спрямованою на шахрайство отримання конфіденційних даних. Зазвичай злочинець надсилає об'єкт електронної пошти фальсифікованим під офіційний лист банку або платіжної системи, де потрібно перевірити певну інформацію або вчинити певні дії.

Троянський кінь – це техніка використовує інтерес людини чи жадібність. Зломщик відправляє електронну пошту, що містить досить цікаву

інформацію про людину, наприклад, свіжі компромати на співробітника, вкладення зазвичай містить вірус, який зчитує інформацію з адресата комп'ютера. Така техніка зберігається ефективною доти, доки користувач неуважно відкриває якісь програми.

"Дорожнє яблуко" – адаптація "троянського коня" і складається з використання фізичних носіїв. Зловмисники можуть підкинути інфекційний CD-носій або флеш у місце, де його легко можна знайти. Носій робиться під офіційним та забезпечений підписом, який покликаний привернути до себе інтерес.

Qui pro quo – шахраї можуть зателефонувати до компанії за випадковими номерами та подати співробітника технічної підтримки, який зобов'язаний опитувати, чи є у них якісь технічні питання. У разі їх наявності співробітник у процесі «рішення» вводить команду, що дозволяє зловмисникам запускати шкідливу програму.

Внутрішні:

а) Необережність співробітників. У більшості випадків співробітники, незважаючи на те, що вони не прагнуть розкривати конфіденційні дані, роблять їх подеколи навіть не розуміючи. Таким чином, необережність можуть бути поділені на дві групи: дії чи бездіяльності працівників, які викликані незнанням у сфері захисту інформації, дії чи бездіяльності працівників, якщо працівники знають чи не знають, але знають можливі негативні наслідки.

По-перше, можна сказати про винність співробітника, але це швидше прорахунки вищого керівника, який не зміг донести до персоналу важливість інформації та захист її. Під самовпевненістю розуміються дії та бездіяльності співробітників, коли вони знали можливі негативні наслідки, передбачали їхнє нанесення, але сильно розраховували на запобігання їх. У кожному із

зазначених випадків ціль співробітника була не розголошення конфіденційних даних, але саме це й сприяло його дії.

b) Умисні спроби працівників розголошення інформації. Намір, на відміну від обережності, передбачав, що мета діяльності працівників була саме розкривати конфіденційну інформацію. Причому працівники могли бути завербовані агентами промислових шпигунств або самі вирішили підставити організацію, до якої вони працювали ініціативно. Для виявлення або запобігання таким діям необхідно визначити, чому працівники йдуть.

Наведено класифікацію мотивації недобросовісних та недобросовісних співробітників для розголошення конфіденційних відомостей організації у таблиці 2. 1. 1.

Таблиця 2.1.1

Клас мотивів	Зміст та характеристика
Особисті мотиви співробітника	особисті фінансові труднощі, неможливість задоволення життєвих потреб своїх та сім'ї; психологічна готовність схильність працівника до зловживання службовим становищем; порочні зв'язки, вчинки, захоплення;
Внутрішні мотиви організації	наявність слабких місць у системі управління діяльністю фірми (зокрема, у системі управлінського обліку); низька кваліфікація керівництва організації; нездоровий діловий клімат у колективі

	організації; слабкий кадровий менеджмент, що дозволяє обіймати відповідальні посади співробітникам-аферистам, неефективна персональна робота з кадрами; відсутність чи слабкість корпоративної політики та етики; слабка організація системи навчання персоналу; неефективна система мотивації (немає аналізу потреб кожної особи та персональної мотивації); неякісна перевірка кандидатів під час прийому працювати
Зовнішні мотиви	умови матеріальної та/або моральної мотивації у конкурентів кращі; зовнішній тиск на працівників;

Аналізуючи загрози конфіденційності даних, пов'язаних із персоналом, можна побачити, що ігнорування цих загроз призводить до появи серйозних збитків та шкоди діяльності організації. Це не тільки фінансові втрати компанії, але також різке падіння іміджу компанії, оскільки вона не здатна захищати конфіденційні дані [46, с.54]. Таким чином, керівництво організації має вкрай серйозно та відповідально ставитися до питання захисту конфіденційних даних від вищезгаданих загроз власними безвідповідальними та несумлінними співробітниками та персоналом організації взагалі.

2.2 Основні поняття та функції та принципи управління кадровою політикою

Кадрова політика визначає основні напрямки та принципи роботи з персоналом у довгостроковій перспективі. Термін «кадрової політики» має широке і вузьке значення. У широкому плані - система усвідомленого та певного сформульованого та закріпленого правила, норми, що призводять людські ресурси до довгострокових стратегій компанії. Воно спрямоване на вирішення проблем виробництва, соціального та особистого характеру людей на різних рівнях відповідальності. У вузькому – це набір певних правил, рекомендацій та обмежень, які діють як у безпосередніх взаєминах співробітників, так і у взаєминах робітників та організацій взагалі.

Кадрова політика формується у державі, керівних партіях і керівних підприємствах, і має конкретний вираз у вигляді адміністративної та моральної норми поведінки людини у суспільстві та організації. В економіці ринку істотно змінюються сутність, принципи кадрового менеджменту. Вона свідомо та навмисно створює високопрофесійний трудовий колектив, який сприятиме розвитку Організації та Людини.

Основне завдання кадрового менеджменту: своєчасне забезпечення організацією певною якістю особистістю відповідно до стратегії розвитку організацій; створення умови для здійснення прав та обов'язків громадян відповідно до законодавства про трудове законодавство; раціонального використання персоналу; формування та підтримання ефективної діяльності підприємства. Кадрова політика формується з врахуванням впливу зовнішніх та внутрішніх факторів, характерних для теперішнього і майбутнього.

До зовнішніх факторів відносяться: національне трудове законодавство; взаємовідношення з профспілкою; стан економічної кон’юнктури; стан і перспектива розвитку ринку праці.

Внутрішніми факторами є: структура, цільові та стратегічні цілі організації, територіальне розташування, технології виробництва, організаційну культуру; кількісність та якісність наявних персоналів та можливе їх зміна у перспективі, фінансову здатність організації, що визначає допустимі рівні витрат на управління персоналом; рівень рівня оплати праці. Таким чином, вибір її пов'язано не тільки з вибором основних цілей - а й з вибором методів, методик, пріоритетних напрямів.

Правила про внутрішній трудовий розпорядок працівників та працівників - важливий нормативний документ, що регламентує найми та звільнення працівників, робочі дні, порядок розгляду трудового спору. Це внутрішня нормативна документація, яка має відповідати Кодексу законів праці та типовим правилам, враховувати особливості підприємства.

До його складу входять такі підрозділи: загальні положення, порядок нарахування та звільнення працівників, час роботи та відпочинку, основні обов'язки робітників та адміністрацій, заходи надання допомоги та покарання.

Колективний договір є правовим актом, що регулює соціальні та трудові відносини найманих працівників та роботодавця. Колективний договір встановлює відокремлені зобов'язання сторін для регулювання трудових, соціальних та економічних взаємин, у тому числі: забезпечити рівноправність сторін, дотримуватися норм законодавства, встановити форми, системи та рівень зарплати, режим роботи та умови праці, забезпечити участь членів трудових колективів у керівництві організацією; забезпечити реальність виконання зобов'язань, контролювати виконання колективного договору та відповідальності сторін. Кадрову політику підприємства здійснюють стратегічні та оперативні системи.

Кадрова стратегія - комплекс організаційних рішень та заходів щодо розробки та реалізації найважливішого кадрового завдання підприємства.

Складові стратегії кадрової політики підприємства – планування потреб у кадрах, підготовка та вдосконалення кваліфікації, система регулювання, заробітна плата. Кадрова тактика є практичною дією, спрямованим на реалізацію стратегій.

Інструмент реалізації кадрових політик є кадрова служба - основна структурна частина апарату управління, що здійснює оперативне супроводження кадрів.

Основні завдання кадрової служби: проводити конкурси на вакантні посади; прогнозувати та визначати поточну та перспективну потребу у кадрах, джерела їх задоволення, уточнювати потреби у навчанні фахівців із прямого зв'язку з навчальним закладом; планувати та регулювати професійний та кваліфікаційний розвиток працівників, процеси їх звільнень та переміщень; забезпечити професійне, економічне навчання, підготовку та перенавчання співробітників, стажування; вивчити професійні, ділові особисті якості працівників на основі тестування, соціологічного досвіду, розробку рекомендацій щодо їх раціонального використання залежно від здібностей та потреб організації; адаптувати молоді кадри.

Кадрова безпека є процесом профілактики негативних впливів на економіку підприємства шляхом ризику та загрози, що виникають щодо персоналу, інтелектуального потенціалу та трудових відносин взагалі.

Якість кадрів залежить від трьох основних чинників:

Наймання – є комплексом заходів безпеки під час роботи та прогнозу добробуту. Цей фактор включає розгляд проблем безпеки компанії на етапах його роботи, таких як пошук кандидатури, процедури вибору, документально-правове забезпечення прийому до роботи, термін їх випробування, а також адаптацію.

Лояльність – задоволеність працівника умовами, зарплатою, перспективою, колективом та захистом від загрози зовнішнього середовища.

Контроль - комплекс заходів, встановлених персоналом, включаючи адміністрацію, регламенти, обмеження, режими, технологічні процеси, оціночні, контрольні та інші операції, процедури безпеки. Комплекс безпосередньо спрямований на ліквідацію можливих причин шкоди, і його зазвичай відпрацьовують служби безпеки або інших підрозділів.

Питання кадрової безпеки включають: забезпечення підприємством необхідних співробітників, заповнення робочих місць, утримання персоналу, його розвиток, розробка мотиваційної схеми та схем виплати праці, усунення шкоди від трудових спорів, підвищення кваліфікації персоналу, аналіз ситуації з конкурентами, робота з сайтами робочих місць, кадрові агенції, аналіз ситуації в регіоні, оцінка підприємством як роботодавця, способи проектувати кар'єру. Визначаючи першокласність працівників у діяльності організації важливо враховувати, що з персоналу виникають істотні загрози підприємствам. Ці ризики за місцем виникнення можуть бути поділені на дві категорії: внутрішня та зовнішня.

Внутрішні загрози включають: не відповідність кваліфікації працівників вимогам їх; нестача кваліфікації працівників; неефективне керування персоналом; неефективне керування ресурсами персоналу; неефективне керування мотивацією; скорочення кількості раціоналістичних пропозицій, ініціатив; повернення кваліфікованих працівників.

Зовнішні ризики включають: найкраща умова мотивації конкурентів; тиск конкурентів на співробітників ззовні; інфляція не може не враховуватися при розрахунку заробітних плат та прогнозуванні їх динаміки.

Найбільш поширені види порушень, пов'язаних з недотриманням кадрової безпеки, є: афери провідних менеджерів, керівників середніх

посадових осіб, які відповідальні за певний напрямок діяльності підприємства, головним чином за стінами фірми, особливо за міжнародними організаціями; фальсифікації «живих» грошей, грошей у касі, а також сум банківських рахунків, підробка документів підприємства, наприклад, переказ коштів підприємства на особисті рахунки, внесення «потрібних» змін до документів, фальсифікації звітів про відрядження, «представницькі витрати», інші потреби підприємства.

Мотивація аферних співробітників підприємства може бути класифікована так: особистими фінансовими труднощами, неможливістю задовольнити життєві потреби та сім'ю, наявність слабкого місця в управлінні діяльністю компанії, низькою кваліфікацією керівництва компанії, нездоровим діловим кліматом колективу компанії, психологічною готовністю працівника зловживати службовим становищем, відсутність налагодженого управління керівництвом за діяльністю співробітників, неефективним кадровим менеджментом, що дозволяє займатися відповідальними посадами співробітників-аферистів, неефективною персональною роботою з персоналом. Основними органами кадрової охорони підприємства є служба кадрового управління та служби безпеки.

2.3 Робота з персоналом для забезпечення кадрової безпеки підприємств

Безпека системи залежить від надійності її слабкого вузла. Людина є найскладнішим, а також найуразливішим елементом будь-якої системи - будь то система людини-машин або підприємницької організації.

Несприятливий вплив людини благополуччя позначається поняттям «людський чинник», тобто сукупність соціальних та економічних можливостей людини, яких ступінь їх реалізації залежить від мотивації та ставлення людини до трудового процесу, морального та матеріального інтересу до високопродуктивної праці.

Основні прояви фактора людського характеру: людина у своїй діяльності, з будь-яких причин, може припуститися помилок різного характеру, особа, яка приймає рішення, перебуває в невизначеності, може приймати помилки, у процесі життя людина може перебувати в екстремальних ситуаціях, коли індивід втрачає здібності до раціональної дії і вирішення, що відповідає сформованим ситуаціям.

Збір та аналіз інформації кандидатів на посаду необхідно для попередньої оцінки та відбору кандидатів за формами, перевірки наданої інформації та забезпечення кадрової безпеки підприємства. Якісні перевірки кандидатів під час роботи зменшать ймовірність їх зловживання з боку інших. Серед злочинів сьогодні найчастіше зустрічаються фальсифікації документів, невідповідності витрат, пов'язаних з виконанням відрядження, представницьких витрат, так званих «відкатів», є одним з найбільш але поширених методів, популярних у разі незаконного продажу та використання майна підприємств і так далі.

Серед способів вибору персоналу варто відзначити розробку, проведення тестів з виявлення професійних орієнтацій, ерудованості, інтелекту, здібностей та розуміння. Головною метою попереднього оцінювання є відсіяння кандидатів, які не відповідають мінімальним вимогам вакансії, що дозволить згодом економити час та зусилля на підготовці та проведенні випробувань. Попереднє оцінювання починається з аналізу резюме, його вивчення – перше знайомство з шукачем.

Залежно від результатів аналізу, резюме кожного кандидата може бути поділено на три категорії:

1. Кандидати з більшими конкурентними перевагами, ніж інші, такі кандидати обов'язково повинні запрошуватися на зустріч.

2. Кандидати з конкурентоспроможності поступаються представникам першого ряду, хоча можуть запросити їх на зустріч, якщо немає достатньої кількості кандидатів у першу групу.

3. Кандидати з недостатньою кваліфікацією для виконання обов'язків за посадою, на яку вони беруть участь. До групи належать і кандидати, які надіслали резюме з помилками граматики. На інтерв'ю не повинні запрошуватись кандидати з найменшим рівнем конкуренції.

У резюме можуть бути: посади, на яких кандидат претендує, компенсаційні очікування; біографічні дані: вік, стать, місце проживання, сім'я, освіта; місце роботи на раніше займаних посадах; дати прийому та звільнення; функції, обов'язки, що виконуються на посадах та місцях роботи; досягнення; індивідуальні особистісні характеристики, інтереси, захоплення, уявлення про бажані місця роботи; можливості надати рекомендації та ін.

Резюме необхідно вивчити по порядку викладу кандидата ланцюжка найважливіших подій навчання та робочого життя. Особливо уважно слід аналізувати дані про кваліфікацію кандидата, у резюме містяться дані про рівень підготовки та підвищення кваліфікації: чи відповідає інформація про вимоги, в якому порядку отримано освіту; в якому навчальному закладі, в якій формі навчається кандидат; чи відповідає тематиці семінарів, курсів, профілю основної діяльності кандидата; чи має кандидат виняткові знання та вміння; наскільки важливо на підприємстві мати професію кандидата, а також чи буде його цінність надалі.

В аналізі трудової діяльності кандидата слід звернути увагу на такі відомості: наскільки докладно описано його функції, обов'язки, наскільки широкі чи спеціалізовані інтереси професійного характеру; наскільки кандидат керувався при виборі певного місця роботи; чи був у кандидата зліт та падіння у трудовому житті.

Крім даних про роботу, рівень навчання та інших формальних характеристик, важливе формальне подання інформації, логічне викладення, формулювання, пунктуальність. За даними, наданими кандидатом, необхідно охарактеризувати його життєві шляхи та знайти важливі відомості про особистість, професійний та діловий потенціал, мотиви поведінки. Для отримання більш детальної інформації щодо кожного кандидата та його правильного структурування, підготовки до бесіди фахівці з персоналу розроблять стандартну форму анкети та оціночних листів. Кандидати, заповнивши форму, можуть надсилати їх на електронну пошту, перш ніж отримати бланки або заповнити їх на підприємствах. Зміст стандартної форми може відрізнятись від специфіки компанії, вимоги до кандидата, політика підприємства з професійного підбору.

У деяких компаніях використовують стандартні персональні листки для обліку кадрів, проте більшість з них розробляють спеціальні детальні анкети для обліку кадрів. Оптимальним та достовірним, об'єктивним напрямком професійного відбору є використання спеціальних психофізичних досліджень, таких як: діагностування нейродинамічної, індивідуальної типологічної та особистісної характеристик людини, визначення індивідуального психосемантичного поля значень у зв'язку з мотивацією надходження на службу та ставленням до наркоманії, алкоголю; поглиблене поліграфне опитування поліграфного скринінгу за методами, які були складені на основі даних, що попередньо одержуються; поліграфний скринінг за методами, сформованими на основі попередньої інформації.

2.4 Політика підвищення надійності співробітників та критерій їх оцінки

Надійність – одна з найважливіших складових підвищення професійної кваліфікації співробітників державних та поза державних установ. Власники такої якості зберігають моральну стабільність і лояльність

до підприємства, де вони працюють, відчувають себе «прив'язаними» до нього, сама робота має високу мотивацію, а втрата її оцінюється як серйозна життєва невдача.

Серед головних завдань щодо покращення ефективності роботи управлінської та виконавчої структури найважливішим є формування їх співробітників, які мають необхідні якості для успіху освоєння обраної посади, створення системи, яка збереже та розвиває їхню робочу здатність та стійкість. Такі завдання неможливо виконати без періодичного спостереження за функціональним станом співробітника та визначення об'єктивного критерію якісного складу таких структур та відділів.

Єдиним критерієм, що свідчить про реальний стан професійної компетентності та стійкості персоналу, є актуальність кадрового потенціалу. Характеризуючи цей показник, можна назвати такі елементи: звільнення працівників із встановленим віком перебування на роботі; звільнення по здоров'ю за середньостатистичними показаннями захворюваності по країні, звільнення через різні соціальні та професійні мотиви; дискредитацію звання співробітника установи, органу, компанії; дисциплінарні злочини та злочини за посадовими злочинами, професійною деформацією та ін.

Надійність робочого персоналу залежить від величини можливих порушень роботи всіх відділів підприємства у зв'язку з несвоєчасним наданням інформації, помилками у розрахунку, порушенням трудовою дисципліною тощо. Комплекс технологій, програм, математики та інформації називається комп'ютерною поліграфією чи детектором ложі. Поліграфічне опитування є комплексом спеціальних випробувань, технік, програм, математики та інформаційних технологій. Взаємодія комплексу з експертом дозволяє з'ясувати приховану інформацію про них. Як правило, у планових перевірках проводяться лише поліграфічні опитування, регулярність яких регламентується відомчим нормативним актом. Позапланова перевірка

проводиться у разі зміни посадових осіб, службового розслідування, оформлення допуску до виконання робіт, які потребують вищих рівнів таємниці. Інформація щодо методів проведення опитувань з поліграфії, технічних можливостей спеціального поліграфування – державна таємниця.

Загальна кількість перевірок включає: перевірки щодо процедури профвідбору персоналу, планові, позапланові перевірки, службове розслідування, заходи щодо протидії злочинності.

Нестабільність, тобто. моральна загроза людини може бути визначена різними причинами та факторами. Їх можна назвати так:

1. Нехтування, навіть презирство щодо загальновизнаних моральних норм.

2. Індивідуалізм особистості, неспроможність та нездатність працювати в одній команді, тверде прагнення протистояти колегам та відсутність почуттів корпоративного характеру, впевненість у місцях та колективі.

3. Підвищений рівень самооцінки, що не відповідає реальній спроможності людини, впевненість у власній непогрішності, непропорційне марнославство, незадоволена амбіція, заздрісність. При цьому істотну роль у цьому відіграє невдоволення кар'єри, конфлікт між високою роботою та дієвим просуванням.

4. Характерні риси характеру, що викликають психопатію, характеризуються помстивістю, злопам'яттю, високою вразливістю. Такі люди не можуть довго звільнитися від негативних емоцій, вони схильні до конфлікту з іншими людьми. Особливо небезпечні стійкі конфлікти по вертикалі, коли співробітник довго зберігає бажання образити свого керівника за завдання образ.

5. Особистість незрілості, відсутності самостійності у судженнях, орієнтації на інших людей, сильніша в психологічному відношенні, у вирішенні та дії легкої добровільної підпорядкованості впливу з боку.

6. Імпульсивна поведінка, що домінує у поведінці людини. Він проявляється тим, що людина легко може втратити самоконтроль і необдумані, бездумні дії. Вони мають слабкості особистого роду, наприклад, вживання алкоголю, пристрасть до гри в азартні ігри і т. д. Вчинки подібних людей визначають не усвідомлені цілі та наміри, а внутрішній імпульс чи зовнішні обставини.

7. Невлаштованість особистого життя, відсторона від інших людей, відсутність самотності, «втрата кореня», відсутність родичів, зв'язку з нею.

8. Гостра ментальна потреба в лікуванні, наприклад, дорогого лікування, яке людина самостійно реалізувати не може. Цей фактор менш передбачуваний, а отже, менш керований. При цьому оперативно отримати повну та правдоподібну інформацію про те, що така ситуація, може зменшити негативний вплив на надійність працівника.

9. Наявність контакту цієї людини з одним із представників конкурентних фірм. Цей фактор дуже небезпечний, оскільки найбільшої шкоди в умовах жорсткої конкуренції може завдавати саме той, хто може спеціально залучити конкурентів до компанії, щоб з'ясувати інформацію про ситуацію в ній «зсередини» або використати інший спосіб завдяки рідним чи іншим близьким людям.

Основні напрямки робіт створені задля підвищення надійності працівників і запобігання недобросовісності працівників:

- проводити серйозний і комплексний відбір кадрів, у якому: не можна прийняти працювати людей із серйозними особистісними вадами, що ганьблять їх соціальний зв'язок; біографії, що свідчать про наявність

моральних вад; обов'язково встановити термін випробування всіх найманих співробітників;

- наявність терміну випробування дозволяє краще оцінити особисту та ділову якість співробітника, визначення його готовності до виконання поставлених перед ним завдань. З метою доповнення загальних умов бажано доповнити такі заходи, як особисті доручення працівників, за рекомендаціями яких кандидат приймає на роботу, отримання відомостей із колишніх навчальних закладів чи робочих місць, аналіз підсумків його минулої діяльності тощо;

- створення умови, у яких співробітник змушений буде не вчиняти дії, які завдають шкоди організації та керівництву організації. У цих умовах має бути включена ціла система заходів для морального і матеріального стимулювання, формування престижу роботи у тій чи іншій компанії, турбота про внутрішній вигляд компанії, створення в ній такого соціально-психологічного середовища, яке буде сприятливим для всіх працівників;

- створення корпоративності співробітників, тобто вживання заходів для того, щоб створити у них почуття приналежності до компанії, щоб вважати її «своєю», а у разі загострень звернутися за допомогою до компанії, не шукати на стороні, попередити ситуації, коли співробітник чи близькі до нього люди можуть перебувати у безвихідності критичної ситуації, коли він може отримати її в конкуруючій організації.

У таку систему можуть бути передбачені заохочення за сумлінну працю, суворе дотримання дисципліни праці та сумлінність компанії, нагородження преміями, цінними подарунками чи іншими нагородами, туристичні путівки тощо, забезпечення поєднання стилю управління. Таким чином, стиль роботи керівних осіб будь-якого рівня в організації не повинен бути суворим авторитарним і не повинен завдавати шкоди для його гідності, виконувати його обов'язки, наскільки вона може виконувати корпоративну культуру, не мати джерела постійного конфлікту, сварки, суперечки тощо;

- створювати та зміцнювати в компанії психологічний клімат, не допускати виникнення випадкових конфліктів та суперечок, не допускати постійного конфлікту, сварки, суперечки тощо; сформувати "командний дух", згуртованість; взяти підписку на нерозголошення службової інформації
- приймати підписки на нерозголошення службової інформації та не допускати постійного конфлікту, сварки, суперечки тощо; створювати "командний дух", згуртованість; приймати підписки на нерозголошення службової інформації та не допускати постійного конфлікту, сварки, суперечки тощо; створювати "командний дух", згуртованість.

У підписці обов'язково мають бути включені пункти: у випадках моральної нестабільності керівництво за собою залишає право притягувати працівника до адміністративної відповідальності за чинним законодавством; періодичні щорічні та щоквартальні нагадування працівникам, що необхідно дотримуватися певних правил поведінки, відновивши відповідну підписку; організаційні заходи, що допоможуть зберегти комерційну та іншу службову таємницю; звільнити працівника за негрубе порушення дисципліни, недобросовісність – «розлучення» мають бути «мирними». У разі заподіяння компанії значної матеріальної чи моральної шкоди працівник, може стати винним персонал та його управління

Існує думка, що безпека кадрів визначається трьома показниками:

1. Рівнем професійної майстерності.

2. Частина співробітників належить до групи ризику співробітникам з різними відхиленнями, з порушеннями особистості, схильними до делінквенному поведінці.

3. Лояльність працівників. Остання частина універсальна у своєму напрямі: ставлення людини до своєї організації є факторами, які або зміцнюють або руйнують систему кадрового забезпечення. Тобто чим

лояльніші працівники, тим більше потенційної шкоди вони можуть завдати своїм вчинкам чи бездіяльності.

Професійна лояльність - доброзичлива, коректна, щира, поважна позиція керівництва, співробітників, інших осіб, їх дій та загалом компанії; усвідомлене виконання працівниками своєї роботи з цілями та завданням та за інтересами компанії, дотримання правил, правил, зобов'язань, у тому числі неформальних, по відношенню до компанії, керівництва, співробітників та інших суб'єктів взаємодії; усвідомлене виконання співробітниками своєї роботи з цілям та завданням, у тому числі стосовно компанії, керівництва, співробітників та інших суб'єктів взаємодії.

Основними складовими лояльності персоналу є задоволеність роботою, відданість персоналу. З погляду економічної служби, яка вважає персонал «слабким місцем організації», усі співробітники вважають потенційно небажаними.

Під «нелояльною» поведінкою розуміється свідома чи несвідома причина шкоди діяльності суб'єкта господарювання. З позиції персональної служби лояльність розглядається як емоційне ставлення до організації, яке залежить від рівня прихильності персоналу до зовнішніх зарплат, пільг, робочих умов тощо, а також внутрішнім змістом виконуваної діяльності, можливостей професійного зростання, визнання та оцінки досягнень стимулу, запропонованого роботодавцем.

Об'єктивні «зовнішні» показники лояльності можуть розглядатися як об'єктивні показники якості та продуктивності праці, ступінь дисципліни працівників, кількість та відсутність виручки тощо. У комплексному дослідженні об'єктивні дані мають бути поєднані з об'єктивними показниками, що характеризують стан суб'єктивної свідомості людини.

Управління персоналом - процес оптимізації наявного людського ресурсу, підвищення ефективності діяльності підприємства, підвищення якості виконаних робіт та включення персоналу у діяльність підприємства, тобто формування високого рівня лояльності.

Основні етапи розвитку системи менеджменту лояльності персоналу:

- розробка концепції менеджменту лояльності персоналу, яка визначає основні аспекти роботи зі співробітниками у кадровій стратегії підприємства;

- внутрішнє та зовнішнє середовище підприємства, аналіз системи ресурсів – визначає, на яких ринках має виходити робоча сила та скільки залучити додаткових співробітників у разі неможливості забезпечення результату внутрішніх ресурсів;

- визначення проблематичних зон підприємства у процесі управління дозволяє визначати пріоритетний напрям дій, вкладених у зміну цієї ситуації, і навіть навести роботу з персоналом з розробленої концепції;

- розробка цілей менеджменту персоналу, тобто визначити конкретні показники та способи її досягнення працівникам, цілі співробітництва мають формуватися відповідно до спільних цілей підприємства;

- формування переліку заходів, спрямованих на створення лояльних співробітників. Повинна бути врахована специфіка підприємства, спрямовано на підготовку співробітника додатковим зусиллям, спрямованих підвищенням ефективності, та продуктивність праці підприємства;

- процес здійснення заходів забезпечує координацію розробки та реалізації планів підприємств і систем менеджменту персоналу;

- контроль – забезпечує визначення відповідності реалізованим напрямам управління, становище довкілля та формування напрямів змін.

2.5 Особливості підготовки та звільнення працівників на підприємствах

Підбір кандидатів для призначення на посаду, пов’язані з конфіденційною інформацією – є одним із найважливіших етапів роботи з персоналом компанії, підбору потенційних кандидатів на посаду, пов'язану з конфіденційними даними. При виборі кандидатів оцінюються відповідність кожної з таких основними вимогами: рівнем підготовки, кваліфікації, що є необхідним досвідом роботи; моральним та діловим якостям; ступенем відповідальності за прийняття управлінських та виконавчих рішень відповідно до посади.

При виборі кандидатів на посаду, пов'язану з конфіденційними даними, обов'язково враховуються рівні кожної конкретної посади в аспекті прийняття управлінського рішення та виконання управлінських функцій, організаторської функції та завдань, що стоять перед підприємством.

З зазначених критеріїв, ці посади поділяються такі категорії:

- керівники підприємств, їх філій, представництва;
- заступники керівників;
- керівники структурних підрозділів;
- керівники служб безпеки підприємств;
- посади співробітників підприємства, які здійснюють на постійній основі роботу з конфіденційною інформацією.

При виборі кандидатів на зазначені посади додатково враховуються обсяги та важливість конфіденційних відомостей, які допускаються працівникам, які обіймають ці посади [11, с.2].

А. Алєксєнцев включає всю конфіденційну інформацію, яка є частиною будь-якої таємниці [12**,** с. 44].

Г. Андрощук конфіденційну інформацію відносить як діловий, виробничий, торговий та інший характер, яка не підлягає розголошенню через її секретність [14, с. 28].

Організаційні заходи, пов'язані з підбором персоналу, що володіє доступом до інформації, можуть бути поділені на такі групи:

- проводити ускладнені аналітичні процедури при прийомі та звільненні працівників,

- документувати добровільну згоду особи, яка не розголошує конфіденційну інформацію, дотримуючись правил безпеки інформації, - інструктувати та навчати працівників практичним заходам захисту.

При розмові та нараді з кандидатами у сфері захисту інформації здійснюються такі завдання:

- Виявлення реальної причини бажання працювати на цій компанії;

- Виявлення можливих злочинців або спроби побачити слабкість кандидата як людину, яка може бути здатна шпигувати;

- Виявлення добровільної згоди кандидата на дотримання правил захисту інформації, та наявність певних обмежень в особистому та професійному житті.

Крім того, співробітник кадрової служби просить необхідні документи та довідки, знайомить кандидата зі змістом договору про допуск до конфіденційних відомостей.

Відповідальний секретар повинен звернутися до аналізу правильності та достовірності оформлення особистих документів: прізвище, ім'я та по батькові, інші персональні дані, наявність у документах необхідної позначки та запису, ідентичність фото та особистість громадянина, дотримання форми документів терміну його використання, неперевірені виправлення, спроби заміни листків, фотографій [11, с.3].

Весь друк має відповідати назві організацій, що видали документ. Наприклад, трудові книжки повинні відповідати формам, встановленим протягом періоду, коли їх було випущено або мати напис «дублікат», містити запис про звільнення з останнього робочого місця, завірений печаткою тощо. За будь-якого сумніву особа просить надати дублікати виправлених документів та завірити виправлення. Документи, що викликали сумнів, громадянину повертаються, а заодно відмовляються розглядати питання про роботу. Тільки після уважного аналізу поданих документів та кандидатів на посаду відбувається співбесіда.

На думку експертів, кандидат на вакантну посаду, в якій передбачено роботу з конфіденційними даними, повинен мати низку персональних якостей. Також передбачено перелік персональних якостей, які є небажаними для співробітника, зайнятого у сфері інформаційних технологій. Після того, як рішення про призначення кандидата, який повністю задовольняє вимоги, буде прийнято рішення про призначення кандидата на посаду з точки зору допуску до конфіденційних даних керівник підрозділу, в якому призначається особа, організує інструктаж спільно із Службою безпеки підприємства. У ході навчання новопризначеній особі доводяться до відома її обов'язки, положення нормативних та зовнішніх організаційних документів, що регулюють питання охорони конфіденційних даних на підприємствах.

Таблиця 2.2

Особисті якості, якими має / не має володіти працівник, що працюватиме з конфіденційною інформацією

Бажані особисті якості	Небажані особисті якості
Порядність, чесність, сумлінність, принциповість	Емоційний розлад
Старанність, дисциплінованість	Неврівноваженість поведінки
Емоційна стійкість	Відчуження від колег по роботі
Прагнення до успіху і порядок у роботі	Розчарування в собі і своїх здібностях
Самоконтроль у вчинках і діях	Ображене приватне самолюбство
Адекватна самооцінка власних можливостей і здібностей	Невдоволення своїм службовим становищем
Помірна схильність до ризику	Вкрай егоїстична поведінка
Вміння зберігати секрети при будь-яких обставинах та в будь-якому стані	Відсутність достатньої розсудливості
Тренована увага	Нечесність
Хороша пам'ять, вміння вести порівняльне оцінювання фактів, пропозицій і т.д.	Небажання і нездатність захищати інформацію
	Фінансова безвідповідальність, бажання отримати гроші без особливих затрат розумових і фізичних сил
	Вживання алкоголю та наркотиків, що призводить до балакучості, необдуманих вчинків

Підготовка працівника до виконання нових посад здійснюється відповідно до плану, затвердженого керівником підрозділу, в якому призначено цього співробітника [12, с.6].

У процесі підготовки персоналу з'являються співробітники, які не відповідають вимогам компанії, а потім на порядок денний може з'явитися питання про звільнення. Звільнення претендентів на посаду, пов'язану із конфіденційними даними. Для працівників підприємства, які допускають конфіденційну інформацію, етап звільнення посідає особливе місце. Після того, як керівництво підприємства вирішило звільнити співробітника, який допустив втрату конфіденційної інформації, або перевести його на роботу, не пов'язану з конфіденційною інформацією, Служба безпеки та Кадрове управління підприємства вживають заходів щодо запобігання можливості розголошення звільненого співробітника конфіденційною інформацією про діяльність компанії [12].

Основа проведення цих заходів полягає в тому, що звільнений співробітник повинен прийняти письмові зобов'язання про не розкриття відомостей, які були відомі йому в період його роботи на підприємствах на певній посаді відповідно до встановленого порядку, внесені до комерційної таємниці підприємства.

Ці обов'язки оформляються через розписку, яка після його оформлення залишається на підприємствах. У розписці вказані, прізвища, по батькові та назва останнього займаного посади, перераховані конфіденційні відомості, які заборонені розголошенню на певний термін або наводяться посилання на пункти списку відомостей, що належать до комерційних таємниць. Угода працівника про умови нерозголошення відомостей, зазначених у розписці, підтверджується підпискою працівника із зазначенням датою. Як правило, оформлення розписки відбувається в ході зустрічі зі співробітником компанії представником служби безпеки та режимно-серверного підрозділу [12]

Після отримання розписки здійснюється інструктаж працівника, що звільняється, за правилами поведінки після його звільнення на роботі, а

також про заборону згадувати конфіденційні відомості у зв'язку з представниками організації, що є конкурентами цього підприємства У ході навчання особлива увага приділяється питанню збереження конфіденційних відомостей щодо іноземних громадян, взаємодії у процесі спільної роботи з організаціями іноземного походження.

У разі звільнення з підприємства, переведення на роботу не пов'язаного з конфіденційними даними, співробітник повинен повернути до режимного підрозділу служби безпеки підприємства отримані раніше накопичувачі конфіденційних даних, включаючи накопичувачі магнітних дисків, номери металевих печаток, ключі сейфа та сховище.

Факт повернення підтверджується відповідним підписом відповідальної посадової особи в обхідному записі працівника, який звільняється. Заповнюючи обхідний лист, працівник отримує оформлену трудову книжку та інші документи щодо звільнення. Після отримання трудової книжки та виконання повного розрахунку з підприємством звільненого співробітника повертають до бюро пропуску на контрольний пункт при виході з підприємства пропуску для проїзду на територію, об'єкти підприємства [13, с.4].

2.6 Основні принципи, методи та методики підготовки персоналу

Існує чимало цілей для навчання співробітників:

1. підвищення робочого рівня, необхідного для роботи;

2. підтримання рівня професійної освіти;

3. підвищення професійної освіти;

4. підвищення кваліфікації персоналу під час відпусток, хвороб, звільнень та інше;

5. підвищення кваліфікації персоналу;

6. ознайомлення персоналу зі стандартами діяльності компанії, стратегіями розвитку, технологіями діяльності;

7. підвищення позитивного ставлення до роботи

Існують різні підходи для навчання співробітників.

- Самоосвіта співробітників включає вивчення спеціальних літератур, відвідування спеціальних виставок, семінарів, збирання і систематизація інформації. Головна відмінність самоосвіти від освіти додаткового характеру - те, що вона зазвичай немає системної природи і може не мати жодного відношення до стратегічних завдань компанії;
- Довгострокова додаткова підготовка персоналу, що відноситься до стратегічних завдань компанії. Це друга вища освіта, ступінь MBA та участь у тривалих навчальних програмах, тренінгах. У бізнесі таку освіту можна вважати інвестицією в персонал, який починає працювати протягом певного часу;
- Короткострокова обов'язкова підготовка персоналу, що з необхідністю підтримки технологічного процесу сучасного рівня; Короткострокові обов'язкові та додаткові тренінги персоналу з оперативних завдань компанії є великим спектром різних заходів для ефективної оперативної роботи, пов'язаної із завданнями стратегічної організації. Ця категорія включає семінари, тренінги з бізнесу, цікаві компанії на поточному етапі та у майбутньому. Це може бути цикл семінарів, конференцій та виставок, де проводиться обмін знаннями. Також можна відзначити участь спеціалістів компанії у діяльності різних професійних спільнот та клубів. Найефективнішим вважається активний спосіб підготовки персоналу. Щоб провести освітні програми, тренери, лектори можуть залучатися з боку та мати у штаті таких осіб.

Основні методи навчання:

1. **Наставництво.**

Це один із найпопулярніших, найпростіших методів організації. Наставник та співробітник обговорюють проблеми та шукають найбільш ефективні рішення. Тому можна навчити і новачків у компанії, досвідченим співробітникам, якщо потрібно ознайомлення з робочою діяльністю кваліфікаційного співробітника;

2. **Інструктаж.**

Спосіб підготовки, у якому співробітник пояснює та демонструє основи роботи на робочому місці. Часто інструктаж здійснюється керівником підприємства;

3. **Ротація.**

Засіб для того, щоб отримати нові навички та отримати інформацію. Це означає перехід з однієї посади на інше в тому самому складі. Можливість ротації у іншому відділенні підприємства. Зміна звичайного обов'язку дає можливість відкрити нові якості. Ротація позитивно позначається на інтерес до роботи і збільшує кругозір,

Розглянемо ситуацію. У процесі навчання розбираються конкретні чи можливі ситуації у процесі. Розглядається такий приклад, розглядаються варіанти розв'язання, вибираються правильні рішення;

4. **Бізнес гра.**

У процесі застосування методики виникають ситуації, що наближаються до реального стану. У рамках бізнес-ігор створені варіанти поведінки у різних ситуаціях. Це підвищує кваліфікацію співробітників для того, щоб вони правильно вели себе у найвідповідальніші ситуації;

5. Тренажери.

Популярним методом є навчання в управлінні часом, ведення переговорів тощо. Метод підготовки є першорядним методом роботи зі співробітниками підприємств, початковим етапом придбання теоретичних навичок та практичних навичок захищення конфіденційних даних у рамках посадових дій за спеціальністю [14, с.7]

За даними статистики, більше половини збитків, які компанії зазнають у зв'язку з інцидентами у сфері інформаційних технологій, пов'язані з діями працівників. І, в основному, це відбувається через погану проінформованість користувача. Таким чином, навчання персоналу є однією з основних вимог Міжнародного стандарту інформаційної безпеки ISO 27001.

Процес підготовки працівників підприємства має бути безперервним та плановим, оскільки система захисту персональних даних підприємства потребує вдосконалення та розвитку.

Завдання підготовки персоналу підприємства включають вивчення:

- нормативних документів про захист використання на підприємстві різних видів інформації;

- структури, та засоби системи захисту інформації підприємства;

- встановлених норм та правил захисту інформації підприємства, стандартів та положень служби безпеки;

- можливих загроз захисту інформації, характеру та способів їх прояву;

- порядок роботи з носіями інформації відповідно до встановлених вимог режиму конфіденційності.

Використовуються такі формі навчання:

- лекції, семінари, практичні тренінги з дії персоналу в різних ситуаціях;

- тестування співробітників, оцінка їх підготовки;

- вирішення різних завдань із захисту конфіденційних даних;

- вирішення інтелектуального завдання, спрямованої на отримання персоналом підприємства умінь прогнозувати різні ситуації, пов'язані з можливими каналами витоку даних, загрозами її безпеці;

- використання спеціальних програм навчання, призначених для підготовки лекцій, практичних тренінгів.

Працівники служби інформаційної безпеки повинні:

- мати хороші організаторські здібності створювати систему безпеки та комплексні заходи, що забезпечують безпеку підприємства;

- володіти короткою та наочною інформацією, включаючи дані в інформаційних системах,

- знання та використання технічних засобів прихованого моніторингу, спостереження та захисту інформації, включаючи дані в інформаційних системах,

- знання та використання технічних засобів прихованого моніторингу, спостереження та боротьби з корупцією,

- підготувати документи з аналізом ринку та оцінкою конкурентів, потенційних покупців;

- ведення періодичної перевірки співробітників компанії, які мають доступ до секретів.

Крім спільних програм компетентності захисту інформації, обмеженого доступу персоналу відділу управління, самостійне відділення має навчатися завданням та обов'язкам, пов'язаним із забезпеченням інформаційної безпеки в цій організації. Поглиблення навчання має залежати від загальної значущості захисту інформації, обмеженого доступу для організації та змінюватись в залежності від вимог захисту організації. Якщо необхідно, необхідно вдатися до більш фундаментального навчання, наприклад, відвідувати лекції в університеті, курси з підготовки фахівців тощо. Програми навчання з безпеки інформації повинні бути розроблені так, щоб до них були внесені всі вимоги організації захисту інформації з обмеженими можливостями доступу.

При виборі персоналу, якому необхідно пройти навчання, слід враховувати:

- основні обов'язки розробки та створення систем інформаційного захисту;

- головні обов'язки щодо забезпечення безпеки та забезпечення безпеки проектів та систем захисту інформації в обмеженому доступі;

- основні обов'язки щодо забезпечення інформаційної безпеки та контролю доступу;

Також необхідно проводити перевірку для визначення необхідності спеціального вивчення системи інформаційної безпеки у поточних, запланованих завданнях, проектах тощо.

Коли почнуться завдання або проекти з особливими вимогами до інформаційної безпеки, необхідно дбати про розробку відповідної програми навчання до безпосереднього початку та виконання її належним чином.

У загальних положеннях можуть бути такі пункти:

- Поняття про безпеку

- запобігання порушенням конфіденційної, цілісної та доступної інформації, потенційних порушень бізнес-активності організації та особистості;

- схема класифікації ризику;

- засоби захисту, супровідні навчання застосуванням засобів захисту.

Актуальна та практична робота із загально-організаційних питань: організація бізнесу компанії, інтелектуальна власність компанії, інформаційна та аналітична робота Служби безпеки, захист бізнесу компанії, основи психічного саморегулювання. Така лекція, семінар, практичні заняття, тренінги проводяться відповідальними працівниками провідних департаментів фірми, служби безпеки та запрошеними експертами.

У плані аудиторських занять мають бути передбачені такі питання:

- Правові підстави діяльності Служби безпеки;

- Правила дій персоналу Служби безпеки у разі виникнення екстремальної ситуації в денному та нічному режимі;

- Характеристики технічних пристроїв охорони та Правила дій при їх відмові або порушенні;

- процедура повідомлення представникам Закону про відповідальність за правопорушення;

- методи виявлення причин зовнішньої загрози Служби безпеки;

- прийоми та хитрощі, які застосовуються особам, які намагаються неправомірно проникнути на об'єкт;

- методи оцінки навчання співробітників підприємства у сфері захисту конфіденційних даних здійснюється диференційованим чином, залежно від категорій працівників, керівників відділів, їх керівників, працівників підприємства.

Вибирати форми та методи підготовки персоналу враховувати рівень професійної майстерності співробітника, досвід роботи за конкретними спеціальними напрямками, специфіку вирішення завдань захисту конфіденційних даних, результати моніторингу діяльності співробітника, що виконує встановлені вимоги щодо захисту даних на підприємствах. Метод інструктажу застосовується керівником підприємства та керівниками структурних підрозділів для того, щоб інформувати співробітників, які працюють з конфіденційними даними, про зміну положень заново прийняте затверджене нормативне законодавство та вимоги органів держвлади.

Особливу увагу при інструктажі має бути приділено аналізу теоретичної роботи, спрямованої на запобігання появи каналу витоку конфіденційних відомостей та запобігання виникненню загрози захисту даних. Метод індивідуальної та виховної праці полягає у систематичному, цілеспрямованому впливі на процес формування та формування особистості працівника підприємства з метою максимального використання її професійних здібностей та можливостей, бізнесу, високої моральної та іншої позитивної якості для збереження конфіденційних відомостей, що зберігаються на службі, Мета моніторингу рівня знання полягає в оцінці

знання працівників підприємств положень нормативних документів та внутрішньо корпоративних організаційних документів, що визначають рівень готовності кожного працівника до практичних завдань захисту інформації. Перевірка рівня знань здійснюється керівником підприємства, а також працівниками режимної служби, охоронної служби, підрозділу безпеки.

2.7 Оцінка якості роботи персоналу в галузі інформаційних технологій

Метод управління персоналом підприємства передбачає оцінку ефективності роботи кожного працівника підприємства із захисту конфіденційних даних, використання сукупності коштів та ресурсів підприємства. Контроль може бути періодичним плановим чи раптовим. Проводять працівники штатних відділів підприємства, які вирішують завдання щодо забезпечення захисту інформації [17].

Рис. 2.4. Форми контрольно-оцінки праці працівників, які у інформаційної сфері.

В умовах виробничих і робочих відносин, що розвиваються, вимоги якості праці постійно збільшуються, особливо в плані наукової організації трудового процесу. Якість роботи є однією з найважливіших категорій, які впливають на стабільність та ефективне функціонування організації. Розглядати якість праці та її операційний обсяг зазвичай пов'язане з вирішенням питання: як підвищити продуктивність праці, не торкаючись додаткових тимчасових та матеріальних витрат [17, с.8].

Продуктивність праці є кількісною характеристикою виконуваної роботою персоналу, що з рівнем його ефективності. Цей процес стимулює і вносить новаторські підходи до виробничої діяльності, що сприяють раціональнішому використанню праці та атестації співробітників та мотивації соціальних та економічних факторів.

Атестація персоналу - основа багатьох управлінських актів: внутрішні переміщення, звільнення, зарахування до резерву вищої посади, матеріальне та моральне заохочення, застосування санкцій, підготовка та кваліфікація, контроль, вдосконалення організації, методів та методик управління, оптимізація структури персоналу.

Під оцінкою розуміється діяльність осіб, які уповноважені на її виконання, представників адміністрацій, колективів, персональних служб, спеціалізованої зовнішньої організації, що визначає ступінь придатності людини до виконання доручених нею зобов'язань, досягнення успіху, ступінь виразності необхідних якостей роботи.

Складність аналізування управлінської діяльності полягає у не чіткій структурі, що становлять цю діяльність не можна розділити на окремі елементи, якими можна буде конкретно визначитися та вимірювати. Тому вона не має чітких виконавчих алгоритмів, хоча її функції відомі, і принципово зрозумілі. Також немає чіткого критерію аналізу управлінської діяльності. У процесі оцінки управлінського персоналу важко уникнути

суб'єктивності, заснованої на участі експертів та психологів у самій процедурі оцінки.

Атестація персоналу організації відділу є спеціальним безперервним чи періодичним формалізованим заходом, у якому оцінюється сам співробітник, його робота та результати діяльності, атестація накопичує результати діяльності конкретного співробітника протягом певного періоду. Це не порівняння між ними а порівняння із стандартом роботи дозволяє порівнювати лише те, наскільки одна робоча група більш-менш відповідає вимогам інших.

Система оцінки атестації персоналу включає три групи даних: що оцінює результати, дії, успіхи; як оцінює процедури; як оцінює методи Проблема вибору значних та незначних якостей, а також рамок допустимості та неприпустимості дозволяє вирішити розроблені кадровими службами основними процедурами та методами оцінки кадрів. Основним моментом є використання загальноприйнятих принципів у розробці нормативно-методичних матеріалів, обробці даних.

Атестація дозволяє вирішувати такі завдання щодо підготовки кадрів:

- охарактеризувати потенціал просування, знизити ризик некомпетентних працівників;

- зменшити витрати на навчання;

- забезпечити у співробітників повагу до справедливості, підвищити мотивацію праці;

- організовувати зворотні зв'язки зі співробітниками для інформування якості своєї роботи;

- розробити кадрові програми з підготовки кадрів та розвитку персоналу;

Щоб організувати ефективну систему оцінки ефективності праці, працівникам необхідно:

- встановлювати стандарти ефективності праці на кожному робочому місці, а також критерії оцінки;

- Виробляти політику оцінки ефективності праці, коли, скільки і ким проводити оцінку;

- Зобов'язати конкретних осіб проводити оцінку;

- Зобов'язати конкретних осіб, які здійснюють оцінку, зібрати дані про ефективність праці.

Зокрема, алгоритм оцінки включає:

- Виявити досягнення та проблеми співробітників;

- визначити їх сильні та слабкі сторони, якості знань, умінь, здібностей та типів поведінки, що впливають на виконання службового завдання, ступінь відповідності їх вимогам робочої посади;

- видати рекомендації щодо подолання існуючих розбіжностей та заохочення покарання, підвищення кваліфікації, розвитку.

Це має відповідати наступним критеріям: об'єктивність незалежності від особистої думки; надійності свободи від впливу на ситуацію та суб'єктивні фактори, що залежать від чіткого визначення предмета, вибору параметрів, якість та кваліфікація експертів, правдивості підходу та відсутності тиску на зовнішні фактори; достовірності результатів; орієнтованості на перспективи; комплексності; доступності інформації за критеріями та результатами.

Позитивні оцінки керівників та співробітників свідчать про соціальне значення, а позитивні оцінки споживачів та клієнтів свідчать про результативність діяльності. Загальні позитивні оцінки покращують результативність діяльності, але сприяють підвищенню їх високого рівня.

Якщо орієнтуватися на негативну оцінку, можна припустити:

- відхилення оцінки при позитивних результатах, у разі чого активність суб'єкта знижується;

- ігнорування переваг, акцентування на недоліках, які навіть у різних випадках викликають протест, і за певному повторенні провокують образу;

- негативне ставлення до результату, яке тягне за собою втрату ініціативи, бажання контактувати з керівництвом, незгоду з його обов'язками.

Атестація персоналу як аспект безпеки. Однією з цілей перевірки персоналу забезпечення безпеки є виявлення співробітників компанії в стані конфліктів внутрішньо-рольового характеру. Працюючи у компанії, кожен працівник отримує нові професійні навички, змінюються системи його цінностей та вимог.

Таке зростання супроводжується постійним виникненням внутрішніх конфліктів у співробітника на основі відповідності його самооцінці та ролі у соціальній сфері. Кожне завдання сертифікації безпосередньо стосується процесу забезпечення безпеки корпоративних організацій. У міжатестаційному періоді працівники, які продемонстрували повну відповідність займаним посадам, проводять планові тренінги та заняття у рамках між атестаційного періоду.

Загрозою безпеки фірми, яка є співробітниками, рівень знання, вміння та навички, які трохи нижче за необхідні, можна значно знизити, використовуючи корпоративне або зовнішнє навчання або перерозподіл

обов'язків у бік зменшення навантажень. Якщо вони відносяться до групи невідповідності посадам, вони повинні проходити додатковий цикл освітніх занять, виходячи з того, в якому компоненті досвіду знань, умінь, навичок, які не вистачають.

Найнебезпечнішими для безпеки організацій є члени групи, у яких рівень професійного розвитку перевищує необхідне роботи. Надмірні професійні досліди народжують самовпевненість і знижують пильність, отже, зменшують надійність працівника загалом. Співробітники зі знаннями, вміннями та навичками, які перебувають на вищих посадах, можуть бути причиною порушень системи контролю.

Професійний співробітник, як правило, знає, як треба робити, але може не правильно виконувати свою працю, оскільки деякі його монотонно нудні чи безглузді, на його думку компоненти під впливом факторів демотивації: обмежені можливості, жорстка субординація, низький соціальний статус і так далі.

Робота в галузі інформаційної безпеки обумовлена підвищеним психоемоційним навантаженням, яке може спричинити негативні особисті зміни. З метою визначення випадків професійного «вигоряння» при атестації звертають особливо увагу на негативні індивідуальні та психологічні риси:

1. характеристика слабкого типу вищої нервової дії;

2. схильність до конфлікту;

3. невротичні стани, що впливають на результати роботи та поведінки;

4. егоцентрична спрямованість особистісних інтересів;

6. некритичні ставлення до себе, до своїх справ і вчинків;

7. емоційний нестійкий стан .

Для з'ясування особистісного інтелекту та його ділових якостей як несприятливі показники розглядаються:

- несистематизований викладений кандидатом матеріал з обговорюваної проблеми,

- поверхневе судження, невідповідний аналіз факторів обговорюваної проблеми,

- неадекватний логічний аналіз факторів обговорюваної проблеми,

- неадекватні категоричні висновки, класифікації та узагальнення,

- незрозумілі та неприпустимі жарти, та ін. [19. с. 1].

У процесі перевірки позитивним ефектом є проведення однієї чи кількох змін, які атестований співробітник служби безпеки повинен виконувати у компанії, і навіть інструктора чи керівника. В даному випадку інструктор не тільки встановлює рівень професійної освіти співробітника, що перевіряється, але і, якщо це необхідно, навчає.

Особливості конкретної професії розкривають специфіку професійної діяльності та вимоги, що пред'являються до людини, описані у стандартній формі, яка називається професіограмою.

Професійна граматика - опис системи показників, які визначають професію. До неї входить перелік вимог та норм, які пред'являються цією професією або спеціальності до працівника. Наприклад, в професіограмі може бути представлений перелік санітарно-психологічних показників, які мають бути відповідними представникам конкретної професійної групи. У ньому описано особливості професії, робочого процесу, вимоги до людини загальної та спеціальної освіти, стажу, професійних навичок тощо.

Професіограми можуть бути засновані на нормативній документації інструкції та положенні або результатах дослідження дійсної групи людей. Людина, яка відповідає вимогам організації та посади робочого місця, визнається професійною придатною.

Висновки до другого розділу

Оскільки персонал підприємства створює найбільше загроз інформаційній безпеці, доцільно визначити три основні аспекти протидії загрозам на підприємстві з вини персоналу.

Насамперед, це проведення відбору потенційних кандидатів для призначення на посади, пов’язані з конфіденційною інформацією, за ускладненою процедурою. При підборі кандидатів оцінюється відповідність кожного з них таким основним вимогам як: рівень підготовки та кваліфікації, наявність необхідного досвіду роботи; морально-ділові й особистісні якості; ступінь відповідальності за прийняті управлінські та виконавські рішення (залежно від займаної посади).

Організаційні заходи при підборі персоналу, що одержує доступ до конфіденційної інформації, можна розділити на кілька груп: проведення ускладнених аналітичних процедур при прийомі і звільнення співробітників; документування добровільної згоди особи не розголошувати конфіденційні відомості та дотримуватися правил забезпечення безпеки інформації; інструктування і навчання працівників практичним діям із захисту інформації.

З огляду на те, що за статистикою основна частина інцидентів у сфері інформаційної безпеки з вини персоналу відбувається через низький рівень їх обізнаності важливим фактором запобігання загрозам інформаційній безпеці з вини персоналу є навчання усіх працівників, задіяних у цій сфері. Навчання персоналу сприяє не тільки отриманню співробітниками нових знань і навичок, необхідних для роботи та підтриманню їх професійного рівня, але й формуванню позитивного ставлення до роботи і почуття причетності до компанії, мотивації до подальшої роботи.

Процес навчання співробітників підприємства у сфері інформаційної безпеки повинен бути постійним і планомірним, включати різні форми і

методи навчання, зокрема навчання на робочому місці (наставництво, інструктування, ротація) та поза ним (лекції, тренінги, курси), короткочасне та довготривале навчання, а також самоосвіту персоналу.

Навчання має передбачати вивчення нормативно-методичних документів щодо безпеки конфіденційної інформації; структури, сил і засобів системи інформаційної безпеки; встановлених норм і правил захисту конфіденційної інформації на підприємстві; можливих загроз інформаційній безпеці підприємства, їх характеру та можливих способів прояву; порядку роботи співробітників підприємства з носіями конфіденційної інформації та реагування на інциденти інформаційної безпеки.

Основними формами контролю якості роботи персоналу підприємства у сфері захисту конфіденційної інформації є: перевірки керівництвом підприємства або службою безпеки дотримання співробітниками положень нормативно-методичних документів із інформаційної безпеки; звіти та доповіді керівників структурних підрозділів про результати роботи підлеглих співробітників; періодична атестація співробітників, допущених до конфіденційної інформації; самоконтроль співробітників.

Розділ 3

ТЕХНІЧНІ АСПЕКТИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА У КОНСПЕКТІ ПРОТИДІЇ ЛЮДСЬКОМУ ФАКТОРУ

3.1 Ідентифікація та автентифікація користувачів

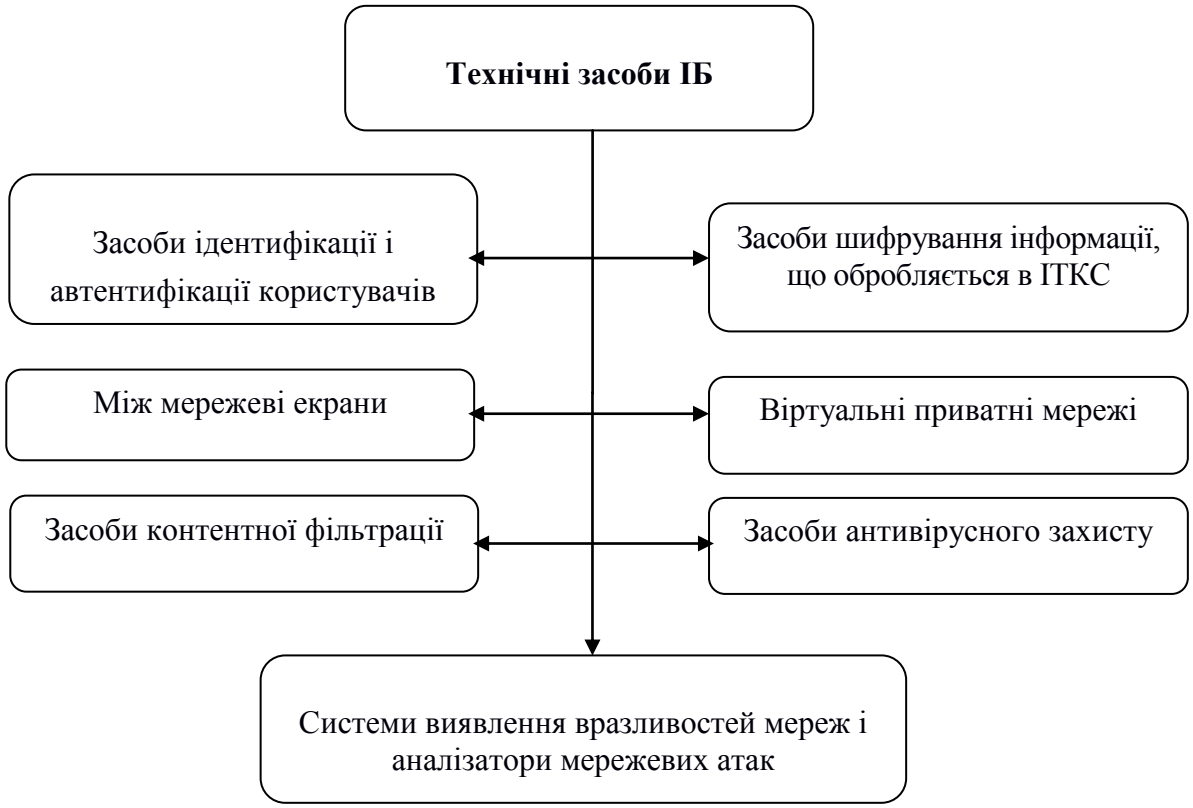

Рис. 3.1. Технічні засоби забезпечення інформаційної безпеки.

Ідентифікацію і автентифікацію можна вважати основою програмно-технічних засобів безпеки, оскільки інші сервіси розраховані на обслуговування іменованих суб'єктів. Ідентифікація та автентифікація – це перша лінія оборони, «прохідна» інформаційного простору організації.

Ідентифікація дозволяє суб'єкту (користувачеві, процесу, чинному від імені певного користувача, чи іншого апаратно-програмному компоненту) назвати себе (повідомити своє ім'я). За допомогою автентифікації друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як

синонім слова «автентифікація» іноді використовують словосполучення «перевірка справжності» [21].

Автентифікація буває односторонньою (зазвичай клієнт доводить свою справжність серверу) і двосторонньої.

Приклад односторонньої автентифікації - процедура входу користувача в систему.

Суб'єкт може підтвердити свою автентичність, пред'явивши, принаймні, одну з наступних сутностей:

– Щось, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ і тощо);

– Щось, чим він володіє (особисту картку або інший пристрій аналогічного призначення);

– Щось, що є частиною його самого (голос, відбитки пальців і т.п., тобто свої біометричні характеристики) [21].

У відкритому мережевому середовищі між сторонами ідентифікації / автентифікації не існує довіреного маршруту; це означає, що в загальному випадку дані, передані суб'єктом, можуть не збігатися з даними, отриманими і використаними для перевірки автентичності. Необхідно забезпечити захист від пасивного і активного прослуховування мережі, тобто від перехоплення, зміни та / або відтворення даних. Передача паролів у відкритому вигляді, очевидно, незадовільна; не рятує становище і шифрування паролів, так як воно захищає від відтворення. Потрібні більш складні протоколи аутентифікації.

Надійна ідентифікація утруднена не тільки через мережеві загрози, але і цілої низки інших причин.

По-перше, майже всі автентифікаційні суті можна дізнатися, вкрасти або підробити. По-друге, є протиріччя між надійністю автентифікації, з одного боку, і з зручностями користувача і системного адміністратора з іншого. Так, з міркувань безпеки необхідно з певною частиною просити

користувача повторно вводити автентифікаційні інформацію (адже на його місце могла сісти інша людина), а це не тільки клопітно, але і підвищує ймовірність того, що хтось може підглянути за введенням даних. По-третє, чим надійніший засіб захисту, тим він є дорожчий [22, с.1].

Сучасні засоби ідентифікації \ автентифікації повинні підтримувати концепцію єдиного входу в мережу. Єдиний вхід в мережу – це, в першу чергу, вимога зручності для користувачів. Якщо в корпоративній мережі багато інформаційних сервісів, що допускають належне звернення, то багаторазова ідентифікація \ автентифікація стає занадто обтяжливою. На жаль, поки не можна сказати, що єдиний вхід в мережу став нормою, домінуючи рішення поки не сформувалися.

Таким чином, необхідно шукати компроміс між надійністю, доступністю за ціною і зручністю використання й адміністрування засобів ідентифікації і автентифікації.

3.2 Між мережеві екрани та віртуальні приватні мережі

Між мережевим екраном називається програмно-апаратний або програмний елемент, який контролює на основі заданих параметрів мережевий трафік, а в разі потребі фільтрує його. Також він може називатися фаєйрволом (Firewall) або брандмауером.

Мережевий екран використовується для захисту окремих сегментів мережі або хостів від можливого несанкціонованого проникнення через уразливості програмного забезпечення, встановленого на ПК, або протоколів мережі. Робота між мережевого екрана полягає в порівнянні характеристик трафіку, що проходить крізь нього,з шаблонами вже відомого шкідливого коду [24].

Найбільш часто мережевий екран Juniper SRX300 інсталюється на кордоні периметра локальної мережі, де він виконує захист внутрішніх вузлів. Проте, атаки можуть ініціюватись зсередини, тому при атаці на сервер

тієї ж мережі, міжмереживий екран не знайде це як загрозу. Це стало причиною, з якої брандмауери почали встановлювати не тільки на кордоні мережі, але і між її сегментами, що значно підвищує ступінь безпеки мережі.

Наприклад, більшість файєрволів при аналізі трафіку послідовно порівнюють його з відомими шаблонами зі списку – очевидно, що найбільш популярні види повинні розташовуватися якомога вище. Мережевий екран – також важливий елемент захисту, який використовується для захисту окремих сегментів мережі від несанкціонованого вторгнення через уразливості програмного забезпечення.

Віртуальна приватна мережа (Virtual Private Network) створюється на базі загальнодоступної мережі Інтернет. І якщо зв'язок через Інтернет має свої недоліки, головним яких є те, що вона схильна до потенційних порушень захисту та конфіденційності, то VPN можуть гарантувати, що спрямований через Інтернет трафік так само захищений, як і передача всередині локальної мережі. У той же час віртуальні мережі забезпечують істотну економію витрат у порівнянні із вмістом власної мережі глобального масштабу [24].

VPN – це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічних віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Технологія VPN створює віртуальні канали зв'язку через загальнодоступні мережі, так звані «VPN-тунелі». Трафік, що проходить через тунелі, що зв'язують віддалені філії, шифрується. Зловмисник, що перехопив шифровану інформацію, не зможе переглянути її, оскільки не має ключа для розшифровки [25, с.1].

Підключення віддаленого користувача до VPN проводиться за допомогою сервера доступу, який підключений як до внутрішньої, так і до

зовнішньої (загальнодоступної) мережі. При підключенні віддаленого користувача (або при установці з'єднання процесу аутентифікації. Після успішного проходження обох процесів, віддалений користувач (дистанційна мережа) наділяється повноваженнями для робити в мережі, тобто відбувається процес авторизації. Класифікувати VPN рішення можна за кількома основними параметрами: типом середовища, що використовується, та способом реалізації рішення (Рис. 3.2.)

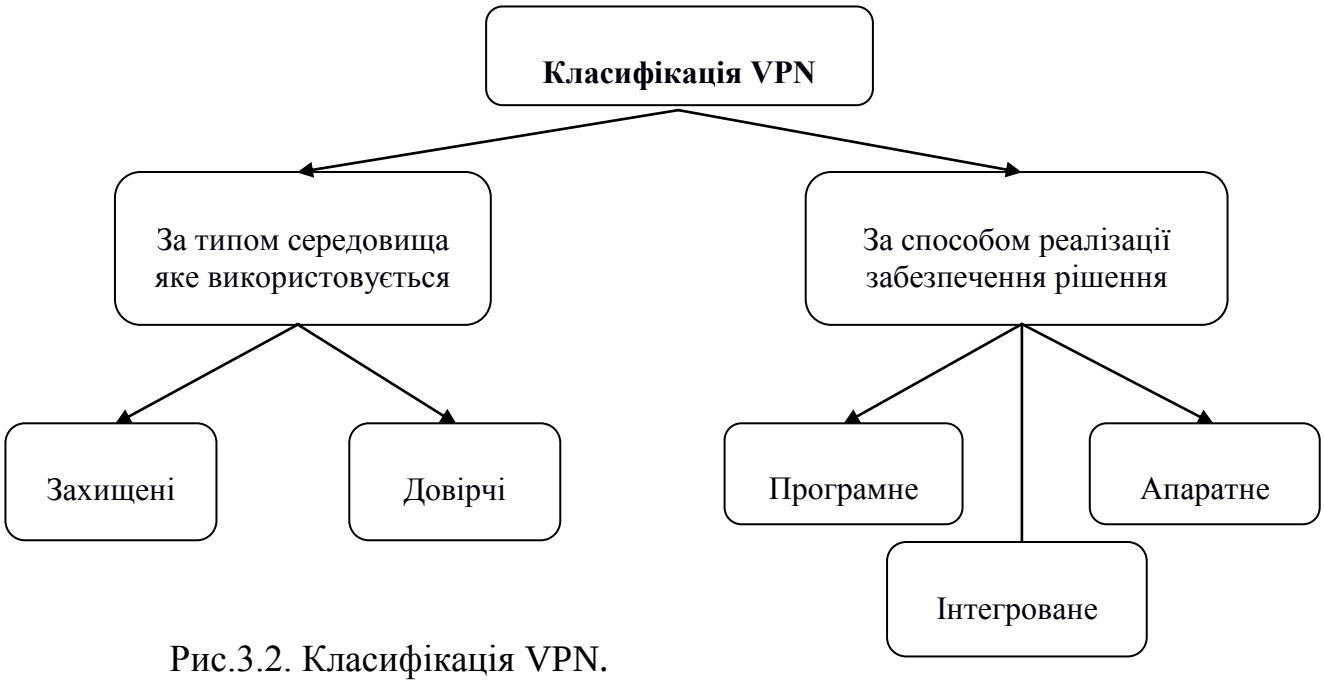

Рис.3.2. Класифікація VPN.

За способом реалізації VPN бувають у вигляді:

Спеціального програмно-апаратного забезпечення. Реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий ступінь захищеності.

Програмного рішення. Використовують персональний комп'ютер зі спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

Інтегрованого рішення. Функціональність VPN забезпечує комплекс, вирішальний також задання фільтрації зв'язку, організації мережевого екрану і забезпечення якості обслуговування.

Отже, VPN забезпечує:

- Захищенні канали зв’язку за ціною доступу в Інтернет, що в кілька разів дешевше виділених ліній;
- При установці VPN не потрібно змінювати топологію мереж, переписувати програми, навчати користувачів – все це значна економія.
- Забезпечується масштабування, оскільки VPN не створює проблему росту і зберігає зроблені інвестиції;
- Незалежність від криптографії і можливість використовувати модулі криптографії будь-яких виробників у відповідності з національними стандартами тієї чи іншої країни;

До недоліків VPN можна віднести порівняно низьку надійність [25, с.2].

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. На думку аналітиків, це не зупинить VPN, оскільки це не суттєво для більшості користувачів.

3.3 Засоби контентної фільтрації

Зростання кількості і обсягів ресурсів мережі Інтернет обумовлює необхідність пошуку нових ефективних методів для вирішення завдання обмеження доступу до ресурсів мережі, які є джерелом надмірного трафіку. Надмірний об’єм широкомовного трафіку погано впливає на кінцеві станції, які визначають, чи потрібні їм цей трафік. Вживання заходів по виправленню або усуненню причин, які лежать в основі цього явища, може підвищити продуктивність роботи мережі і допоможе уникнути подальших проблем.

Проте без відповідальних інструментів і методів усунення несправностей ця робота може затягнутися надовго. До джерел небажаного або надмірного трафіку, по-перше, відносяться сторінки розважальних

порталів, сайтів знайомств, Peer to Peer (P2P) застосувань, послуги ICQ або Skype [26].

По-друге, існує ще декілька категорій сайтів: так звані «сайти для дорослих», екстремістські і інші сайти з сумнівним інформаційним змістом. Відвідування подібних сайтів співробітниками організацій в робочий час часто є прямим порушенням корпоративного регламенту, оскільки в результаті доступу до нецільової інформації витрачаються мережні ресурси (наприклад, трафік), а також робочий час співробітників організації. Крім того, багато розважальних сайтів сприяють розповсюдженню шкідливих програм (використовуючи вразливості Web-браузерів або пропонуючи користувачам посилання на «закачування» неперевіреного або неліцензійного програмного забезпечення). Окрім цього при експлуатації корпоративної телекомунікаційної мережі можуть епізодично виникати ситуації порушення режиму нормального функціонуванням каналів мережі, зокрема – зовнішнього.

Вказані ситуації можуть спричинити відмову в роботі служб окремих комп’ютерах, під мережах і мережі в цілому. Часто такі перевантаження не є наслідком навмисної атаки на мережу або вірусної активності, а виникають при роботі на деяких комп’ютерах тих або інших мережних застосувань, що створюють надмірне навантаження на канали мережі. При цьому причини нестабільної роботи мережі досить важко діагностувати. Відзначимо, що досить часто застосування, які створюють аномальне навантаження на канали, є «непрофільними» для корпоративної мережі. Вони не використовуються для вирішення тих або інших інформаційно_--обчислювальних задач власника мережі. Тому завдання виявлення факту наявності непрофільного трафіку, а також комп’ютерів, які є джерелами або споживачами вказаного трафіку – вельми актуальне.

Шляхом обмеження мережної активності таких комп’ютерів технічними або адміністративними заходами можливе виключення аномального завантаження каналів трафіком цих комп’ютерів.

Пірінгові мережі, як основне джерело надмірного трафіку. Торент, як і багато інших пірінгових мереж, повністю заблокувати непросто: концепція цієї технології така, що за бажанням можна скористатися масою обхідних маневрів і маленьких хитрощів, що дозволяють обійти як прямі, так і непрямі заборони.

Взагалі, розглядаючи можливі методи блокування небажаного трафіку, можна виділити в два ключові підходи:

– Індивідуальний

– Груповий, або мережевий

Методи аналізу трафіку. Існуючи системи обмеження доступу до мережних ресурсів мають можливість перевіряти на відповідність заданим обмеженням не лише окремі пакети, але і їх зміст.

У даний час в системах контентної фільтрації застосовуються наступні методи фільтрації Web-контенту: на ім'я DNS або конкретної IP-адреси, за ключовими словами Web-контенту і за типом файлу.

Щоб блокувати доступ певного Web-вузла або групі вузлів, необхідно задати безліч URL, контент яких є небажаним. URL-фільтрація забезпечує ретельний контроль безпеки мережі. Однак не можна передбачити наперед всі можливі неприйнятні UPL - адреси. Крім того, деякі Web-вузли з сумнівним інформаційним наповненням працюють не з URL, а виключно з IP-адресами. Виявлення непрофільного трафіку може виконуватись з використанням засобів класифікації мережевого трафіку за типами додатків, що генерують цей трафік [26].

Методи аналізу змісту пакетів можна розділити за місцем знаходження сигнатури: в заголовках мережевого, транспортного або прикладного рівнів або в корисному навантаженню пакету. Аналіз сигнатури являє собою перевірку відповідності налаштувань системи і активності користувача з базою даних відомих атак, що постачається продавцем.

Додаткові сигнатури, встановлені клієнтом, також можуть бути додані як частина процесу конфігурації системи виявлення атак.

Найбільш поширеним методом цього типу є метод ідентифікації прикладного протоколу за відомим номером використовуваного ним порту [27, с.1]. Цей метод має як явні переваги, так і певні недоліки. Основною перевагою методу є його «швидкодія». У той же час і точність класифікації всупереч інтуїтивним очікуванням найчастіше виявляється невисокою. Це пов’язано з тим, що деякі мережні додатки «маскуються» від розпізнавання цим методом шляхом використання портів, які стандартно використовуються іншими широко відомими застосуваннями. Загальним недоліком усіх сигнатурних методів є складність розширення набору сигнатур при виявленні того, що використовуваний набір не забезпечує розпізнавання деякого нового класу трафіку. Для виконання такого розширення потрібні досить великі трудовитрати кваліфікованих фахівців. Методи другого типу застосовані на використані статистичного аналізу трафіку мережевих з’єднань. Ці методи, в свою чергу, поділяються на методи аналізу особливостей поведінки вузлів мережі і засновані на аналізі особливостей інформаційних потоків між мережевими додатками. Всі різновиди, що засновані на методах класифікації трафіку, вимагають їх попереднього «навчання» заздалегідь підготовлених даних.

За результатами аналізу розглянутих методів і засобів кваліфікації трафіку далі буде запропоновано методи обмеження трафіку мережевих додатків.

Програмні засоби контролю трафіка і управління доступом до мережі. Існують декілька способів заборони доступу на певні сайти. Розглянемо кожен з них детальніше.

Найпростіший спосіб – це створення фіктивного DNS-запису. На комп’ютері, звідки здійснюється доступ в Інтернет, редагується текстовий файл hosts, який знаходиться в папці c:\windows\system32\ drivers\etc\, що містить список DNS-імен сайтів, до яких закривається доступ.

Мінус цього методу – в необхідності примусового налаштування браузерів клієнтських комп'ютерів на використання проксі-сервера. Крім того, необхідно передбачити, щоб користувачі не користувалися Internet в обхід проксі-сервера та не використовували анонімні проксі-сервери [27, с.2].

3.4 Засоби захисту комп'ютерних вірусів та їх особливості

Для захисту від різноманітних вірусів існує декілька видів антивірусів, які за своїм призначенням поділяють на детектори, фаги, ревізори, фільтри та вакцини. Розглянемо їх характеристики більш докладно.

Детектори (сканери) – перевіряють оперативну або зовнішню пам'ять на наявність вірусу за допомогою розрахованої контрольної суми або сигнатури і складають список ушкоджених програм. Якщо детектор-резидентний, то програма перевіряється і тільки в разі відсутності вірусів вона активується. Детекторами є, наприклад, програма MS AntiVirus.

Фаги (поліфаги) – виявляють та знешкоджують вірус (фаг) або кілька вірусів. Сучасні версії поліфагів, як правило, можуть проводити евристичний аналіз файлу, досліджуючи його на наявність коду, характерного для віруси (додання частини однієї програми в іншу, шифрування коду тощо). Фагами є, наприклад, програми Aidstest, DrWeb.

Дуже часто функції детектора та фага суміщені в одній програмі, а вибір режиму роботи здійснюється завданням відповідних параметрів (опцій, ключів). На початку вірусної ери кожний новий вірус визначався та лікувався окремою програмою. При цьому для деяких з вірусів (наприклад,VIENNA) цих програм було не менше десятка. Згодом окремі програми почали виявляти та лікувати декілька типів вірусів, тому їх стали звати полідекторами та поліфагами відповідно.

Сучасні антивірусні програми знаходять і знешкоджують багато тисяч різновидів вірусів і заради простоти їх звуть коротко детекторами та фагами. Серед детекторів та фагів найбільш відомими та популярними є програми

Aidstest, DrWeb (фірма «Диалог Наука», Росія), Scan, Clean (фірма McAfee Associates, США), Norton AntiVirus (фірма Symantec Corporation, США). Ці програми періодично поновлюються, даючи користувачеві змогу боротися з новими вірусами.

Ревізори – програми, що контролюють можливі засоби зараження комп'ютера, тобто вони можуть виявити вірус, невідомий програмі. Ці програми перевіряють стан BOOT-сектора, FAT – таблиці, атрибути файлів. При створенні будь-яких змін користувачеві видається повідомлення (навіть у разі відсутності вірусів, але наявності змін).

При першому запуску ревізор утворює таблиці, куди заносить інформацію про вільну пам'ять, Partition Table, Boot-сектор, директорії, файли, що містяться у них, погані кластери тощо. При повторному записку ревізор сканує пам'ять та диски і видає повідомлення про всі зміни, що відбулися у них з часу останнього сеансу ревізії. Нескладний аналіз цих змін дозволяє надійно визначити факт зараження комп'ютера вірусами. Серед ревізорів найбільш популярно є програма Adinf [28] .

Свого часу, коли не було надійних засобів боротьби з вірусами, широкого поширення набули так звані фільтри. Ці антивірусні програми блокують операцію записування на диск і виконують її тільки при вашому дозволі. При цьому легко визначити, чи то ви санкціонували команду на запис, чи то вірус намагається щось заразити. До числа широко відомих свого часу фільтрів можна віднести програми VirBlk, FluShot та ін. Зараз фільтри майже не використовують, оскільки вони, по-перше, дуже зручні, бо відволікають час на зайвий діалог, по-друге, деякі віруси можуть обманювати їх.

Сторожі – резидентні програми, які постійно зберігаються у пам'яті комп'ютера й у визначений користувачем час перевіряють оперативну пам'ять комп'ютера, файли, BOOT-сектора, FAT-таблицю. Сторожем є, наприклад, програма AVP.

Вакцини – це програми, які використовуються для оброблення файлів та завантажувальних секторів з метою передчасного виявлення вірусів.

Існують три рубежі захисту від комп'ютерних вірусів:

1. Запобігання надходженню вірусів.
2. Запобігання вірусній атаці, якщо вірус усе-таки потрапив у комп'ютер.
3. Запобігання руйнівним наслідкам [28, с.3]

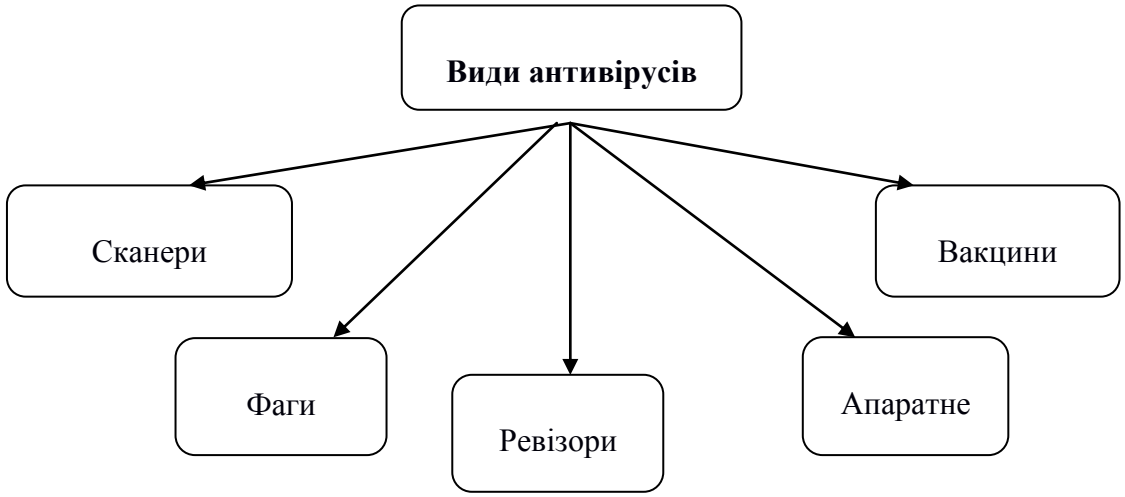

Рис. 3.3 Види антивірусів:

Є три методи реалізації рубіжної оборони:

- Програмні методи захисту;
- Апаратні методи захисту;
- Організаційні методи захисту.

Основним засобом захисту інформації є резервне копіювання найцінніших даних. У разі втрати інформації внаслідок будь-якої з названих вище причин, жорсткий диск треба відформувати й підготувати до нової експлуатації. На «чистий» диск установлюють операційну систему з дистрибутивного компакт-диска, потім під її керуванням треба встановити все необхідне програмне забезпечення, яке теж беруть з дистрибутивних носіїв. Відновлення комп'ютера завершують відновленням даних, які беруть з резервних носіїв [29, с.4].

Створюючи план заходів з резервного копіювання інформації, необхідно враховувати, що резервні копії повинні зберігатися окремо від комп'ютера. Тобто, наприклад, резервне копіювання інформації на окремому жорсткому дискові того самого комп'ютера лише створює ілюзії безпеки. Відносно новим і досить надійним методом зберігання даних є зберігання їх на віддалених серверах в Інтернеті. Є служби, які безплатно надають простір для зберігання даних користувача.

Одними з основних захистів інформації є антивірусні програми та засоби апаратного захисту. Так, наприклад, просто відключення перемички на материнській платі не дозволить здійснити стирання перепрограмованої мікросхеми ПЗП, незалежно від того, хто буде намагатися зробити це: комп'ютерний вірус чи неакуратній користувач.

Існує досить багато програмних засобів антивірусного захисту, їхні можливості такі:

1. Створення образу жорсткого диска на зовнішніх носіях. У разі виходу з ладу інформації в системних ділянках жорсткого диска, збережений «образ диска» може дозволити відновити якщо не всю інформацію, то принаймні її більшу частину. Цей засіб може захистити від утрати інформації під час апаратних збоїв та неакуратного формування жорсткого диска.

2. Регулярне сканування жорсткого диска в пошуках комп'ютерних вірусів. Сканування звичайно виконують автоматично під час кожного ввімкнення комп'ютера або при розміщені зовнішнього диска у зчитувальному пристрої. Під час сканування треба мати на увазі, що антивірусна програма шукає вірус шляхом порівняння коду програми з кодами відомих їй вірусів, що зберігаються в базі даних. Якщо база даних застаріла, а вірус є новим, то програма сканування його не виявить. Для надійної роботи варто регулярно оновлювати антивірусну програму. Так, наприклад руйнівні наслідки атаки вірусу W95.CIM.1075 («Чорнобиль»), який знищив інформацію на сотнях тисяч комп'ютерів.

3. Контроль за змінами та розмірів інших атрибутів файлів. Оскільки на етапі розмноження деякі комп'ютерні віруси змінюють параметри заражених файлів, програма контролю може виявити їх діяльність і попередити користувача.

4. Контроль за зверненням до жорсткого диска. Оскільки найбезпечніші операції, пов'язані з діяльністю комп'ютерних вірусів, так чи інакше спрямовані на модифікацію даних, записаних на жорсткому дискові, антивірусні програми можуть контролювати звернення до нього та попереджати користувача щодо підозрілої активності [29, с.5].

3.5 Рекомендації щодо забезпечення інформаційної безпеки на підприємстві

З розвитком інформатизації, яка спостерігається останніми роками, з'явилась ще одна глобальна проблема – інформаційна безпека. Цілеспрямовані або навмисні дії з боку зовнішніх або внутрішніх джерел можуть задавати шкоду цим інтересам і становлять реальну загрозу для подальшої діяльності підприємства. Все більше керівників розуміють, наскільки небезпечна може бути інсайдерська інформація, система обробки інформації і дії співробітників, які беруть участь у діяльності підприємства.

Згідно цього необхідно надати рекомендації щодо забезпечення інформаційної безпеки на підприємстві будуть наступними:

Для регулювання безпеки на підприємстві має створюватися служба інформаційної безпеки, що має виявляти, а також демонструвати власникам підприємства весь спектр загроз в інформаційній сфері.

Завдання керівників служби переконати, що протистояти загрозам можна тільки на основі створення і упровадження ефективних систем захисту інформації.

Виділимо найпоширеніші види потенційних загроз безпеці діяльності підприємства у сфері інформаційних технологій зображених на Рис. 3.3:

- Відсутність регламентованого доступу до файлів даних;
- Вільне втручання в програмне забезпечення;
- Відсутність протоколювання змін у програмному забезпеченні;
- Відсутність дублювання важливих документів на документальних носіях даних;

Рис. 3.3. Найпоширеніші види потенційних загроз

Для досягнення задовільного рівня інформаційної безпеки на підприємстві необхідно застосувати комплекс організаційних і технічних заходів, спрямованих на захист даних.

Організаційні заходи включають документовані процедури і правила роботи з різними видами інформації, IT-сервісами, засобами захисту і т. д.

Технічні заходи полягають у використанні апаратних і програмних засобів контролю доступу, моніторингу витоків, антивірусного захисту між мережевого екранування, захисту від електромагнітних випромінювань.

Створюючи системи захисту на підприємстві, необхідно враховувати, що, для ефективного захисту інформаційних ресурсів потрібна реалізація різноманітних заходів, які можна розподілити на три групи: Юридичні, організаційно-економічні й технологічні. Завдання забезпечення інформаційної безпеки необхідно вирішувати системно.

На сьогоднішній день рекомендовано використовувати такі основні способи захисту: управління, примус, спонукання.

Усі перераховані методи націлені на побудову ефективної технології захисту інформації.

Під перешкодою розуміється спосіб фізичного захисту інформаційних систем, завдяки якому зловмисники не мають можливості потрапити на територію, що охороняється.

– Маскування – способи захисту інформації, що передбачає перетворення даних у форму, не придатну для сприйняття сторонніми особами. Для розшифровки потрібне знання принципу та ключ.

– Управління – способи захисту інформації, при яких здійснюється управління над всіма компонентами інформаційної системи.

– Регламентація – найважливіший метод захисту інформаційних систем, що припускає введення особливих інструкцій, згідно з якими повинні здійснюватися всі маніпуляції з даними, що охороняються.

– Примус – методи захисту інформації, тісно пов’язані з регламентацією, що припускають введення комплексу заходів, при яких працівники змушені використовувати встановлені правила.

Для зберігання втрати та витоку таємних даних рекомендую використовувати засоби:

– Фізичні;

- Апаратні;
- Програмні;
- Апаратно-програмні;
- Законодавчі;
- Криптографічні та організаційні методи.

Фізичні засоби захисту – це засоби які необхідні для зовнішнього захисту засобів обчислювальної техніки, території на об’єктів. Їх реалізують на базі ЕОМ, які спеціально призначені для створення фізичних перешкод на можливих шляхах проникнення і несанкціонованого доступу до інформаційних систем, що захищаються.

Апаратні засоби захисту – це електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, тощо.

Програмні засоби захисту, які вмонтовані до складу програмного забезпечення системи, необхідні для виконання логічних та інтелектуальних функцій захисту.

Апаратно-програмні засоби захисту – це засобі, які основані на синтезі програмних та апаратних засобів.

Законодавчі засоби – це комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку конфіденційної інформації.

Що стосується практики захисту конфіденційної інформації на друкованих носіях, то проконтролювати такі носії технічно складніші, ніж електронні. Після виходу паперового документа з принтера стежити за ним можна лишу «вручну», за допомогою спеціально навчених спеціалістів та організаційних процедур.

Програмно-технічні методи захисту, які дешевші, перестають працювати. До того ж діючі засоби захисту від витоків інформації не контролюють такий канал, як надсилання на друк. І тут конфіденційна інформація виходить з-під контролю. Типовий «паперовий» витік – це збій або навмисна помилка співробітника при автоматичному роздрукуванні листів, адресованих великому числі клієнтів. Як відомо, адреса на листі або конверті друкується теж автоматично, часто і конверти заклеює автомат.

Для того щоб знизити кількість «паперових» витоків та підвищити рівень захисту конфіденційної інформації на друкованих носіях, необхідно реалізувати заходи за двома ключовими напрямками:

– По-перше, необхідна установка DLP-системи, яка блокує відправку на друк недозволеної інформації та перевіряє відповідність поштової адреси та адресата;

– По-друге, необхідно комплекс організаційних заходів щодо вдосконалення обліку руху паперових документів з конфіденційною інформацією.

До складу принципів організації обліку паперових документів з конфіденційною інформацією додати такі:

– Принцип комплексності згідно з яким при побудові систем захисту облікових необхідно передбачати прояв усіх видів можливих загроз включаючи канали несанкціонованого доступу до конфіденційної інформації на друкованих носіях, та всі можливі засоби захисту;

– Принцип безпеки та контролю даних, який передбачає захист друкованою інформації шляхом встановлення обмеження користувачів, віднесення до інформації конфіденційного характеру та введення обмежень при роботі з нею;

– Принцип адекватності, застосування вищезазначених заходів захисту слід об’єднувати з можливими видами загроз, а засоби захисту на друкованих носіях мають функціонувати у межах єдиного комплексу захисту

конфіденційної інформації, взаємно доповнюючи одне-одного у функціональному і технічному аспектах. Відповідальність за захист даних на друкованих носіях , що становлять комерційну таємницю, необхідно покладати як на службу безпеки, так і на весь персонал, необхідно вживати відповідні заходи, диференціюючи їх відповідно д певних загроз;

– Формування правових умов захисту інформації, шляхом розробки нормативно-правових документів захисту всіх видів інформації , якими повинні керуватися взаємини;

– Забезпечення контролю за паперовими носіями інформації, перш за все працівниками у частині дотримання ними встановленого режиму захисту інформації, своєчасне реагування на всі порушення захисту інформації;

– Впровадження надійної системи документообігу, що виключає можливість несанкціонованого доступу до документів, їх втрати, знищення або модифікації;

– Забезпечення надійної охорони з метою унеможливлення доступу до інформації, винесення документів або їх копій;

– Підвищення кваліфікації персоналу в галузі економічної та інформаційної безпеки;

– Підвищення прозорості звітності та посилення вимог щодо забезпечення достовірності інформації, проведення зовнішнього та внутрішнього аудиту.

Чільне місце в організації надійного захисту конфіденційної інформації в усній формі відводиться роботі з кадрами. Фахівці вважають що збереження секретних даних, отриманих в усній формі а 80% залежить від правильного підбору розміщення та виховання кадрів. Цю роботу слід розпочинати з дня прийому людини на роботу, другим за важливістю є обмеження доступу до секретної інформації. Роботу необхідно організувати таким чином, щоб кожний співробітник мав доступ тільки до інформації, яка

необхідна йому в процесі виконання його обов'язків. Цей захід не зможе повністю захистити від можливого витоку інформації, але дозволить звести можливу школу до мінімуму.

Третім напрямом у роботі з кадрами є проведення виховних робіт та мотивації працівників, у зв'язку з цим доцільно дати так рекомендації:

– Використовувати будь-яку можливість пропагувати програми забезпечення режиму секретності;

– Різнобічно стимулювати зацікавленість працівників у виконанні режиму таємності;

– Періодично винагороджувати працівників за успіхи в захисті секретної інформації.

Зазначимо, самі заклики не дають позитивних результатів, тому значне місце у виховній роботі відводять навчанню, метою якого є:

– Знання працівником обсягів інформації, за безпеку якої він несе особисту відповідальність;

– Розуміння виконавцем суті конфіденційних відомостей, характеру та цінності даних, з якими він працює;

– Навчання правилам зберігання та захисту секретних даних.

Значну роль відіграє вміння вести перемовини, співробітник повинен чітко знати, яку інформацію він має право повідомити партнеру з перемовин, а яку – ні. Виходячи з можливості перехоплення мовної інформації під час проведення розмов конфіденційного характеру за допомогою впровадження закладених пристроїв, акустичних, віброакустичних та лазерних технічних засобів розвідки, протидія цим загрозам має здійснюватися всіма доступними засобами та методами. Зокрема у процесі захисту передачі усної інформації за допомогою ліній телекомунікацій, доцільно застосувати методи аналогового скремблювання та дискретизації мови з наступним шифруванням.

Візьмемо для прикладу уявне підприємство і запровадимо рекомендації:

1. Прохідна підприємства має бути оснащена турнікетом або засобом контролю щоб контролювати доступом персоналу до підприємства, а працівники мають відповідно мати ідентифікаційні картки.

2. Кожний працівник має мати своє особисто-закріплене місце. Це потрібно для того, щоб персонал якщо і допустить помилку, то можна було швидко визначити з якого комп'ютера було це зроблено.

3. На кожному комп'ютері необхідно створити акаунт користувача під паролем і тримати його в секреті, як тільки потрібно зайти в акаунт, потрібно пройти автентифікацію, тобто система має перевірити чи паролі збігаються, якщо так – система пропускає. У разі 3 неправильних вводів, акаунт блокується

4. На кожному комп'ютері встановити програму, яка не буде давати можливості займатися сторонніми справами під ас робочого дня.

5. Персоналу має бути надана тільки та інформація, з якою він працює, то якщо умовно інформація надана на період необхідності користування, а при його закінченні, вона блокується.

6. Відділ кадрів має підбирати такий персонал, який знається на роботі з конфіденційною інформацією.

7. З кожним працівником необхідно підписати контракт про нерозголошення конфіденційної інформації, в разі розголошення робітник може бути притягнутим до відповідальності.

8. Важливо навчати персонал, як працювати з програмним забезпеченням або проводити курси для підвищення кваліфікації. Це мінімізує ризик того, що працівники по необізнаності допустять помилку, що призведе до втрати інформації.

На рівні роботи з персоналом розроблено такі рекомендації:

1. Прийняття внутрішніх актів, що встановлюють перелік відомостей, що становлять комерційну таємницю, порядок доступу до неї,

правила використання даних та запобігання незаконному розголошенню; доповнення існуючої політики інформаційної безпеки відповідними пунктами, що регулюють питання використання як корпоративних, та і приватних мобільних телефонів, комп'ютерів, електронної пошти та інших засобів комунікації.

2. Проведення профілактичної роботи, що включає мотивацію та виховання у кожного працівника дбайливого та відповідального ставлення до інформації, що використовується в роботі. Розробка та реалізація організаційних заходів, що полягають у проведенні регулярних тренінгів персоналу з дотриманням політики та безпеки поводження з різними документами, відповідно до категорії конфіденційності.

3. Доповнення трудових договорів з працівниками відповідними пунктами , що є так званими угодами про «не конкуренцію» які встановлюють для працівників певні обмеження по роботі на конкурентів у разі звільнення, тим самим обмежуючи можливості витоку інформації.

4. Запровадження певних штрафних санкцій за те, що не повідомлено про певний інцидент: нетиповий інтерес до конфіденційної інформації, розголошення таємниці, саботаж, несанкціонований доступ до документів та баз даних.

На мою думку сьогодні питання безпеки інформації слід розглядати не просто як розробку приватних механізмів захисту, а як реалізацію системного підходу, що включає комплекс взаємопов'язаних заходів, які мають розширюватись та вдосконалюватись. Тому впровадження регламентів інформаційної безпеки при використанні телекомунікацій, дотримання персоналом внутрішніх нормативних актів, а також досягнення конфіденційності, цілісності та доступності усної інформації, дозволять не тільки підвищити ефективність системи інформаційної безпеки, а й сприятимуть зміцненню зовнішніх позицій.

Висновки до третього розділу

Встановлено, що на сьогоднішній день існує багато технічних засобів забезпечення інформаційної безпеки підприємства, серед яких засоби ідентифікації і автентифікації користувачів; засоби шифрування інформації, що зберігається на комп'ютерах і що передається по мережах; між мережеві екрани; віртуальні приватні мережі; засоби контентної фільтрації; засоби антивірусного захисту; системи виявлення вразливостей мереж і аналізатори мережевих атак.

Ідентифікацію і автентифікацію можна вважати основою програмно-технічних засобів безпеки. Ідентифікація та автентифікація - це перша лінія оборони інформаційного простору організації, тому їм потрібно приділяти значну увагу.

Очевидно, найзручнішим засобом захисту на даний час є віртуальні приватні мережі, саме через їх порівняно невисоку вартість і економію часу, а також зручність і простоту використання.

Засоби контентної фільтрації повинні використовуватись на кожному підприємстві. Окрім своєї основної функції - захисту, це допоможе дисциплінувати співробітників та підвищити продуктивність за рахунок унеможливлення займатись сторонніми справами на робочому місці.

Засоби захисту від комп'ютерних вірусів також займають одну з основних позицій серед усіх засобів від несанкціонованого доступу до інформації, оскільки спроби злому, викрадення інформації здійснюються за допомогою шкідливих програм. Тому що на даний час це є найбільш відомим способом викрадення та пошкодження інформації.

ВИСНОВКИ

Отримані у процесі дослідження результати дають підстави стверджувати про досягнення поставленої мети, реалізацію визначених завдань та зробити такі головні висновки: Забезпечення інформаційної безпеки підприємства – 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.

До основних методів забезпечення інформаційної безпеки підприємства відносять: правові, організаційні та програмно-технічні заходи. Правові методи включають сукупність нормативно-правових актів, які регулюють відносини, пов'язані з використанням інформації в діяльності підприємства. Програмно-технічні методи реалізуються за допомогою засобів програмного та апаратного забезпечення. Організаційні методи полягають в забезпеченні збереження конфіденційної інформації підприємства шляхом формування корпоративної системи захисту.

Встановлено, що під загрозою ІБ підприємства розуміють явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію бізнес-інтересів в інформаційній. Серед основних видів загроз ІБ виділяють: природні, техногенні та антропогенні; реальні та потенційні; закономірні та випадкові; допустимі та недопустимі; навмисні та ненавмисні; зовнішні та внутрішні.

Внутрішніми загрозами ІБ підприємства, тобто загрозами з вини персоналу є дії чи бездіяльність (навмисні чи не навмисні) співробітників, що шкодять інтересам діяльності підприємства, наслідком яких може бути нанесення економічних збитків компанії, втрата інформаційних ресурсів, тощо.Внутрішні загрози об’єктам інформаційної безпеки підприємства за способом впливу можуть бути об’єднані в п’ять груп: інформаційні, фізичні, організаційно-правові, програмно-математичні, радіоелектронні.

Оскільки персонал піприємства створює найбільше загроз інформаційній безпеці, необхідно визначити три основні аспекти протидії загрозам на підприємстві з вини персоналу: проведення відбору потенційних кандидатів для призначення на посади, пов’язані з конфіденційною інформацією; постійне навчання усіх працівників, задіяних у сфері інформаційної безпеки; контроль якості праці персоналу та її оцінювання.

На сьогоднішній день існує безліч технічних засобів забезпечення інформаційної безпеки: засоби ідентифікації і автентифікації користувачів; засоби шифрування інформації, що обробляється в ІТКС; між мережеві екрани; віртуальні приватні мережі; засоби контентної фільтрації; засоби антивірусного захисту; системи виявлення вразливостей мереж і аналізатори мережевих атак.

Ідентифікацію і автентифікацію можна вважати основою програмно-технічних засобів безпеки. Ідентифікація та автентифікація - це перша лінія оборони інформаційного простору підприємства, тому їм потрібно приділяти значну увагу. Очевидно, найзручнішим засобом захисту на даний час є віртуальні приватні мережі, саме через їх порівняно невисоку вартість і економію часу, а також зручніть використання.

Засоби контентної фільтрації мають використовуватись на кожному підприємстві. Окрім своєї основної функції - захисту, це допоможе дисциплінувати співробітників та підвищити продуктивність за рахунок відсутньої можливості займатись сторонніми справами на робочому місці.

Засоби захисту від комп'ютерних вірусів також займають одну з основних позицій серед усіх засобів від несанкціонованого доступу до інформації, оскільки спроби злому та викрадення інформації здійснюються за допомогою шкідливих програм, вірусів. Адже на данний час це є найпоширенішим та найзручнішим способом викрадення та пошкодження інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фурашев В. М. Питання законодавчого визначення понятійно-категорійного апарату у сфері інформаційної безпеки: 46 – 56 с.

2. Гуцу С. Ф. Правові основи інформаційної діяльності: навч. посіб. Харків, 2009. 48 с.

3. Литвиненко О. В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах: 1997. 18 с.

4. Тацюра М. Ю. Проблемні аспекти стандартизації у галузі інформаційної безпеки підприємства. Сімферополь, 2010. 451 - 453 с.

5. Матиєв Д. Засоби захисту інформації : проблема вибору і відповідності URL: http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/

6. Аніловська Г. Я. Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій: URL: http://www.nbuv.gov.ua/portal/chem_biol/nvnltu/18_9/270_Anilowska_18_9.pdf

7. Легомінова С. В. Теоретичні засади інформаційної безпеки підприємства: 2015. 87 – 92 с.

8. Євдоченко Л. О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації: 2011. 24 с.

9. Фатьянов А. А. Правове забезпечення безпеки інформації в РФ : навч. посібник. 2001. 412 с.

10. Закон України Про інформацію: *Відомості Верховної Ради України.* 1992. Ст. 650

11. Капіца Ю. М., Цвєткова В. В., Кубко Є.Б. Проблеми правової охорони комерційної таємниці, ноу-хау та конфіденційної інформації в праві України : Салком, 2000. 296 с.

12. Алексенцев А. І. Про класифікацію конфіденційної інформації за видами таємниці: 1999. 42 - 45 с.

13. Суханов Е. А. Цивільне право : 1998. 816 с.

14. Андрощук А. Секретна інформація як об’єкт правової охорони : 1999. 27-32 с.

15. Ортинський В. Л., Керницький І. С. Контроль персоналу. Економічна безпека підприємств організацій та установ : навч. посіб. 2009. URL: http://pidruchniki.com/ 1734030851318/ekonomika/kontrol_personalu.

16. Печенюк А. Особливості організації інформаційної безпеки сучасного підприємства. Інститут бухгалтерського обліку, контроль та аналіз в умовах глобалізації : 2014. 165 – 168 с.

17. Скляренко А. К. Загрози витоку інформації через персонал. Автоматизований інформаційнй аналіз : веб-сайт. URL: http://analiz.at.ua/publ/informacija/zakhist_informaciji/zagrozi_vitoku_informaciji_cherez_personal/3-1-0-32.

18. Програмні засоби захисту від комп’ютерних вірусів : URL: https://sites.google.com/site/siteallaboutviruses/programni-zasobi-zahistu-vid-komp-uternih-virusiv.

19. Технології захисту інформації в ЛОМ : URL: http://stud.com.ua/50145/informatika/tehnologiyi_zahistu_informatsiyi_mizhmerezhevi_ekrani.

20. 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.

21. Інформаційна безпека, проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Запоріжжя, 2001.

22. Системи виявлення мережевих атак: URL: http://ukrbukva.net/page,10,97306-Sistemy-obnaruzheniya-atak.html.

23. Грайворонский М. В., Новиков А. М. Безпека інформаційно-комунікаційних систем: 2009. 608 с.

24. Данюк В. М., Петюх В. М., Цимбалюк С. О. Менеджмент персоналу: навч. посіб. КНЕУ, 2004.

25. Методи підбору персоналу: п’ять рекомендацій : URL: http://cikavosti.com/metodi-pidboru-personalu-p-yat-rekomendatsiy

26. Ожиганова М. І., Хорошко В. О., Яремчук Ю. Є. Контроль якості праці управління персоналом : навч. посіб. Вінниця : ВНТУ.

27. Дворський М. Н., Палатченко С. Н. Ідентифікація та аутентифікація користувачів: URL: http://biblio.royalwebhosting.net/identifikatsiya-autentifikatsiya-polzovateley-40481.html.

28. Інформаційна безпека підприємства. Основні положення та ввідні поняття. URL: http://stud.com.ua/21678/ekonomika/informatsiyna_bezpeka_pidpriyemstva.

29. Коваленко Ю. О. Забезпечення інформаційної безпеки на підприємстві. Економіка промисловості : 2010. 123 – 129 с.

30. Крушельницька О., Мельничук Д. Управління персоналом : навч. посіб : Кондор, 2005. 308 с.

31. Міжмережеві екрани або фаєрволи : URL: http://texnonews.com/Mizhmerezhevi-ekrani-abo-faervoli.html.

32. Ходаницкая А. Методы оценки персонала : 2008. 1 – 3 с.

33. Ліпкан В. А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні: 2013. 344 с.

34. Кормич Б. А. Інформаційна безпека : навч. посібник : Кондор, 2008. 384 с

35. Забезпечення інформаційної безпеки підприємства : URL: http://www.arinteg.ru/articles/informatsionnaya-bezopasnost-predpriyatiya-25799.html

36. Коновал Д. Комплексний підхід до організації системи захисту інформації на підприємстві: URL: http://www.epamgroup.ru/aboutus/news-and-events/articles/2009/aboutus-ar-gaz-prom-09-01-2009.html#sthash.qruifGvr.dpuf

37. Цілі і методи ІБ: URL: http://www.arinteg.ru/articles/tseliinformatsionnoy-bezopasnosti-26725.html

38. Андріанов В. В., Зефиров С. Л., Голованов В. Б., Голдуев Н. А. Забезпечення інформаційної безпеки бізнесу: 2010. 265 с.

39. Гладких А. А., Дементьєв В. Є. Базові принципи інформаційної безпеки обчислювальних мереж: 2009. 156 с.

40. Гатчин Ю. А., Клімова Е. В. Основи інформаційної безпеки: навч. посіб. СПбДУ ІТМО, 2009. 84 с.

41. Лагун А., Кухарська Н. Ризики інформаційної безпеки ІТ-підприємства:URL:http://www.google.com.ua/url?url=http://sci.ldubgd.edu.ua:8080/bitstream/handle/ 123456789/750.

42. ISO/IEC 27003 : Information security management system implementation guidance. 2010

43. Герасіменко В. А., Малюк А. А. Основи захисту інформації: МГІФІ, 1997. 538 с.

44. Давидовский А. І., Максимов В. А. Вступ в захист інформації: 1990. 17 – 20 с.

45. Соснін О.В., Шіменській Л.Є. Про правові основи удосконалення системи державного управління інформаційнімі ресурсами. *Політологічній вісник*, 2002. 212 с.

46. Агафонов Г. Г., Буришев С. А., Прохоров С. Л. Концепции безопасности. / - К.: А-ДЕПТ, 2005.-Кн. 2.

47. Браіловський М. М., Дорошко В. О., Чирков Д. В., Шелест М. Е. Захист економічної інформації: Навч. посібник / За ред. проф. В. О. Хорошка: - К.: НАУ, 2002

48. Стаття «Управління безпекою підприємств в умовах ринкової економіки». – Електронний ресурс. – Режим доступу: https://gospodarstva.com/upravlinnya-bezpekoyu-pidpriyemstv/

49. Азаров Д.С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації: Автореф. дис. ... канд. юрид. наук: 12.00.08 / НАН України; Іа-т держави і права ім. В.М. Корецького. — К., 2003.

50. Брижко В.М., Гальченко О.М., Цимбалюк В.С. і ін. Інформаційне суспільство. Дефініції: людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція. - К.: Інтеграл, 2002.

51. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. Академический Проект; Фонд "Мир", 2003.

52. Василъченко 3. М. Структурні диспропорції у розвитку банківської системи України // Фінанси України. - 2005.

53. Віхорсв С. В., Кобцев Р. Ю. Як дізнатися - звідки напасти або звідки виходить загроза безпеці інформації // Захист інформації. Конфідент. – 2002

54. Вольоводз А. Г. Проект Європейської конвенції про кіберзлочини // Захист інформації. Конфідент -2001

55. Живко М. О. Захист інформації в системі економічної безпеки та підприємства / Регіональне і місцеве самоврядування в нових умовах: партійна публічна адміністрація і безпосередня демократія: Мат-ли НІ укр.-польськ. наук.- практ. конф. (Львів, 2-4 березня 2006р.). - Л., 2006 82

56. Зегжда Д. П., Івашко А. М. Основы безопасности информационных систем.- М.: Гаряча лінія - Телеком, 2000. 33. Зубок М., Ніколаєва Л. Організаційно-правові основи безпеки банківської діяльності в Україні. - К.: Істина, 2000.

57. Організаційно-правові основи захисту інформації з обмеженим доступом: Навч. посібник / А. Б.Стоцький, А. М. Гуз, А. І. Марущак та ін.; За заг. ред. В. С. Сідака - К.: Вид-во Європ. ун-ту, 2006

58. Стаття: «Изменения в нормативных документах Украины по вопросам защиты информации» – Електронний ресурс – Режим доступу: http://www.dut.edu.ua/ru/news-1-0-5143

59. Стаття «Інформаційна безпека і її складові». – Електронний ресурс – Режим доступу: https://egrivna.com/informacijna-bezpeka-i-ii-skladovi-2/

60. Стаття «Система економічної безпеки підприємства та її методологічні засади» – Електронний ресурс – Режим доступу:

https://studopedia.su/8_58207_sistema-ekonomichnoi-bezpeki-pidpriiemstva-ta-iimetodologichni-zasadi.html

61. Про захист інформації в автоматизованих системах: Закон України // Відомості Верховної Ради. 1994.-№31.-286 с.

62. Батюк А.Є. Інформаційні системи в менеджменті / А.Є. Батюк, З.П. Двуліт, К.М. Обельовська, І.М. Огороднік, Л.П. Фабрі. – Львів: «Інтелект-Захід», 2004. – С. 343–384.

63. Агафонов Г. Г., Буришев С. А., Прохоров С. Л. Концепции безопасности. / - К.: А-ДЕПТ, 2005.-Кн. 2.