МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: "ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ"

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Дмитро ЯНОВСЬКИЙ
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Дмитро ЯНОВСЬКИЙ

Керівник:
к.т.н. Дмитро РАБЧУН

Рецензент:

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут Захисту інформації

Кафедра Управління інформаційною та кібернетичною безпекою

Ступінь вищої освіти магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Управління інформаційною безпекою

ЗАТВЕРДЖУЮ
Завідувач кафедрою УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Яновському Дмитру Вікторовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ"

керівник кваліфікаційної роботи Дмитро РАБЧУН, к.т.н.
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р

3. Вихідні дані до кваліфікаційної роботи: *інформаційна безпека підприємства, методи та засоби управління інформаційною безпекою, система управління інформаційною безпекою, комплексний підхід до управління інформаційною безпекою.*

4. Перелік питань, які потрібно розробити:
   1. Проаналізувати системи управління інформаційною безпекою підприємства.
   2. Дослідити формування системи управління інформаційною безпекою на підприємстві.
   3. Визначити підхід до створення систем управління інформаційною безпекою підприємства.

   Перелік ілюстративного матеріалу: *презентація*

5. Дата видачі завдання "02" жовтня 2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	виконано
2.	Збір та аналіз літератури.	23.10.2023	виконано
3.	Аналіз системи управління інформаційною безпекою підприємства.	27.10.2023	виконано
4.	Дослідження формування системи управління інформаційною безпекою на підприємстві.	10.11.2023	виконано
5.	Визначення підхід до створення систем управління інформаційною безпекою підприємства.	15.11.2023	виконано
6.	Формулювання висновків зарезультатами проведеного дослідження.	22.11.2023	виконано
7.	Оформлення роботи.	04.12.2023	виконано
8.	Оформлення презентації.	14.12.2023	виконано
9.	Отримання рецензії на роботу.	18.12.2023	виконано
10.	Захист в ЕК.	17.01.2024	виконано

Здобувач вищої освіти _____ Дмитро ЯНОВСЬКИЙ
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня бакалавра

Направляється здобувач Яновський Д.В. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ"

Кваліфікаційна робота і рецензія додаються.

Директор ННІЗІ _____ Віталій САВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника кваліфікаційної роботи

Здобувач **ЯНОВСЬКИЙ Дмитро** у кваліфікаційній роботі дослідив сучасні системи управління інформаційною безпекою в Україні, визначив основні проблеми та розробив пропозиції і рекомендації керівникам структурних підрозділів кібербезпеки щодо підвищення ефективності систем управління інформаційною безпекою організацій (підприємств). **ЯНОВСЬКИЙ Дмитро** показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів уміння самостійного застосування методів наукового дослідження, проявив себе як організований, відповідальний виконавець. Результати дослідження апробовані на трьох науково-практичних конференціях.

Це дозволяє оцінити виконану кваліфікаційну роботу здобувачу **ЯНОВСЬКОГО Дмитра** на оцінку "задовільно" та присвоїти йому кваліфікацію "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Дмитро РАБЧУН
(підпис) *(Ім'я,ПРІЗВИЩЕ)*

"____" _____2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Здобувач Яновський Д.В. допускається до захисту даної роботи в екзаменаційній комісії.

Завідувач кафедрою
Управління інформаційною
та кібернетичною безпекою _____ Світлана ЛЕГОМІНОВА
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

здобувача вищої освіти **Яновського Дмитра Вікторовича**
на тему "ВИКОРИСТАННЯ КОМПЛЕКСНОГО ПІДХОДУ ДО ПОБУДОВИ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ НА ПІДПРИЄМСТВІ"
Актуальність Як свідчать реалії, різноманітні засоби інформаційної безпеки зараз активно застосовуються конкуруючими фірмами та корпораціями в ринковій боротьбі. Тому важливим завданням сучасного підприємства є її захист від різноманітних загроз системам управління інформаційною безпекою. З огляду на зазначене дослідження проблем забезпечення інформаційної безпеки підприємства є актуальним для дослідження.

Позитивні сторони

1. У роботі досліджено побудову систем управління безпекою на підприємстві. Проаналізовано загрози інформаційним системам підприємства та розкрито сутність безпеки підприємства.
2. Кваліфікаційна робота оформлена відповідно до вимог. Виклад матеріалу здійснено відповідно до плану, зроблено логічні висновки. Ключові положення роботи представлено у вигляді рисунків. Автор опрацювала значну джерельну базу: близько 50 публікацій та електронних джерел, в тому числі англомовних.
3. За результатами дослідження запропоновано рекомендації щодо забезпечення інформаційної безпеки.

Недоліки

1. Доцільно було б приділити більше уваги вивченню і класифікації методів протидії загрозам інформаційних систем, а також особливостям їх використання у вітчизняних реаліях.

Однак, вищезгадані зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

Висновок: Кваліфікаційна робота виконана на належному науково-методичному рівні і заслуговує позитивної оцінки, а здобувач **ЯНОВСЬКИЙ Дмитро** заслуговує присвоєння кваліфікації Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент: _____
підпис

ЗМІСТ

ВСТУП

Актуальність теми. Сучасний світ неможливо уявити без інформаційних технологій, а саме технологій зв'язку та передачі даних. Новинки науково-технічного прогресу поглинули всі сфери людської діяльності, що дає змогу спростити працю людини при вирішенні певних завдань і при виконанні певних видів робіт.

Тому питання безпеки таких інформаційних каналів передачі даних займає одне з перших місць у забезпеченні загальної безпеки підприємства [1].

Сьогодні підприємства вживають низку заходів, які дозволяють протистояти несанкціонованому доступу, розголошенню комерційної інформації та притягувати порушників до відповідальності.

Питання є досить актуальним з огляду на зростання динаміки злочинів, пов’язаних із посяганнями та зловмисним використанням інформації третіми особами.

У зв’язку з цим можна зробити висновок, що тема дипломної роботи, присвячена дослідженню створення системи управління інформаційною безпекою підприємства, є актуальним завданням.

Мета і завдання дослідження. Мета роботи – збільшення ефективність функціонування системи управління інформаційною безпекою підприємств в сучасних умовах розвитку інформаційних технологій.

Для досягнення мети в роботі необхідно вирішити наступні завдання:

1) провести аналіз систем управління інформаційною безпекою підприємства;

2) визначити основні аспекти інформаційно-технічної безпеки підприємств та їх вплив на здатність виконувати свою місію;

3) вибрати модель інформаційних загроз в інформаційних системах підприємства;

4) сформулювати вимоги до побудови системи управління інформаційною безпекою підприємства на основі галузевих стандартів України;

5) формалізувати систему управління інформаційною безпекою підприємства;

6) розробити рекомендації щодо підвищення ефективності системи управління інформаційною безпекою підприємства.

Об'єктом дослідження в роботі є стратегія та шляхи забезпечення інформаційної безпеки підприємства.

Предмет дослідження процес створення системи управління інформаційною безпекою підприємства.

Методи дослідження. Для вирішення вищезазначеного наукового завдання в роботі використовуються методи математичного аналізу, теорії інформаційної безпеки, теорії прогнозування та прийняття рішень, методи теорії операцій.

Наукова новизна отриманих результатів. У роботі отримано нові науково обґрунтовані результати:

1) формування до побудови системи управління інформаційною безпекою підприємства на основі галузевих стандартів України;

2) рекомендації щодо підвищення ефективності системи управління інформаційною безпекою підприємства.

Практичне значення отриманих результатів у зв'язку з тим, що запропоновані в роботі підходи можуть бути використані при розробці, впровадженні та експлуатації систем захисту інформації на об'єктах інформаційної діяльності та систем управління інформаційною безпекою підприємства.

Розділ 1
АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Інформаційна ера принесла кардинальні зміни в те, як багато професій виконують свої завдання. Завдання, які колись виконували висококваліфіковані програмісти, тепер можуть виконувати нетехнічні професіонали середньої ланки. Співробітники мають доступ до більш точної та своєчасної інформації, ніж будь-коли раніше. Цьому сприяє швидке поширення сучасних інформаційних і особливо комп'ютерних технологій [2].

Водночас використання таких технологій створює низку проблем для будь-якої організації та її керівництва. Як правило, об'єднані в мережу комп'ютери забезпечують доступ до великих обсягів різноманітних даних. Тому вони стикаються з небезпеками, ризиками, викликами та загрозами, пов'язаними з автоматизацією та розширенням доступу до конфіденційних, персональних та інших важливих даних, а також необхідністю забезпечення інформаційної безпеки. Кількість комп'ютерних злочинів продовжує зростати і може призвести до економічних злочинів. На цьому тлі зростає усвідомлення того, що інформація є важливим ресурсом, який потребує захисту.

1.1 Основні аспекти інформаційно-технічної безпеки підприємств

Інформаційна безпека на підприємствах є одним із основних елементів управління сучасними багатофункціональними та комплексними підприємствами та організаціями всіх форм власності. Відсутність інформаційної безпеки є найбільш небезпечною для підприємств, і при

вирішенні цієї проблеми необхідно враховувати, що однією з головних умов стабільного функціонування кожного підприємства є обмін інформацією. Іншими словами, інформаційна безпека повинна базуватися не тільки на створенні відповідної законодавчої бази, яка регламентує порядок доступу, зберігання та використання інформації в компаніях, фірмах і на підприємствах, а й на заходах захисту інформації в засобах її передачі і обробки та в мережах. Створення системи захисту конфіденційної інформації базується на таких законодавчих актах: Закон України «Про інформацію», Закон України «Про захист інформації в автоматизованих системах» тощо.

Розглядаючи статті цих законів, склад інформації на підприємстві можна виділити так, як зазначено на рис. 1.1.

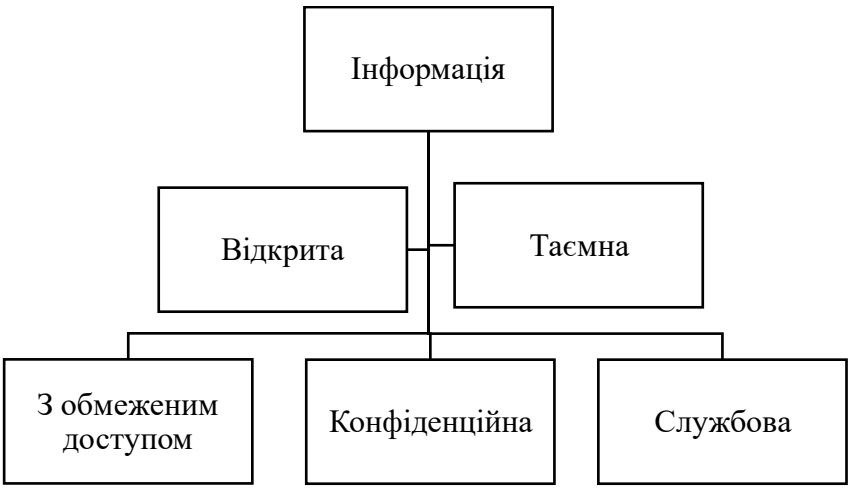

Рис. 1.1-Режими доступу до інформації на підприємстві

Погіршення інформаційної безпеки організації може бути викликано наступними факторами:

- збільшення обсягу інформації, що накопичується, зберігається та обробляється на комп'ютерах;

- збільшення обсягу інформації, що зберігається та обробляється в базах даних

- концентрація інформації в базах даних з різним призначенням і власниками

- розширення кола користувачів, які мають прямий доступ до ресурсів комп'ютерних систем і масивів даних

- ускладнення принципів роботи технічних засобів комп'ютерних систем;

- обмін інформацією через локальні та глобальні мережі, в тому числі на великі відстані.

Ключовим елементом у всіх аспектах інформаційної безпеки є аналіз дій, які можуть порушити функціонування інформаційних систем компанії.

Під цими діями розуміються дії, що підвищують вразливість інформації, що обробляється автоматизованими системами, і призводять до її витоку, випадкової чи навмисної зміни чи знищення. Випадкові загрози включають помилки та упущення, а також події поза контролем людини, такі як природні або спричинені людиною катастрофи. Заходи захисту від них мають переважно організаційний характер [8].

До апаратних і програмних помилок відносяться пошкодження комп'ютерів і периферійних пристроїв (наприклад, магнітних носіїв), а також помилки в прикладних програмах. Ненавмисні помилки зазвичай виникають під час технічного циклу обробки, передачі та зберігання даних і включають помилки користувача, оператора та програміста, втручання у виконання програми та пошкодження носія. Навмисні погрози можуть здійснюватися як учасниками процесу обробки інформації (внутрішні), так і «хакерами» (зовнішні).

Згідно з опитуванням, прямий несанкціонований доступ до робочих місць, систем і комп’ютерних мереж найчастіше здійснюють працівники підприємства, які є користувачами комп’ютерів, або обслуговуючий персонал, наприклад програмісти, інженери та оператори (41,9%). 8,6% злочинів вчинено звільненими працівниками, 25,5% – сторонніми особами.

Найпоширенішими видами навмисних погроз сьогодні є наступні

За періодичністю впровадження:

- Копіювання та піратство програмного забезпечення

- Несанкціоноване введення даних

- Зміна або знищення даних на магнітних носіях

- Саботаж

- Крадіжка інформації

- Несанкціоноване використання ресурсів комп'ютера

- несанкціоноване використання систем автоматизації
- несанкціонований доступ до конфіденційної інформації [4].

Основним завданням корпоративної інформаційної безпеки є забезпечення умов для запобігання незаконному чи несанкціонованому розголошенню конфіденційної інформації чи її використанню для злочинної чи протиправної діяльності.

Розголошення інформації - це умисне або необережне передавання, оприлюднення, оголошення, розголошення, передача, пропозиція винагороди, передача або втрата такої інформації особою, якій вона відома, навіть якщо це пов'язано з її професійною діяльністю і не є службовою необхідністю. [13].

Під несанкціонованим доступом до інформації розуміється доступ до інформації з порушенням встановлених правил розмежування доступу. Усі перераховані способи отримання інформації можуть бути використані конкурентами, промисловим шпигунством та спецслужбами шляхом створення так званих каналів витоку та передачі інформації. Такі методи спрямовані на створення належних умов для передачі інформації від носія до споживача. Загальновідомо, що інформація передається за допомогою енергії або речовини. У фізичній природі інформація може передаватися світловими променями, звуковими хвилями, електромагнітними хвилями, матеріалами та речовинами.

Для створення відповідних систем передачі інформації використовуються певні фізичні поля:

- Джерело інформації
- Передавач
- Канал передачі
- Реципієнт і приймач інформації.

Те саме стосується передачі інформації та людських стосунків. Передавачі знань (джерела) передають знання одержувачам через «передавачів», а в деяких випадках через «приймачів». Джерелами інформації є люди, документи, публікації, технічні засоби, що забезпечують виробничу діяльність, продукція, відходи промисловості та виробництва [21].

Для спонтанного витоку інформації та несанкціонованого доступу використовуються відповідні канали збору інформації:

- Візуально-оптичні (спостереження, відеозапис, фотозйомка),
- Акустична та акустична обробка,
- електромагнітні (включаючи магнітні та електричні),
- матеріальні (наприклад, магнітні носії, папір, фотографії).

Крім незаконного отримання інформації, існують інші загрози, які не пов'язані з отриманням інформації, але є не менш небезпечними. До них відносяться знищення або модифікація інформації (зміна її змісту). Слід зазначити, що згідно з дослідженнями спеціалізованих установ, до факторів, що створюють умови для витоку (передачі) інформації, належать наведені в таблиці. 1.1.

Зі сказаного вище можна зробити висновок, що спецслужби, конкуренти та злочинці отримують інформацію переважно за допомогою технічних засобів, якими користуються фірми, підприємства та їх співробітники [6].

Таблиця. 1.1

Причини витоку конфіденційної інформації підприємства

Фактори	**%**
Зайва балакучість співробітників компанії	32
Бажання співробітників заробити гроші будь-яким способом/за будь-яку ціну	24
Відсутність заходів захисту інформації в компаніях	14
Звичка співробітників ділитися один з одним новинами, чутками та інформацією	12
Безконтрольне використання інформаційних систем	10
Велика кількість конфліктних ситуацій між співробітниками	8

Для оцінки безпеки інформаційних систем компанії проводиться дослідження, яке можна розділити на наступні етапи:

- Збір інформації про мережу (наприклад, визначення типу операційної системи атакуючого хоста);
- Виявлення інформаційних загроз і вразливостей;
- Вторгнення в мережу;
- Оцінка ризиків, пов'язаних з виявленими вразливими місцями та їх потенційне використання для отримання несанкціонованого доступу до мережі;
- Розробка рекомендацій щодо створення систем захисту інформації та відповідної політики безпеки;
- За погодженням з керівництвом підприємства надання рекомендацій щодо впровадження, налаштування та супроводу комплексної системи захисту інформації (мережевих та комп’ютерних ресурсів).

Якщо така експертиза неможлива, одним із варіантів є використання спеціалізованого програмного забезпечення, призначеного для пошуку відомих вразливостей в інформаційній системі або помилок у параметрах конфігурації операційної системи. У процесі аналізу безпеки враховуються конкретні елементи інформаційної системи, які потребують захисту, відповідно до важливості (ранжування) інформації, яка обробляється, зберігається та

передається, відповідно до політики безпеки, прийнятої компанією та безпосередньо інтегрована з глобальною мережею Інтернет.

Сьогодні компанії використовують спеціальні програмні комплекси для перевірки рівня інформаційної безпеки комп'ютерних мереж. До таких складних систем відносяться спеціальні мови ідентифікації вразливостей Internet SafeSuit (Internet Security System) [9].

Відповідне програмне забезпечення використовується комп'ютерними злочинцями для запобігання витоку конфіденційної інформації шляхом «злому» інформаційних мереж.

В даний час на ринку представлено достатню кількість програмного забезпечення в категорії засобів виявлення мережевих вторгнень. Вони включають:

1. Сканери безпеки в Інтернеті.
2. OpenVas.
3. NetProbe (Qualix).
4. Ballista (Secure Networks).
5. Tenable Nessus.
6. NetGuard (Network Guardian).
7. NetSonar (WheelGroup).

Українські підприємства та організації в основному використовують спеціальне іноземне програмне забезпечення:

- Комплексний захист корпоративних мереж забезпечує програмний продукт VPN ZASTAVA 3.3 від компанії «ЕЛВІС ПЛЮС»;
- Криптографічний захист CSP, розроблений компанією «Кріпто Про», допомагає ефективно перевіряти електронний цифровий підпис.

1.2 Аналіз загроз інформаційним системам підприємства та їх характеристики

Інформаційні загрози, пов’язані з впливом на організацію та її оточення, включають дискредитацію організації (поширення негативної та неправдивої інформації про організацію; маніпулювання індивідуальною та колективною свідомістю працівників, клієнтів, акціонерів чи просто широкої громадськості; маніпулювання індивідуальною та колективною свідомістю). акціонерів, споживачів або просто широкому загалу, надання неправдивої інформації про різних осіб, пов’язаних з емітентом), (поширення негативних чуток про емітента, вчинення актів інформаційного тероризму, провокування інформаційних конфліктів, втягнення емітента в інформаційні війни).

Такий вплив людей на об'єкти пов'язаний з тим, що хоча люди живуть в реальному світі, вони сприймають його через системи зв'язку. Тому, створюючи нові комунікаційні технології та впроваджуючи світові стандарти надання інформації, можна спотворити реальний світ і замінити його інформацією в сприйнятті споживачів інформації. Іншими словами, інформаційний простір організації дуже керований, і в залежності від того, хто вміє ним керувати, розрізняється і сам простір, а відповідно і конкретна організація. Вплив на споживачів інформації в такій ситуації відбувається шляхом створення відповідних схем, таких як інформаційні повідомлення, коментарі, експертні думки, поширення чуток, наведення прикладів і порівнянь. Велика кількість інформації надходить в інформаційний простір організації за певний проміжок часу по ряду каналів. Споживачі під впливом стандартизованої структури системи інформаційного забезпечення сприймають цю інформацію як реальну, а не штучно створену. Метою таких дій є створення ситуації, яка ускладнює роботу підприємства, шкодить його іміджу і, відповідно, робить його менш конкурентоспроможним на ринку.

При виявленні бізнес-загроз в інформаційній сфері особливу увагу слід звернути на промислове шпигунство, об’єктом якого є практично всі складові ринкової економіки. Промислове шпигунство — це отримання тим чи іншим способом відповідних технологій, планів, розробок, ідей та інформації, що характеризує рішення, що цікавлять конкурентів. Інформація не обов'язково має бути конфіденційною, але вона має бути корисною для конкурентів та інших організацій. Володіючи такими знаннями, вони можуть заощадити багато часу та ресурсів і отримати перевагу на ринку. Підприємці часто не усвідомлюють, наскільки цінною може бути інформація, якою вони володіють. Інформація про ціни на їхні продукти, маркетингові та рекламні плани, аналіз робочої сили, якість їхніх клієнтів і споживачів, а також оцінки конкурентів часто не є конфіденційною, але тим не менш цінною для суб’єктів промислового шпигунства. Сучасні технологічні та інтелектуальні можливості створюють сприятливі умови для розвитку промислового шпигунства. Останній є постійним супутником сучасних підприємств, у тому числі й вітчизняних. Більшість бізнес-структур збирають і використовують у своїй діяльності інформацію про конкретні компанії, спеціалістів і керівників. І для вирішення цієї проблеми не обов’язково бути надмірно професійним спеціалістом, достатньо мати спеціальні знання в галузі економіки та певний рівень знань про розвідувальну діяльність. Загрозливий характер промислового шпигунства полягає в тому, що це явище набуло майже масового характеру, особливо в діяльності середніх і великих підприємств, у міжнародній економічній діяльності. На промислове шпигунство витрачаються великі гроші, сотні тисяч професіоналів працюють у цій сфері. У деяких країнах це стало важливим чинником боротьби за лідерство в економічній конкуренції.

До них відносяться США, Велика Британія, Франція, Німеччина, Японія. В останні роки Китай приєднався до цих країн у створенні технічних коледжів, де студенти вивчають наукові та технологічні теорії інтелекту. Після закінчення навчання випускників університетів відправляють до розвинених країн для збору

інформації в рамках культурного обміну між країнами [36]. Відповідно до практики захисту від промислового шпигунства, промислове шпигунство найчастіше передбачає:

- фінансові звіти, плани і прогнози;

- Маркетингові дослідження та методи формування цінової стратегії;

- технічні характеристики продукції, що планується до виробництва;

- Умови договорів і угод;

- Перспективні плани розвитку промислової та комерційної діяльності;

- Фінансовий стан і виробничий потенціал підприємства;

- Організаційна структура підприємства;

- Системи безпеки підприємства.

Очевидно, що втрата такої інформації, особливо її використання конкурентами, представляє дуже серйозну загрозу для організації, оскільки така інформація дуже цінна для організації.

Підприємства пострадянського простору швидко опановують методи і прийоми промислового шпигунства та надають їм національного колориту. Об'єктами промислового шпигунства на пострадянському просторі зазвичай є дослідження і розробки, фінансові операції, фінансування проектів, інвестиційна політика організацій, характеристики технічних процесів, специфікації продукції, результати випробувань, ланцюги поставок, списки клієнтів, інформація про транзакції, організація виробництва. . , комерційна політика та стратегії. Враховуючи ці цілі шпигунства, не можна стверджувати, що пострадянські країни з ринковою економікою є менш ризикованими чи безпечнішими, ніж подібні економіки в розвинених країнах. У цьому контексті забезпечення інформаційної безпеки, в тому числі в контексті боротьби з промисловим шпигунством, є дуже актуальним завданням для бізнесу.

Ще однією дуже небезпечною загрозою для сучасного бізнесу в інформаційній сфері є відомий кібертероризм. Кібертероризм є особливо небезпечним, оскільки він одночасно загрожує іміджу та суспільній репутації підприємства щодо його інформаційних ресурсів та діяльності. Експерти також відзначають, що останнім часом кібератаки стали дуже різноманітними, з'явилися кібершпигунство, хактивізм і кібершантаж. Кібератаки стали більш поширеними, організованими та масштабними. Значна їх кількість торкається комерційних організацій. Атаки зазвичай спрямовані на нафтові компанії, телекомунікаційні компанії, аерокосмічні компанії, суднобудівні та високотехнологічні компанії тощо. У 2013 році світова економіка втратила 113 мільярдів доларів США через кібертероризм. З 2009 по 2017 рік світові прибутки від кіберзлочинності зросли в десять разів і досягли 2 трильйонів доларів. В Україні прибутковість кібертерористів перевищує сукупний дохід від торгівлі наркотиками та зброєю [37]. Найпоширенішою загрозою тут є поширення вірусів і різного роду шкідливих програм, які не тільки псують програмне забезпечення, але й унеможливлюють його відновлення. Як правило, кібератаки починаються зі збору інформації про жертву за допомогою так званих шпигунських програм. Слід зазначити, що до кібератак схильні як стаціонарні комп’ютери, так і мобільні пристрої, підключені до комп’ютерних мереж; У 2015 році Україна увійшла до трійки лідерів за кількістю заражених мобільних пристроїв. За ризиком зараження через Інтернет наша країна посідає 9 місце серед країн високого ризику (45,6% користувачів). Це означає, що сучасні IT-інфраструктури компаній надзвичайно вразливі та потребують ефективного захисту. У той же час забезпечення такого захисту з часом стає все дорожчим і складним. Сьогодні злом баз даних, викрадення логінів і паролів електронної пошти, доступ до повідомлень електронної пошти та інших ресурсів Інтернету корпоративних організацій є поширеним явищем у всіх сферах корпоративної інформації.

Не можна ігнорувати так звані офісні загрози інформації суб’єкта господарювання, тобто інформації, яка міститься в документах і зберігається та використовується офісними працівниками в процесі їх роботи. Якщо дати відповідь на зміст поняття офісної діяльності, то воно складається з наступного: комплексу організованих у часі та просторі дій персоналу підприємства, спрямованих на забезпечення управління діяльністю підприємства [39]. Іншими словами, ведення документації є частиною процесу управління. І коли в такій діяльності присутні певні загрози, це впливає на процес управління, в даному випадку на діяльність організації. Оскільки менеджмент значною мірою пов'язаний з інформаційними технологіями, офісна діяльність спрямована на виконання різноманітних завдань, процедур та операцій, пов'язаних з інформаційним забезпеченням процесів управління. Структура, методика іЗміст цього положення називається оргтехнікою. Останні є відповідними джерелами інформації, які обробляються, інтерпретуються та використовуються для підтримки управлінської діяльності. Таким чином, діловодство базується на обробці інформації організації, і зрозуміло, що робота в ланцюжку управління визначає особливу важливість цього виду діяльності. Основними складовими діловодства є знання діловодства та пов’язаної з ним документації. За таких обставин зусилля зловмисників з метою отримати інформацію про організацію або підірвати суспільну репутацію діяльності організації будуть зосереджені на персоналі та документації.

Реалізація планів отримання офіційної інформації через персонал може становити загрозу як для персоналу, так і для організації. Найпоширенішими загрозами є залучення співробітників з оргтехнікою в конкуруючі організації для інформаційного забезпечення управлінських рішень; залучення таких працівників або третіх осіб до комерційної діяльності; залякування офісних працівників з метою отримання доступу до офіційних інформаційних ресурсів; неналежне використання оргтехніки або використовуваної в ній інформації. Заохочення співробітників до спроб неправомірного використання або

розголошення офісних технологій або інформації, яка в них використовується. В останньому випадку провокація може статися в самому офісі або в середовищі, де задовольняються потреби та інтереси офісних працівників. Невдоволення умовами, що впливають на задоволення цих потреб та інтересів, може спровокувати поведінку, яка може становити загрозу для інформації офісу. Також не обов'язково, щоб співробітники раніше були чесними або нелояльними до компанії. Такі риси можуть бути спровоковані атмосферою в офісі, стилем стосунків і графіком роботи, що саме по собі є загрозою і, зрештою, серйозною загрозою для інформації організації. Причому такі погрози зазвичай не пов'язані з матеріальними цінностями і не обов'язково викликають почуття провини за те, що витік інформації стався з вини людини. Необхідність організацій документувати свою діяльність створює додаткові ризики для інформаційних ресурсів. Можуть бути такі загрози службовій інформації:

- втрата або незаконне знищення документів;

- офісні працівники не ознайомлені з вимогами до формування, обробки, обліку, передачі та зберігання документів;

- використання документів з обмеженим доступом у присутності осіб, які не мають права доступу до них; несанкціонована передача таких документів таким особам;

- використання інформації з обмеженим доступом у нерейтингових документах, публікаціях та особистих справах;

- включення надлишкової інформації з обмеженим доступом до документів;

- порушення спеціальних режимів роботи з документами;

- копіювання офіційних, конфіденційних чи таємних документів, крім випадків службової необхідності;

- несвоєчасна передача документів на зберігання, порушення правил зберігання;

- усний переклад документів заочно, цитата з листування, передача електронною поштою.

Заходи інформаційної безпеки в офісі повинні враховувати, що більшість загроз походить від співробітників, незалежно від того, походять вони від їх власної інформації чи від інформації, що міститься в документах. Тому важливо знати основні фактори, які визначають поведінку співробітників і можуть підштовхнути їх до розголошення службової інформації. До таких факторів відносяться об'єктивні умови, в яких працівники є основним джерелом інформації. Іншим об'єктивним фактором є непередбачуваність і низька контрольованість поведінки співробітників у різних ситуаціях. Крім того, передбачення - це лише ймовірність і лише надія на те, що поведінка та реакція людей будуть такими, як очікувалося. Інші фактори включають недоліки в навчанні співробітників і особистісні риси співробітників, які можуть схиляти їх говорити або поводитися неадекватно. Недостатня професійна підготовка працівників, особливо щодо роботи з документами та інформацією з обмеженим доступом, безвідповідальність, недисциплінованість та інші негативні риси також можуть призвести до витоку інформації офісними працівниками. Як видно з наведених характеристик діловодства та умов, за яких можуть виникати інформаційні загрози, інформаційні загрози можуть виникати як з об’єктивних, так і з суб’єктивних причин. Тому створення системи захисту інформації в будь-якому офісі повинно включати заходи, спрямовані на створення безпечних умов для використання інформації в офісі, а також заходи, які виключають або істотно обмежують можливість шахрайства з боку персоналу щодо інформації в офісі. офіс. Офіс

1.3 Нормативно-правове регулювання організації безпеки підприємства

На забезпечення інформаційної безпеки підприємницької діяльності впливають різні умови, провідне місце серед яких посідають законодавчі вимоги. Останній складається з чотирьох правових норм: Конституції України, законів, підзаконних актів та положень господарських товариств.

Важливість правових умов у забезпеченні інформаційної безпеки полягає в тому, що без законів, які встановлюють ці умови, процес організації інформаційної безпеки був би абсолютно неможливим. Завдяки цим законам регулюються інформаційні відносини, здійснюються заходи безпеки інформації, визначається правомірність певних дій щодо інформації, встановлюються основи відповідальності за дії в інформаційній сфері. Як наслідок, правові норми гарантують захист підприємств від незаконних посягань на їхні права, інтелектуальну власність та інформацію, які можуть виникнути в процесі їх діяльності.

Положеннями статті 55 Конституції України визнається право на захист від порушень і протиправних посягань на права і свободи будь-якими не забороненими законом способами [39]. До таких засобів належать, зокрема, нормативно-правові акти (норми та положення Конституції та законодавства України, нормативні акти органів державної влади, нормативні акти юридичних осіб та інших організацій, рішення та постанови судів, судових органів, нормативні акти Міністерства). юстиції України). України, договірні умови, договори, укладені юридичними особами, рішення, накази та приписи наглядових і контролюючих органів). Права охоплюють і інформаційну сферу. Зокрема, право на інформацію включає можливість вільно отримувати,

використовувати, поширювати, зберігати та захищати інформацію, необхідну для реалізації своїх прав, свобод і законних інтересів [20].

Крім того, Конституція України гарантує право на правовий захист у разі спростування недостовірної інформації, право вимагати видалення будь-якої інформації, право на відшкодування матеріальної та моральної шкоди, завданої збиранням, зберіганням і поширенням недостовірної інформації. інформації. . Конституція забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, якщо інше не встановлено законом (ст. 32). Конкретизуючи зміст конфіденційної інформації про особу, слід зазначити, що до такої інформації належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, адресу, дату та місце народження [20]. Іншими словами, Конституція України встановлює загальні умови поведінки організацій і громадян в інформаційній сфері.

Усі види інформації є загальнодоступними, крім тієї, доступ до якої обмежено законодавством. Важлива інформація, яка підпадає під обмеження, а не документи, які її містять. Якщо документ містить таку інформацію, то перевірці підлягають ті частини документа, які не містять інформації з обмеженим доступом [40].

Конфіденційна інформація - інформація про фізичну особу, до якої мають доступ фізичні або юридичні особи, крім суб'єктів владних повноважень. Така інформація може бути поширена керівником за бажанням (згодою) відповідної особи на визначених ним умовах та в порядку, визначеному ним, в інших випадках, передбачених законодавством. До уповноважених суб'єктів законодавець відносить органи державної влади, органи місцевого самоврядування, інші органи, які на основі законодавства здійснюють владні управлінські функції, у тому числі на виконання делегованих повноважень.

Важливо визначити тих, хто має право обмежувати доступ та надавати інформацію з обмеженим доступом. Очевидно, що така особа може бути як власником відповідної інформації, так і особою, яка має право нею

розпоряджатися. В останньому випадку законодавець визначає перелік розпорядників інформації, види інформації, якою вони можуть розпоряджатися, їхні обов'язки та функції (статті 13-18 Закону України «Про доступ до публічної інформації»).

Конфіденційною є інформація, доступ до якої обмежено відповідно до вимог статті 6 Закону України «Про доступ до публічної інформації» та розголошення якої може завдати шкоди особі, суспільству та державі. Інформація, що містить державну, професійну, комерційну та іншу визначену законом таємницю, є конфіденційною.

До службової інформації належать відомості, що містяться в документах суб'єктів владних повноважень, а також відомості, зібрані під час здійснення оперативно-розшукової, контррозвідувальної чи антитерористичної діяльності та не віднесені до державної таємниці.

Доступ до конфіденційної інформації визначається установами та організаціями, які володіють такою інформацією, відповідно до чинного законодавства. Доступ до приватної інформації визначається відповідно до Закону України "Про доступ до публічної інформації" та в порядку, визначеному внутрішніми документами суб'єктів владних повноважень.

Відносини у сфері доступу до публічної інформації регулюються Законом України «Про доступ до публічної інформації». Зокрема, Закон визначає «публічну інформацію» як відображену та задокументовану будь-якими засобами та на будь-яких носіях інформацію, отриману чи створену в процесі здійснення суб'єктами владних повноважень, передбачених чинним законодавством, або яка знаходиться в у володінні суб'єктів владних повноважень, інших розпорядників бюджетних коштів, крім випадків, передбачених законом.

Відповідно до вищезазначеного законодавства доступ до публічної інформації забезпечується шляхом її оприлюднення в установленому порядку та подання розпоряднику інформації запиту. Інформація надається безкоштовно.

Відповідальними організаціями у сфері доступу до публічної інформації є запитувач інформації, розпорядник інформації, структурний підрозділ або особа, відповідальна за надання відповіді на запит.

Окремо організована система доступу до інформації про фізичних осіб. Тут за основу слід взяти положення Закону України «Про захист персональних даних», Закону України «Про доступ до інформації» та Закону України «Про інформацію». Зокрема, передбачено, що не допускається збирання, зберігання, використання та поширення інформації про фізичну особу без її згоди, якщо інше не встановлено законом. Обсяг такої інформації має бути максимально обмеженим і використовуватися лише для цілей та у спосіб, визначений законодавством.

Відповідними суб'єктами у сфері доступу до персональних даних є суб'єкт персональних даних, володільці та розпорядники баз персональних даних, треті особи (яким володілець або розпорядник бази персональних даних передає персональні дані відповідно до закону), стан. органи, уповноважені здійснювати захист персональних даних, інші державні органи, до повноважень яких належить захист персональних даних, органи місцевого самоврядування.

Фізичні особи повинні бути проінформовані володільцем або розпорядником бази про свої права у зв'язку зі збором відомостей про них та оприлюдненням інформації про них у базі персональних даних протягом 10 днів з дня створення бази. Водночас таке повідомлення не вимагається, якщо персональні дані збираються із загальнодоступних джерел [41].

Поширення персональних даних можливе лише за згодою фізичної особи. У разі ненадання згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини, визначених законом. Порядок доступу до

персональних даних та відносини особи з ними регулюються положеннями статей 16-19 Закону України «Про захист персональних даних».

Питання правового регулювання доступу до персональних даних за міжнародним правом регулюється Конвенцією Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних, Додатковим протоколом до Конвенції про захист осіб у зв'язку з автоматизованою обробкою. персональних даних. Обробка персональних даних і транскордонних потоків даних по відношенню до наглядових органів і узгоджується з положеннями Директиви Ради Європи «Про захист осіб у зв'язку з вільним переміщенням таких даних» і «Директиви про обробка персональних даних».

Основними принципами захисту персональних даних, визначеними зазначеними законодавчими актами, є:

- Збір та обробка персональних даних має здійснюватися правильно та відповідно до законодавства;

- використання персональних даних має відповідати меті та бути обмеженим у часі;

- Персональні дані мають бути точними, оброблятися лише за згодою суб'єкта даних і бути доступними для суб'єкта даних;

- Персональні дані мають бути надійно захищені. [42].

З точки зору інформаційної безпеки важливим є відповідне правове регулювання у сфері захисту інформації з обмеженим доступом. Важливим питанням комерційної діяльності є захист комерційної інформації.

Правові засади комерційної таємниці регулюються Господарським кодексом України, Цивільним кодексом України, Кримінальним кодексом України, Кодексом України про адміністративні правопорушення, Законом України «Про захист від недобросовісної конкуренції», «Інформаційним Кодекс» та іншими нормативно-правовими актами. Зокрема, сутність комерційної таємниці як виду інформації з обмеженим доступом визначено Цивільним кодексом України.

Відповідно до нього комерційна таємниця - це відомості, що становлять таємницю в цілому або в певному вигляді та сукупності його складових, які в цілому або в певному вигляді та сукупності його складових є невідомими та недоступними особам. які мають інтерес у типі інформації, до якого вона належить, має комерційну цінність у зв'язку з нею, і особа, яка законно контролює цю інформацію, вжила відповідних заходів для збереження її конфіденційності за умов, що виникли Інформація, яка є характер комерційної таємниці . За змістом до комерційної таємниці належать відомості технічного, організаційного, комерційного, виробничого та іншого характеру, за винятком відомостей, які відповідно до закону не можуть бути віднесені до комерційної таємниці [43]. Перелік відомостей, які можуть становити комерційну таємницю, визначено постановою Кабінету Міністрів України № 611.

Постанова Кабінету Міністрів України № 611.

Відповідно до положень Господарського кодексу України склад та обсяг відомостей, що становлять комерційну таємницю, а також спосіб їх захисту визначаються підприємством [44].

Таким чином, законодавець не визначає конкретний зміст комерційної таємниці, а лише дає вказівки щодо того, що має містити інформація, що становить таку таємницю. Також слід зазначити, що така таємниця, як комерційна таємниця, поширюється лише на суб'єктів підприємницької діяльності, тобто на юридичних та фізичних осіб, зареєстрованих як суб'єкти підприємницької діяльності. Право власності на таку інформацію набувається або шляхом використання власних ресурсів і засобів, або шляхом її створення іншою особою за рахунок юридичної особи та на користь юридичної особи на підставі договору з юридичною особою, або придбавши таку інформацію в іншої особи.

Створення відомостей, що становлять комерційну таємницю, іншими особами на користь юридичної особи, як правило, відноситься до продукту інтелектуальної власності. У таких випадках комерційна таємниця захищає

інформаційні властивості цих продуктів. До прав власності належать права володіння, користування, розпорядження чи розподілу.

Оскільки власником комерційної таємниці є компанія, вона визначає умови її захисту та доступу до неї, у тому числі у відносинах з іншими компаніями. Відповідно до положень Цивільного кодексу України (ст. 506) право на розголошення комерційної таємниці належить володільцю майнових прав інтелектуальної власності на комерційну таємницю. Іншими словами, підстави, умови та способи захисту інформації, що становить комерційну таємницю, можуть бути різними на різних підприємствах і регламентуються кожним підприємством відповідно до специфіки його діяльності, інформаційних потреб і можливостей. Інформаційні відносини між організаціями щодо комерційної таємниці зазвичай будуються на договірних засадах з урахуванням нормативних документів організацій у сфері захисту інформації.

Окремо регламентується порядок захисту комерційної таємниці організацій у конкурентних відносинах. Так, відповідно до глави 4 Закону України «Про захист від недобросовісної конкуренції» неправомірним є збір відомостей, що становлять комерційну таємницю, у випадках, коли незаконне збирання цих відомостей завдає або може завдати шкоди підприємству. Незаконним є також впровадження у виробництво відомостей, що становлять комерційну таємницю, або їх врахування при плануванні чи здійсненні господарської діяльності без дозволу уповноваженої на це особи (неправомірне використання). Розголошення або заохочення до розголошення комерційної таємниці вважається протиправним [45]. Такі дії суперечать чинному законодавству та можуть тягнути за собою кримінальну, адміністративну та цивільно-правову (компенсаційну) відповідальність.

За порушення комерційної таємниці законодавством України передбачена дисциплінарна, кримінальна, адміністративна та цивільно-правова відповідальність.

Є дві основні цільові групи порушників такої інформації. Ті, хто незаконно володіє таємною інформацією, і ті, хто законно отримує таку інформацію, але порушує зобов’язання щодо її конфіденційності (працівники, підрядники, партнери, клієнти та державні службовці).

Кримінальна відповідальність передбачена за умисне заволодіння відомостями, що становлять комерційну таємницю, з метою їх розголошення чи іншого використання, а також за їх незаконне використання, якщо такими відомостями завдано істотної шкоди господарській діяльності.

Кримінальна відповідальність передбачена також за умисне розголошення комерційної особою, якій ця таємниця відома у зв'язку з професійною або службовою діяльністю, без згоди її володільця, з корисливих чи інших особистих мотивів, якщо це заподіяло істотну шкоду. шкоди суб'єкту господарювання.

Адміністративна відповідальність може наставати, якщо комерційну таємницю було отримано, використано чи розголошено з метою заподіяння шкоди діловій репутації чи майну конкурента.

Цивільним кодексом України передбачено, що інформація є об'єктом цивільних прав і учасники відносин в інформаційній сфері можуть вимагати усунення порушень своїх прав та відшкодування завданої цими порушеннями матеріальної та моральної шкоди.

Враховуючи особливий статус та значний обсяг електронної інформації у комерційній діяльності, законодавець визначив належні правові умови відносин в інформаційній сфері. Основним нормативно-правовим актом тут є Закон України «Про захист інформації в інформаційно-комунікаційних системах». Відповідно до Закону основними об’єктами захисту є інформація, яка використовується в інформаційно-комунікаційних системах, та програмне забезпечення, яке використовується для обробки інформації, а заінтересованими особами є власники інформації, власники системи, користувачі та органи управління, наділені спеціальними повноваженнями у сфері зв’язку та інформації. захисту. . Відносини між сторонами є договірними. Порядок доступу

до інформації, яка обробляється системою, перелік користувачів та їх повноваження визначаються власником інформації. Якщо система обробляє інформацію з обмеженим доступом, доступ до цієї інформації визначається законом. Закон регулює відносини між власником інформації та власником інформаційно-комунікаційної системи, між власниками різних систем та між власником системи та користувачами.

Організація захисту інформації, що обробляється в системі, є обов'язком власника системи. Порушення порядку та правил захисту інформації, що обробляється в інформаційно-комунікаційних системах, може призвести до адміністративної та кримінальної відповідальності.

Сьогодні документообіг в електронному інформаційному просторі є одним із елементів ділового документообігу. Безперечно, воно потребує правового регулювання та захисту. Це питання регулюється двома законами: Законом України «Про електронні документи та електронний документообіг» та «Про електронний цифровий підпис», а також Положеннями «Про технічний захист інформації в Україні» та «Про порядок запровадження Криптографічний захист інформації в Україні» [48], 49, 50, 51.] Ці нормативно-правові акти визначають інституційні та правові основи електронного документообігу, використання електронних документів, правовий статус електронного підпису та регулювання відносин що виникають у зв'язку з їх використанням. Зокрема, законодавчий акт визначає поняття електронного документа та наголошує на його правовому статусі (документ не може бути оскаржений на підставі того, що він створений в електронній формі). Також регламентується обіг документів, що містять інформацію з обмеженим доступом, та їх спеціальний захист в електронних мережах та на електронних носіях. Законом також встановлено, що обов'язковим реквізитом електронних документів є електронний підпис. За своїм правовим статусом він прирівнюється до власноручного підпису (печатки) на умовах, передбачених Законом України «Про електронний цифровий підпис».

"Про електронний цифровий підпис" прирівнюється до власноручного підпису (печатки) на умовах, передбачених Законом України.

Ці правила визначають порядок технічного та криптографічного захисту інформації та інформації з обмеженим доступом.

Організовуючи інформаційну безпеку організації по відношенню до представників ЗМІ, необхідно досконало знати законодавчі акти, що регулюють діяльність ЗМІ. Зокрема, рекомендовано ознайомитись із положеннями законів: «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації», «Про інформацію», «Про друковані засоби масової інформації». (преса) в Україні», «Про телебачення і радіомовлення», «Про інформаційні агентства», «Про авторське право і суміжні права», «Про державну підтримку засобів масової інформації та соціальний захист журналістів», «Про захист суспільної моралі» .

Діяльність організацій інформаційної безпеки часто передбачає взаємовідносини з правоохоронними та судовими органами, а також з органами управління та контролю, які регулюються спеціальним законодавством, що регламентує їх діяльність. Насамперед, це закони України «Про прокуратуру», «Про міліцію», «Про Службу безпеки України», «Про оперативно-розшукову діяльність», «Про основи організації боротьби з організованими особами. осіб». злочинності», «Про судоустрій і статус судів», «Про адвокатуру та адвокатську діяльність», «Про державну контрольно-ревізійну службу», «Про боротьбу з корупцією», «Про оподаткування прибутку підприємств, установ і організацій», а також інші нормативно-правові акти, що регулюють діяльність цих органів.

Питання правового регулювання інформаційної безпеки організацій не можна обійти власними нормативними документами організацій. Такі нормативні документи становлять засновану на законодавчих і нормативних положеннях правову основу для регулювання діяльності організації та встановлення належного інформаційного режиму в інформаційних відносинах з іншими організаціями, контрагентами, замовниками і кредиторами, а також

мають певне значення у відносинах з державними органами. Такі документи обґрунтовують поведінку суб’єктів господарювання в інформаційному полі за різних обставин.

На жаль, сьогодні, як і в сфері інформаційної безпеки господарських організацій в цілому, самі організації не мають стабільної позиції з точки зору нормативних документів і правового регулювання.

З урахуванням цілей, завдань і змісту інформаційної безпеки підприємства, структури організації та набутого досвіду можна запропонувати наступний перелік нормативних документів.

- Положення про комерційну таємницю та її зберігання на підприємствах;

- Положення про конфіденційну інформацію на підприємствах;

- Положення про конфіденційну інформацію на підприємствах;

- Інструкції про порядок підготовки, обліку, зберігання та знищення на підприємстві документів, справ, публікацій і матеріалів, що містять комерційну таємницю та конфіденційну інформацію;

- Положення про захист електронної інформації та електронних документів на підприємствах;

- Інструкції про порядок оформлення документів, що надійшли на підприємство від правоохоронних органів, суду та інших державних органів;

- Положення про архівний фонд та архівну діяльність підприємств;

- Інструкції про проведення внутрішніх розслідувань підприємства;

- Положення про інформаційно-аналітичну роботу підприємства;

- Інструкція з діловодства публічних документів; Інструкція з діловодства приватних документів;

- Положення про використання, поширення та зберігання інформації в процесі діяльності підприємства;

- пам'ятки для працівників підприємства щодо зберігання інформації з обмеженим доступом;

- інші документи [52, 53, 54].

Незважаючи на таку велику кількість документів, усі вони формують правове поле підприємства у сфері забезпечення інформаційної безпеки та обґрунтовують поведінку підприємства в інформаційному середовищі.

Висновки до розділу 1

У розділі проведено аналіз сучасних вимог до побудови та впровадження СУІБ на підприємстві.

Відповідно до наведених основних аспектів інформаційно-технічної безпеки підприємств України визначені основні вектори загроз інформаційним системам, причини та фактори їх виникнення.

Аналіз нормативно-правового регулювання інформаційної безпеки України показав, що незважаючи на відсутність основних системо утворюючих законодавчих актів з питань безпеки підприємницької діяльності, можна зазначити, що правова основа захисту інтересів підприємців все ж таки є. Наявність відповідних положень законодавчих і нормативних актів дає змогу використовувати права підприємців щодо створення системи заходів безпеки своєї діяльності. Разом з тим правова система є однобокою і спрямовує заходи безпеки підприємницької діяльності переважно на її захист, а не на протидію недобросовісним конкурентам і злочинним елементам. Таке положення робить підприємця пасивним, змушеним тільки захищатись. Майже не передбачають з боку підприємця активних його дій з питань безпеки.

Таким чином, нормативна база підприємства з питань інформаційної безпеки не вимагає якихось великих зусиль та витрат для її створення, але вона

є основою для правового захисту як конфіденційної інформації підприємства, так і всієї його діяльності.

Розділ 2 ФОРМУВАННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

Системи захисту інформації повинні забезпечувати безпеку і надійність інформаційних систем підприємства та їх окремих елементів. Таким чином, впровадження та функціонування системи захисту інформації є комплексним завданням, спрямованим на забезпечення безпеки інформаційних ресурсів і стосується всіх підприємств, їх підрозділів та власників бізнес-процесів [46].

У статті визначено наступні основні принципи, яким повинні відповідати системи захисту інформації

- Конфіденційність - характеристика інформації, яка означає, що інформація не може бути отримана неавторизованими користувачами або процесами;

- Цілісність – це характеристика інформації, яка означає, що інформація не може бути змінена неавторизованими користувачами або процесами. Цілісність системи — це характеристика системи, яка означає, що жоден системний компонент не може бути видалений, змінений або доданий у спосіб, який порушує політику безпеки;

- Доступність - властивість системного ресурсу, яка означає, що належним чином авторизований користувач і/або процес можуть використовувати ресурс, не чекаючи більше певного (невеликого) періоду часу, згідно з правилами, встановленими політикою безпеки;

- Підзвітність - дозволяє фіксувати дії користувачів і процесів, використання пасивних об'єктів і чітко ідентифікувати користувачів і процеси, причетні до тієї чи іншої події, з метою запобігання порушенням політики безпеки та/або забезпечення відповідальності за певні дії. Особливості системи.

Незважаючи на стрімкий розвиток інформаційно-комунікаційних технологій, це залишається творчим процесом, оскільки ефективні рішення проблем інформаційної безпеки є унікальними для кожної організації.

Застосування стандартів управління інформаційною безпекою при створенні та впровадженні СУІБ організації дозволяє:

- Оптимізувати витрати на створення та підтримку корпоративної системи захисту інформації;

- постійний моніторинг та оцінка ризиків у світлі цілей компанії;

- ефективно визначати найбільш суттєві ризики та знижувати ймовірність їх виникнення;

- Розробити ефективну стратегію інформаційної безпеки та дотримуватися її реалізації;

- ефективно розробляти, впроваджувати та тестувати корпоративні інформаційні системи та сучасні інформаційно-комунікаційні технології для підтримки господарської діяльності;

Загальна схема системи захисту інформації відповідно до стандарту ISO/IES 27001 наведена на рис. 2.1 [18].

Рис. 2.1. Схема системи захисту інформації відповідно до стандарту ISO/IES 27001

Для цілей даної роботи корпоративна безпека визначається як стабільний стан життєдіяльності, який гарантує реалізацію основних інтересів і пріоритетних цілей компанії та захищений від зовнішніх і внутрішніх дестабілізуючих факторів, незалежно від бізнес-ситуації.

Слід зазначити, що «формальний» підхід до розробки, впровадження та функціонування системи управління інформаційною безпекою, а також незаінтересованість керівництва та працівників у підвищенні рівня інформаційної безпеки не забезпечить зазначене вище описані переваги.

2.1 Сутність безпеки підприємства, її мета, завдання та методи

При створенні та впровадженні системи управління інформаційною безпекою рекомендується використовувати так звані «best practices» (досвід провідних міжнародних компаній, формалізований у вигляді вимог і стандартів).

Відповідно керівництво підприємства повинно забезпечити визначення цілей інформаційної безпеки, їх відповідність вимогам законодавства України та їх інтеграція у відповідні бізнес-процеси та впровадження у спосіб, що відповідає вимогам законодавства України, перевірка ефективності впровадження та функціонування СУІБ, забезпечення необхідними ресурсами для інформаційної безпеки та навчання персоналу з інформаційної безпеки питань. Це перший крок у процесі впровадження СУІБ.

Для вирішення цих завдань необхідно визначити організаційну структуру управління інформаційною безпекою, а також повноваження та відповідальність за розроблення, впровадження та функціонування СУІБ.

Управління СУІБ може здійснюватися керівником або заступником керівника підприємства або діючою організацією управління, наприклад, інформаційним пультом з обов'язковою участю фахівців з інформаційної безпеки.

Залежно від розміру організації ці обов’язки також можуть бути покладені на спеціальний орган управління інформаційною безпекою, який складається з керівників відділів, відповідальних за важливі бізнес-процеси.

У цьому випадку питання інформаційної безпеки або залишаться поза увагою керівників, відповідальних за критичні бізнес-процеси, або питання інформаційної безпеки будуть розглядатися окремо для кожного бізнес-процесу, що не тільки створить додаткові умови для несанкціонованого доступу до інформації та порушення конфіденційності. , але також призведе до додаткових фінансових витрат. У разі необхідності до роботи Колегії з окремих питань можуть залучатися сторонні експерти з питань інформаційної безпеки за умови підписання договорів про конфіденційність.

Діяльність у сфері інформаційної безпеки має координуватися між представниками різних підрозділів організації, які відповідають за функціонування критичних бізнес-процесів/сервісів та забезпечують їх функціонування. Організації повинні створити єдину систему інформаційної безпеки для всіх бізнес-процесів і координувати дії різних підрозділів для забезпечення дотримання загальних вимог інформаційної безпеки. Для виконання цих обов'язків може бути створена окрема група з міжвідомчими обов'язками, до складу якої можуть входити спеціалісти різних відділів. Якщо окрема група з міжвідомчими обов'язками не створюється, ці завдання повинен виконувати спеціальний орган управління або окремий керівник.

Координація інформаційної безпеки зазвичай вимагає співпраці та координації між менеджерами, користувачами, адміністраторами, розробниками програм, аудиторами та персоналом безпеки, а також експертами в таких сферах, як страхування, право, кадри, IT та управління ризиками.

Наступним кроком у процесі впровадження СУІБ є визначення існуючої інфраструктури та заходів безпеки. Це складний процес, який складається з наступних етапів [13]

1) Класифікація інформації. Відповідно до законодавства України про інформацію вся інформація, доступ до якої обмежено, має бути надійно захищена. Відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» та Закону «Про захист персональних даних» підприємства можуть визначати такі категорії інформації з обмежений доступ:

- комерційна таємниця
- особисті дані
- інша конфіденційна інформація

2) Визначення критичних бізнес-процесів та програмно-технічних комплексів, що забезпечують їх функціонування. Відповідно до вимог українських нормативно-правових документів сферою застосування СУІБ є все підприємство. Тому дуже важливо чітко визначити бізнес-процеси/сервіси, які обробляють інформацію з обмеженим доступом і потребують захисту [29].

Короткий опис кожного бізнес-процесу/послуги має містити таку інформацію:

- назва бізнес-процесу/послуги;
- призначення бізнес-процесу/послуги;
- класифікація інформації з обмеженим доступом, яка обробляється бізнес-процесом/сервісом;
- назва бізнес-процесу/послуги;
- призначення бізнес-процесу/послуги;
- власник бізнес-процесу/послуги;
- структурний підрозділ, що забезпечує функціонування бізнес-процесу/послуги;
- назва бізнес-процесу/послуги; - призначення бізнес-процесу/послуги;

- зобов'язання перед третіми особами (контракти на розробку, модифікацію, підтримку та обслуговування);

- вхідні/вихідні дані бізнес-процесу/послуги;

- перелік процедур бізнес-процесу та блок-схема послідовності виконання з визначеними зв'язками (включаючи додаткову вхідну інформацію з інших бізнес-процесів);

- вимоги щодо забезпечення безперервності бізнес-процесу/послуги (максимально допустимий час простою);

- види (групи) ролей бізнес-процесів/сервісів;

- наявність заборонених поєднань рольових типів;

- програмно-технічний комплекс, що забезпечує функціональність бізнес-процесу;

- кількість користувачів програмно-технічного комплексу;

- архітектура та технології роботи (зокрема, обмін файлами або режим реального часу (за наявності), у тому числі обмін інформацією з іншими програмно-технічними комплексами);

- тип операційних систем і баз даних програмно-технічного комплексу, що використовуються для виконання функцій бізнес-процесу/послуги;

- географічне розташування програмно-технічного комплексу (серверів і робочих станцій);

- наявні в програмно-технічному комплексі засоби захисту;

- взаємодія з іншими програмно-технічними комплексами;

- принцип резервування обладнання та інформації в програмно-технічному комплексі (за наявності іншого принципу для цього програмно-технічного комплексу).

3) Опис організаційної структури організації, до якої застосовується СУІБ.

4) Опис структури інформаційних систем підприємства**.** Для подальшого аналізу ІТ-безпеки підприємства необхідно описати структуру інформаційних систем підприємства, їх захист та існуючі засоби управління. Підприємство

повинно мати внутрішній регламент, який містить наступну інформацію про інформаційну систему підприємства:

- опис принципів побудови мережі та принципів резервування мережевого обладнання;

- принципи поділу IP на сегменти (підмережі), якщо такі є;

- принципи розподілу адресного простору;

- Системи управління ІВ;

- створення точок доступу до Інтернет-ресурсів;

- політики доступу до мереж інших організацій (за наявності);

- наявність та правила роботи через канали зв'язку зовнішніх провайдерів телекомунікаційних послуг, у тому числі опис принципів резервування каналів зв'язку;

- засоби захисту інтелектуальної власності від несанкціонованого доступу із зовнішніх і внутрішніх джерел;

- принципи надання доступу до ІБ та ресурсів Інтернет співробітникам підприємства;

- політики та процедури надання віддаленого доступу до ІТ співробітникам компанії;

- принципи та процедури надання бездротового доступу до ІТ компанії, якщо такі є; Принципи та процедури надання бездротового доступу до ІТ підприємства, якщо такі є;

- Принципи резервного копіювання інформації.

5) Визначення фізичного середовища. Захист інфраструктури компанії також є частиною СУІБ.

Підприємства повинні мати такі документи:

- опис географічного та територіального розташування приміщень підприємства, у тому числі відокремлених підрозділів підприємства (наприклад, регіональний центр, філії, відділи тощо) для виявлення загроз із зовнішнього середовища;

- опис принципів роботи системи контролю доступу;

- наказ про визначення заборонених зон та опис відповідної охорони, що забезпечує контроль доступу до цих зон;

- визначення принципів роботи систем відеоспостереження;

- визначення систем електропостачання та заземлення;

- визначення систем охоронної та пожежної сигналізації;

- визначення умов зберігання магнітних, магнітооптичних, паперових та інших носіїв (у тому числі електронних архівів).

6) Визначення принципів забезпечення безперервності бізнесу.

Підприємство повинне регулярно тестувати всі компоненти, необхідні для впровадження планів забезпечення безперервності бізнесу та аварійних процедур, включаючи можливість відновлення резервної інформації, що зберігається у віддалених місцях резервного копіювання.

2.2 Формування вимог до системи управління інформаційною безпекою підприємства

При аналізі інформаційних ризиків слід використовувати моделі систем захисту інформації на основі міжнародних стандартів. Ця робота базується на моделі, побудованій на основі стандартів (ISO 15408 «Загальні критерії оцінки безпеки інформаційних технологій») та даних аналізу ризиків (ISO/IEC 27001:2013 «Інформаційні технології – Технології безпеки – Системи управління інформаційною безпекою)) - Вимоги"). Модель враховує прийняті в Україні окремі нормативні документи з інформаційної безпеки, міжнародний стандарт ISO/IEC 15408 «Інформаційні технології – Технології безпеки – Критерії оцінки

інформаційної безпеки», стандарт ДСТУ СУІБ 1.0/ISO/IEC27001:2010 «Інформаційна безпека». управління». система» та тенденції розвитку національної нормативно-правової бази з питань інформаційної безпеки.

Детальний опис загальної мети створення системи управління інформаційною безпекою організації виражається в сукупності факторів або критеріїв, що визначають мету. Сукупність факторів є основою для визначення системних вимог (вибору варіантів) [43].

На рисунку 2.2 модель інформаційної безпеки відображає сукупність об'єктивних зовнішніх і внутрішніх факторів та їх вплив на стан інформаційної безпеки об'єкта та захищеність матеріальних та інформаційних ресурсів. Фактори безпеки можна поділити на технічні, технологічні та організаційні.

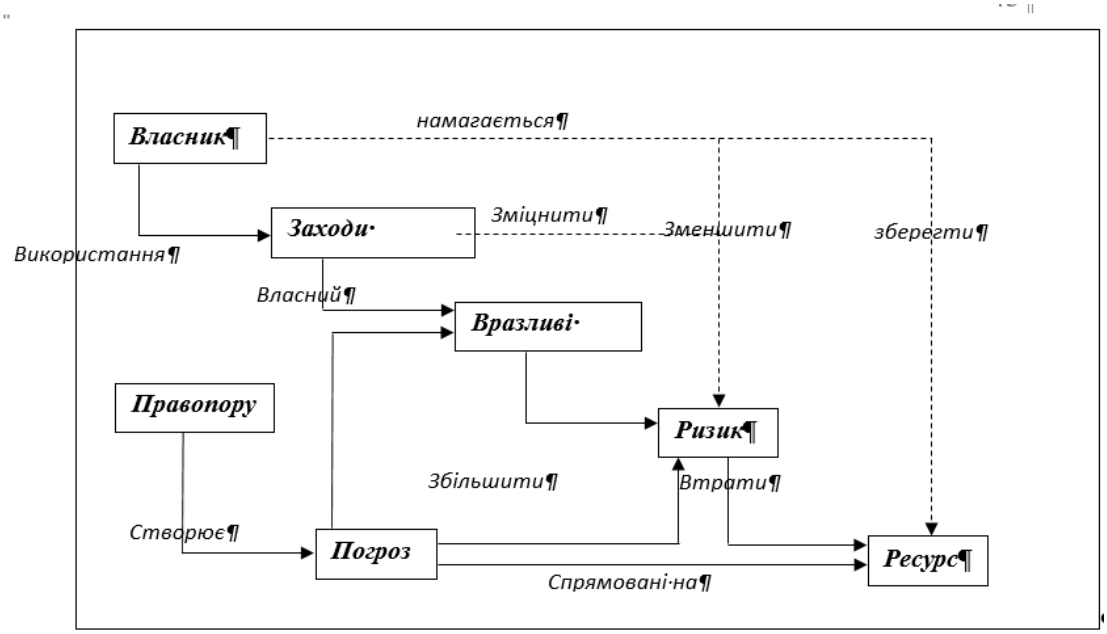

Рис. 2.2. Модель системи інформаційної безпеки підприємства

Процес оцінювання системи управління інформаційною безпекою потребує визначення джерел інформаційної системи. Необхідно відрізняти ці ресурси від зовнішніх елементів, з якими вони взаємодіють. Ресурси включають комп'ютерне обладнання, програмне забезпечення та дані. Прикладами зовнішніх елементів є комунікаційні мережі та інші інструменти.

Визначення взаємозв'язків між ресурсами є основою побудови організаційної моделі інформаційної безпеки.

Цільові елементи моделі:

- загрози інформаційній безпеці підприємства, які характеризуються можливістю реалізації;

- уразливість інформаційних систем або систем протидії (систем захисту інформації);

- ризики - фактори, що відображають можливу шкоду організації в результаті загроз інформаційній безпеці: витік інформації або її неправомірне використання (ризики відображають можливість прямих або непрямих фінансових втрат).

Принципи побудови збалансованої системи інформаційної безпеки організації:

- аналіз ризиків у сфері інформаційної безпеки;

- визначення оптимального рівня ризику для бізнесу на основі встановлених критеріїв;

- вибір заходів, що забезпечують досягнення прогнозованого рівня ризику.

Ця методика дає змогу проаналізувати вимоги до забезпечення інформаційної безпеки підприємства. Для досягнення цієї мети необхідно вирішити певні питання:

- розподіл інформації за рівнями доступу;

- своєчасне прогнозування та виявлення загроз безпеці інформаційних ресурсів;

- створення ситуацій, за яких імовірність виникнення загроз безпеці інформаційних ресурсів є найменшою;

- створення механізмів та умов для забезпечення оперативного реагування на загрози інформаційній безпеці з метою виконання робіт у стислі терміни;

- створити механізми та умови для максимального відшкодування та локалізації шкоди, завданої протиправними діями фізичних та юридичних осіб;

- забезпечити оптимальний вибір заходів;

- оцінити ефективність заходів і порівняти різні варіанти.

На основі моделі можна раціонально підібрати систему протидії, здатну знизити ризик до прийнятного рівня. Важливими елементами контрзаходів є регулярна перевірка ефективності системи, перевірка відповідності існуючої системи захисту інформації політиці безпеки та перевірка відповідності сертифікації інформаційної системи (технічної) вимогам конкретного стандарту безпеки.

Отже, першим етапом моделювання інформаційної безпеки є оцінка ризиків. Метою процесу оцінки ризиків є визначення характеристик інформаційної системи та її ресурсів [33]. На основі цих даних вибираються необхідні засоби управління інформаційною безпекою.

Ризики - це небезпеки, яким може наражатися система та організація, що її використовує. Ризик визначається цінністю ресурсу, ймовірністю пошкодження ресурсу (виражається як ймовірність загрози для ресурсу), ступенем зручності, з якою система захисту від уразливостей може бути використана в разі загрози, а також індикатор існуючих або планованих заходів безпеки інформації.

Процес оцінки ризику складається з кількох етапів: ідентифікація об’єкта та заходів захисту, ідентифікація ресурсів та оцінка їх кількісних показників (визначення можливого негативного впливу на бізнес), аналіз загроз інформаційній безпеці, оцінка слабких сторін, оцінка поточних та майбутніх заходів безпеки інформації, оцінка ризиків .

На етапі профілювання безпеки розробляється проектний план системи захисту інформаційного середовища замовника. Існуючі інструменти оцінюються та аналізуються, а засоби захисту плануються для розробки та інтеграції. Необхідним елементом цієї роботи є вимоги клієнта щодо прийнятних рівнів ризику [21, 37].

Перед розробкою системи технічних рішень необхідно сформулювати політику безпеки організації. Ця політика повинна передусім визначати процедури надання та використання прав доступу користувачів.

Розробка політики безпеки організації складається з кількох етапів:

- додати структуру витрат до опису об'єкта автоматизації та провести аналіз ризиків;

- визначити правила процесу використання таких прав доступу до ресурсів об'єкта автоматизації.

Усі вимоги до функцій безпеки діляться на два види: контроль доступу до інформації та контроль потоку інформації.

На цьому етапі необхідно правильно визначити складові функцій безпеки об’єкта. Компонент функції безпеки визначає певний набір вимог безпеки (мінімальний набір вибраних вимог безпеки, які включені в профіль безпеки). Між компонентами можуть існувати залежності.

Структура вимог до забезпечення результуючої безпеки подібна до структури функціональних вимог і включає класи, групи, компоненти, елементи та рівні достовірності. Класи та групи підтримки відображають такі теми, як розробка, керування конфігурацією, робочі документи, підтримка життєвого циклу, тестування та оцінка вразливостей.

Вимоги до забезпечення виражаються через оцінку можливостей служби інформаційної безпеки об'єкта. Такі оцінки виконуються на рівні окремих механізмів безпеки, які можуть визначити здатність відповідних функцій безпеки протистояти виявленим загрозам. Залежно від відомої ймовірності атаки надійність функції безпеки визначається, наприклад, категоріями «базова», «середня» і «висока».

Імовірність атаки визначається шляхом аналізу можливостей, ресурсів і мотивації зловмисника. Рекомендується використовувати зведену таблицю рівнів безпеки. Рівні гарантії структуровані ієрархічно, і кожен наступний рівень забезпечує гарантії та включає всі вимоги попереднього рівня. [29]

Перелік вимог, ескізний проект та план захисту системи захисту інформації (далі – технічний документ, ТД) є вимогами до безпеки інформаційного середовища на об’єкті замовника та можуть містити посилання на відповідні профілі захисту та чітко сформульовані вимоги.

У загальному вигляді ТД визначає:

- визначення функцій безпеки;

- вибір архітектурних принципів побудови систем захисту інформації;

- формулювання логічної структури системи захисту інформації (чітке визначення інтерфейсів);

- уточнення функціональних вимог щодо забезпечення надійності системи захисту інформації;

- Розробка методик і програм тестування на відповідність сформульованим вимогам.

На етапі оцінки досягнутого рівня безпеки проводиться оцінка рівня безпеки інформаційного середовища об’єкта автоматизації на основі оцінки надійності інформаційного середовища об’єкта після впровадження запропонованих заходів.

Одне з основних припущень цієї методології полягає в тому, що ступінь гарантії безпеки залежить від ефективності зусиль, витрачених на оцінку безпеки. Збільшення цих зусиль означає

- значне збільшення кількості елементів інформаційного середовища об'єкта, залучених до процесу оцінювання

- розширений опис типів проектів та їх реалізації при розробці систем безпеки; і

- більш ретельний підхід до роботи, тобто використання більшої кількості дослідницьких інструментів і методів для виявлення менш очевидних недоліків або зменшення ймовірності їх наявності.

Висновки до розділу 2

Система інформаційної безпеки повинна забезпечити безпечність і надійність функціонування системи та окремих її елементів. Тому впровадження та функціонування системи інформаційної безпеки є комплексним завданням, спрямованим на забезпечення безпеки інформаційних ресурсів, їхніх підрозділів і власників підприємств. Виділено базові принципи, яким повинна бути система інформаційної безпеки.

У розділі сформульовано мету, завдання та основні методи, які використовуються при створенні системи управління інформаційною безпекою підприємства.

Розглянута методика дає змогу оцінити або переоцінити поточний стан інформаційної безпеки підприємства, виробити рекомендації щодо її гарантування (підвищення), знизити потенційні втрати підприємства за рахунок підвищення стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки підприємства, а також запропонувати плани захисту його конфіденційної інформації, що передається відкритими каналами зв'язку, захисту інформації підприємства від умисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання або використання.

Розділ 3 РОЗРОБКА ПІДХОДУ ДО СТВОРЕННЯ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

3.1 Формалізація системи управління інформаційною безпекою підприємства

Розділ 2 визначає, що корпоративна безпека – це стабільний стан життєдіяльності, який забезпечує реалізацію головних інтересів і пріоритетних цілей і захист від зовнішніх і внутрішніх дестабілізуючих факторів, незалежно від стану управління. Тому в процесі розробки концепції корпоративного управління необхідно визначити основні операційні процеси та виключити можливість витоку інформації, зловживань, збитків та упущеної вигоди для всіх зацікавлених сторін і в напрямку досягнення основних цілей діяльності [14]. Реалізація цих положень гармонійно вписується в концепцію корпоративного управління господарською діяльністю і зараз використовується все більшою кількістю компаній. (Рис. 3.1).

Рис. 3.1. Взаємозв'язок системи захисту інформації із загальною системою корпоративного управління підприємством

Основним критерієм ефективності та якості інформаційної безпеки підприємства є його сталий розвиток відповідно до планів і цілей, незалежно від обставин, що змінюються.

Цілі безпеки досягаються шляхом виконання відповідних завдань, таких як:

- захист законних інтересів підприємства та його працівників;

- попередження та припинення правопорушень і злочинних посягань на майно підприємства та його працівників;

- своєчасне виявлення реальних і потенційних загроз бізнесу та вжиття заходів щодо їх нейтралізації;

- виявлення внутрішніх і зовнішніх причин і ситуацій, які можуть завдати матеріальної, моральної чи іншої шкоди підприємству, його працівникам, клієнтам і акціонерам і сприяти перешкоджанню його нормального функціонування;

- оперативне реагування елементів корпоративної структури на загрози та негативні тенденції зовнішнього та внутрішнього середовища; виявлення та

формування сприятливих причин і умов для реалізації основних інтересів підприємств; навчання та навчання співробітників компанії з питань безпеки;

- зменшення шкідливих наслідків дій конкурентів і злочинців, спрямованих на підрив безпеки підприємства; захист та ефективне використання фінансових, матеріальних та інформаційних ресурсів підприємства.

Організація корпоративної безпеки здійснюється за принципом центрального стратегічного спрямування цієї діяльності на рівні менеджменту (табл. 3.1).

Таблиця 3.1

Вимоги до ефективності організації безпеки підприємства

Безперервність безпеки	Безпека не може бути тимчасовою. Це безперервний процес, який включає найбільш раціональні форми, методи та засоби створення, удосконалення та розвитку системи безпеки, її постійний контроль, а також обґрунтування та здійснення контролю за її функціонуванням.
Планування безпеки	Заходи безпеки не повинні бути епізодичними або відставати від реальних подій. Планування стосується рівня та характеру безпеки
Специфіка безпеки	Необхідно захистити конкретні цілі, а загрози можуть завдати шкоди організації.
Проактивна безпека	Постійні зусилля, спрямовані на виявлення загроз для організації та їх своєчасну та ефективну нейтралізацію
Універсальна безпека	Заходи безпеки повинні охоплювати всі можливі аспекти загроз, незалежно від їх розташування.

Складність безпеки	Для забезпечення безпеки необхідно максимально повно використовувати всі форми і методи захисту та протидії загрозам.

При цьому надійність і ефективність безпеки визначається виконанням вимог.

Розглядаючи IT-безпеку підприємства як багаторівневу систему, необхідно визначити її тип та організаційну форму. Типи організаційної безпеки включають наступне [43]

Особиста безпека - це здатність кожного працівника підприємства протистояти загрозам здоров'ю, життю та професійній діяльності на основі засвоєння норм і правил безпечної поведінки. Це досягається шляхом забезпечення дотримання всіма працівниками заходів безпеки, передбачених умовами праці та нормами особистої поведінки. Спеціальні заходи безпеки для співробітників компанії, завдяки яким кожен співробітник засвоює правила поведінки в складних або екстремальних ситуаціях і грамотно діє в них;

Колективна безпека - це здатність підрозділів компанії забезпечувати ефективну діяльність в умовах дії різноманітних дестабілізуючих факторів. Це створення доброзичливої та мирної атмосфери в колективі, дотримання принципів справедливості, грамотне стимулювання праці, постійне вивчення психологічної обстановки в колективі, своєчасне виявлення підвищеної напруженості у відносинах співробітників, попередження та швидке вирішення конфліктних ситуацій, здійснення заходів безпеки, охорони території, будівель і земельних ділянок, забезпечення постійного стану будівель і обладнання. Це забезпечується обстеженням та паспортизацією приміщень та виконанням протипожежних заходів;

Економічна безпека – це стан, за якого забезпечується економічний розвиток і стабільність підприємства, гарантується збереження фінансових і

матеріальних ресурсів, здатність адекватно і без істотних втрат реагувати на зміни внутрішніх і зовнішніх умов. Це передбачає створення дієвого комплексу заходів щодо захисту інформаційних ресурсів компанії та запобігання відтоку коштів шляхом підробки фінансових документів; Наявність приміщень для зберігання грошових коштів, матеріальних цінностей, технічних засобів, транспортних засобів та обладнання, що відповідають встановленим вимогам, їх уміла експлуатація, охорона праці на підприємстві та заходи безпеки досягаються належною організацією техніки безпеки, дбайливим ставленням до майна підприємства. та створення обставин суворої та невідворотної відповідальності за фізичну та інформаційну крадіжку.

Інформаційна безпека - це ефективний захист усіх видів інформації від зовнішніх і внутрішніх загроз, забезпечення необхідного рівня поінформованості керівництва компанії, співробітників і зовнішнього середовища. Це включає збір інформації про внутрішнє та зовнішнє середовище компанії; проведення інформаційно-аналітичних досліджень про клієнтів, партнерів і конкурентів; проведення інформаційного аудиту та інформаційного моніторингу компанії; аналіз та обробка інформації; організація системи інформаційного забезпечення прийняття рішень керівництвом підприємства; визначення та захист категорій конфіденційної інформації. Це реалізується шляхом розроблення відповідних заходів, дотримання відповідних форм діяльності підприємства та забезпечення дотримання всіма працівниками відповідних правил. Заходи корпоративної безпеки реалізуються у вигляді захисту (фізичного та технічного), організації (впровадження відповідних систем захисту корпоративної інформації) та інформаційно-аналітичного забезпечення діяльності підприємства (ділової інформації).

Основні об'єкти захисту на підприємствах:

- персонал суб'єкта господарювання (виконавче та вище керівництво суб'єкта господарювання, особи, які мають доступ до таємниці суб'єкта господарювання, інші працівники);

- матеріальні цінності (будівлі, склади, обладнання, транспорт, інформаційно-технічні засоби і системи);

- інформаційні ресурси організації, доступ до яких обмежений (відомості, що становлять комерційну таємницю та конфіденційну інформацію суб'єкта господарювання).

Основними елементами системи інформаційної безпеки компанії є заходи безпеки, технології безпеки, сили безпеки та засоби безпеки. До загальних заходів забезпечення інформаційної безпеки належать: організаційно-правовий вплив на діяльність працівників підприємства та клієнтів, пов'язану з питаннями безпеки; підбір, перевірка та управління працівниками; розробка ефективної кадрової політики та програм стимулювання праці; організація корпоративної безпеки, спеціального адміністрування; захист корпоративних інформаційних ресурсів, розробка технологій виробництва, впровадження елементів захисту, формування позитивного іміджу підприємства, планування та надання послуг із захисту інформації.

До конкретних заходів безпеки інформації належать: організація та впровадження бізнес-розвідки; створення інформаційних ресурсів підприємств; інформаційно-аналітичне дослідження клієнтів, партнерів і конкурентів підприємства; взаємодія з правоохоронними органами з метою забезпечення безпеки підприємства; запобігання, виявлення та локалізація проявів недобросовісної конкуренції та промислового шпигунства, а також дій і поведінки. Це, зокрема, здійснення заходів із забезпечення здійснення заходів протидії, виявлення та локалізації актів недобросовісної конкуренції та промислового шпигунства; проведення внутрішніх розслідувань підприємств; здійснення заходів щодо запобігання наданню конкурентами інформації конкурентам.

3.2 Рекомендації щодо створення ефективної системи управління інформаційною безпекою підприємства

Відповідно до стандарту ISO/IEC 27001, практики інформаційної безпеки повинні реалізовуватися такими способами:

- встановлення політики системи управління інформаційною безпекою;
- забезпечення відповідності цілей системи управління заходам інформаційної безпеки;
- визначення ролей та відповідальності за інформаційну безпеку;
- доведення до відома персоналу організації важливості впровадження та дотримання політики інформаційної безпеки;
- забезпечення відповідними ресурсами для підтримки інформаційної безпеки;
- створення системи управління ризиками для забезпечення належного рівня інформаційної безпеки;
- проведення внутрішнього аудиту систем управління інформаційною безпекою;
- перегляд прийнятих керівництвом управлінських рішень для забезпечення належного рівня інформаційної безпеки.

Реалізацію та підтримку заходів із захисту інформації забезпечує служба безпеки підприємства, спеціалізовані підприємства організації безпеки, інформаційно-комунікаційних технологій і технічних засобів захисту інформації.

Одним із ключових елементів створення системи інформаційної безпеки підприємства є створення системи управління ризиками підприємства.

3.3 Методика оцінки ризику

Аналіз ризиків можна проводити з різним ступенем деталізації в залежності від критичності ресурсу/бізнес-процесу/послуги СУІБ, відомих вразливостей і попередніх інцидентів інформаційної безпеки. Методи оцінки ризику можуть бути кількісними, якісними або комбінованими. На практиці зазвичай спочатку проводиться якісна оцінка для визначення загального рівня ризику та визначення основних ризиків. Тоді може знадобитися більш конкретний або кількісний аналіз основних ризиків. Кількісна оцінка ризиків складніша і вимагає більше часу та ресурсів. Однак такі оцінки можуть бути дуже корисними, коли рішення щодо усунення ризику залежить від вартості заходів безпеки, яка може бути більшою, ніж економічні втрати у випадку інциденту інформаційної безпеки.

Методи якісної оцінки ризику використовують шкалу атрибутів для опису величини потенційних наслідків загрози та ймовірності виникнення цих наслідків. Перевага якісних методів полягає в тому, що вони легко зрозумілі всім співробітникам. Недоліком цього підходу є те, що він покладається на суб’єктивний вибір шкал ознак.

Для проведення якісної оцінки ризику необхідно оцінити наслідки загрози та потенціал використання уразливості для кожного бізнес-процесу/послуги, мережі, обладнання, програмного забезпечення, що забезпечує функціонування бізнес-процесу/послуги, загальної організаційної ІТ, фізичне середовище, персонал тощо. Необхідно розглянути оцінку впливу загрози та можливість використання вразливості.

Для проведення оцінки ризику необхідно визначити шкалу різних параметрів:

- Оцінка ступеня впливу загрози на служби безпеки (цілісність, конфіденційність, доступність і спостережливість),

- Оцінка ймовірності того, що загроза стане реальністю.

Загальний рейтинговий рівень впливу кожної загрози на служби безпеки визначається як максимальне значення індивідуальних рейтингів впливу на цілісність, конфіденційність, доступність і спостережливість.

Рівень ризику окремих пар загроз і вразливостей, які можуть бути використані для реалізації цієї загрози, визначається шляхом множення загального рівня оцінки наслідків на ступінь ймовірності реалізації загрози.

Загальний рівень ризику для бізнес-процесу/послуги, персоналу, фізичного середовища тощо дорівнює максимуму всіх ризиків для кожної пари загроза/вразливість.

У дипломній роботі рекомендовано використовувати наступну шкалу оцінки ризику:

Таблиця 3.2

Шкала оцінки ймовірності реалізації загроз

Оцінка ймовірності	***Опис***
1	Виникнення інциденту практично неможливо
2	Виникнення інциденту малоймовірно (не частіше 1 разу на 1 рік)
3	Інцидент трапляється раз на 3 місяці
4	Виникнення інциденту ймовірно до 1 разу на тиждень
5	Виникнення інциденту ймовірно до 1 разу на добу

Таблиця 3.3

Масштаб наслідків реалізації загрози: вплив на цілісність

Оцінка рівня наслідків	***Опис***
1	Невеликі фінансові втрати або їх відсутність
2	Заподіює незначні фінансові збитки (вказати суму) та незначно впливає на репутацію підприємства
3	Спричиняє значні фінансові збитки (вказати суму) та суттєво впливає на репутацію підприємства
4	Спричиняє значні фінансові збитки (вказати суму) та суттєво впливає на репутацію підприємства та може призвести до призупинення бізнес-процесів
5	Призводить до призупинення бізнес-процесів та порушує законодавство України.

Таблиця 3.4

Масштаб наслідків реалізації загроз: вплив на конфіденційність

Оцінка рівня наслідків	***Опис***
1	Майже не призводить до значного розголошення конфіденційної інформації

2	Призводить до розкриття певних документів, що містять «комерційну таємницю» або «особисту інформацію», і не призводить до фінансових втрат
3	Призводить до розголошення певних документів, що становлять комерційну таємницю або особисту інформацію, і призводить до незначних фінансових втрат.
4	Призводить до розголошення певних документів, що становлять «комерційну таємницю» або «інформацію про особу» та призводить до значних фінансових втрат, які можуть суттєво вплинути на репутацію підприємства та призвести до призупинення бізнес процеси.
5	Призводить до призупинення бізнес-процесів та порушує законодавство України.

Таблиця 3.5

Масштаб наслідків реалізації загроз: вплив на доступність

Оцінка рівня наслідків	***Опис***
1	Незначний вплив на доступність
2	Незначний вплив на доступність незначний (менше 1/10 максимально допустимого простою для цього бізнес-процесу)
3	Помірний вплив на доступність (менше L від максимально допустимого простою для цього бізнес-процесу)

4	Значний вплив на доступність (до максимально допустимого простою для конкретного бізнес-процесу)
5	Бізнес-процес не працює протягом тривалого часу, що перевищує максимально допустимий час простою)

Таблиця 3.6

Масштаб наслідків реалізації загрози: вплив на спостережливість

Оцінка рівня наслідків	***Опис***
1	Практично не впливає
2	Ефект незначний
3	Унеможливлює моніторинг деяких дій виконавців бізнес-процесів.
4	Унеможливлює контроль за поведінкою виконавців та керівників бізнес-процесу/програмно-технічного комплексу.
5	Унеможливлює контроль за діями виконавців та керівників бізнес-процесу/програмно-технічного комплексу, які можуть призвести до зупинки бізнес-процесу, вплинути на репутацію підприємства та порушити законодавство. України.

При визначенні конкретних значень параметрів оцінки враховуються досвід відповідних співробітників компанії, вимоги нормативного законодавства України, історія попередніх інцидентів інформаційної безпеки, відомі випадки

порушень інформаційної безпеки та досвід інших організацій. слід брати до уваги. в обліковому записі.

Рівень ризику конкретної пари загроз і вразливостей, які можуть бути використані для реалізації цієї загрози, визначається множенням рівня загальної оцінки наслідків на оцінку ймовірності реалізації загрози. Загальний рівень оцінки впливу на службу безпеки в разі реалізації кожної пари загроз і вразливостей визначається як максимальне значення індивідуальних оцінок впливу на цілісність, конфіденційність, доступність і спостережуваність.

Загальний рівень ризику бізнес-процесу дорівнює максимальному значенню загального ризику кожної пари загроз вразливостей.

У разі використання кількох програмно-технічних комплексів для одного бізнес-процесу та наявності відмінностей у системах захисту інформації необхідно детально визначити місце розташування загрози/вразливості для кожної пари загроза/вразливість. Особливу увагу слід звернути на безпеку інтерфейсів обміну інформацією між програмними та апаратними системами.

Такий підхід до оцінки ризиків дозволяє чітко визначити найбільші ризики та найбільш значні загрози в бізнес-процесах.

Наступним етапом оцінки ризиків є управління ризиками. Після завершення оцінки ризику компанія повинна оцінити альтернативні варіанти управління ризиками.

Можливі варіанти реагування на ризик включають:

- Зниження ризиків шляхом впровадження відповідних заходів безпеки

- Свідоме та об'єктивне прийняття ризику за умови чіткого дотримання політики організації та критеріїв прийняття ризику;

- Уникнення ризику.

- Передача відповідних ризиків іншим сторонам (наприклад, страховикам, постачальникам).

Щоб визначити, як боротися з конкретними ризиками, корисно визначити наступні критерії для окремих ризиків

- Низький ризик - 1 - 6

- Середній ризик - 7 - 14

- Високий ризик - 15 - 25

Необхідно вжити відповідних захисних заходів, щоб зменшити ризики. При виборі таких додаткових заходів безпеки необхідно враховувати всі вимоги законодавства України, нормативно-правових актів, внутрішніх документів, політики та стратегії компанії. Також при виборі слід враховувати вартість додаткових заходів безпеки, час їх реалізації, вплив на технологію виконання оперативних завдань, інтерфейс користувача тощо. З урахуванням цих факторів розробляється план управління ризиками. Якщо для підготовки до впровадження додаткових заходів безпеки потрібен час, деякі ризики можуть бути тимчасово визнані залишковими та включені до наступного плану управління ризиками з переглянутою оцінкою ризиків.

Прийняття всіх залишкових ризиків має бути задокументовано та схвалено керівництвом. Це середній або високий ризик, і його слід ретельно розглянути. Документація про прийняття залишкових ризиків повинна містити причини прийняття ризику та, за необхідності, терміни впровадження додаткових заходів безпеки для зниження ризику. Наприклад, якщо організація використовує застарілу програмно-апаратну систему з високим ризиком однієї або кількох загроз і планує замінити її новою, більш сучасною системою протягом двох років, ці ризики Нова система може розглядатися як проміжне рішення і нова система може бути впроваджена

Деякі ризики притаманні існуючим бізнес-процесам/послугам/програмному та апаратному забезпеченню. Особливу увагу слід звернути на вразливість програмно-технічних комплексів, які використовують застарілі або незахищені нові технології. У деяких випадках слід уникати ризиків, змінюючи робоче середовище, бази даних, апаратно-програмні комплекси, технології обробки та зберігання інформації.

3.4 Організація процесу управління інформаційною безпекою підприємства

У будь-якій інформаційній системі з точки зору інформаційної безпеки виділяють чотирьох учасників інформаційного обміну: відправника інформації, одержувача інформації, зловмисника і арбітра.

Політику безпеки можна визначити як набір законів, правил і практик, які регулюють управління, захист і розподіл критичної інформації в системі.

Політика безпеки повинна охоплювати всі етапи обробки інформації і визначати поведінку системи в різних ситуаціях. Тому при розробці політики безпеки системи необхідно враховувати основні принципи, яких необхідно дотримуватися при побудові системи безпеки, а також оцінювати ризики, які можуть виникнути у разі загрози від порушення безпеки. системи різними елементами інформаційної системи компанії [37].

Як зазначалося в розділі 2, особливим напрямком забезпечення інформаційної безпеки на підприємстві є захист інформаційних систем. Тому при розробці архітектури та побудові інфраструктури інформаційних систем компанії необхідно передбачити захист від загроз. Вирішенням цієї проблеми є детальний аналіз проектування та впровадження інформаційних систем, їх документування, аудити, дослідження безпеки та інші взаємопов’язані дії на підприємстві.

Концепція захисту інформаційних систем підприємства включає низку законодавчих ініціатив, науково-технічних і технологічних рішень, які дають змогу забезпечити надійний рівень інформаційної безпеки (табл. 3.8).

Таблиця 3.8

Трирівнева модель проблеми безпеки ІБ підприємства

Система цілей	*Загальна мета:*	захист банківської інформаційної системи
	Цілі:	– безпека; – безвідмовність; – ділова взаємодія
Засоби	*Настанови:*	– захищеність; – конфіденційність; – цілісність; – готовність до роботи; – точність; – керованість; – безвідмовність; – прозорість; – зручність використання
	Підтвердження:	– внутрішня оцінка; – акредитація; – зовнішній аудит
Виконання	*Забезпечення:*	– закони, норми; – характер організації банківської діяльності; – договори, зобов'язання; – внутрішні принципи; – міжнародні стандарти банківської діяльності
	Реалізація:	– методи взаємодії із зовнішнім і внутрішнім середовищем; – методи здійснення банківських операцій; – аналіз банківських ризиків; – методи розроблення та впровадження банківських інформаційних систем; – експлуатація та супровід банківських інформаційних систем; – навчання персоналу

Заходи захисту інформації в засобах і мережах її передачі та обробки в основному передбачають використання апаратних, програмних і криптографічних засобів захисту (табл. 3.9).

*Таблиця*3.9

Засоби захисту інформації

Апаратні	Програмні	Криптографічні
Організаційні забезпечують регламентацію доступу і використання технічних засобів передачі та обробки інформації; Організаційно-технічні забезпечують блокування можливих каналів витоку інформації через технічні засоби забезпечення виробничої і трудової діяльності за допомогою спеціальних технічних засобів, що встановлюються на елементи конструкцій будівель і споруд, приміщень і технічних засобів, потенційно створюючи канали витоку інформації; Технічні забезпечують використання в процесі виробничої діяльності спеціальних, захищених від побічних випромінювань технічних засобів передачі та обробки конфіденційної інформації	Спеціалізовані забезпечують ідентифікацію об'єктів і суб'єктів, розмежування доступу до банківських інформаційних ресурсів, контроль і реєстрацію дій з банківською інформацією і програмами; Універсальні забезпечують ідентифікацію середовища, з якого буде запускатися програма, аутентифікацію середовища, з якого запущена программа, відклик на запуск з несанкціонованого середовища, реєстрацію санкціонованого копіювання, протидії вивченню алгоритмів роботи системи	забезпечують такий захист інформації, при якому у разі перехоплення її та обробки будь-якими способами, вона може бути дешифрована тільки протягом часу, необхідного їй для втрати своєї цінності

Функції безпеки обладнання можна розділити на функції виявлення та функції захисту для запобігання несанкціонованому доступу. Слід зазначити, що існують заходи виявлення та захисту для кожної функції залежно від типу перешкод, оскільки не існує універсального засобу захисту. За таких обставин заходи проти несанкціонованого видалення інформації за допомогою апаратного

захисту досить трудомісткі та дорогі та вимагають спеціальної підготовки спеціалістів із безпеки [5].

На практиці всі заходи щодо застосування апаратних засобів захисту можна розділити на три групи: організаційні заходи, організаційно-технічні заходи та технічні заходи.

Організаційні заходи апаратного захисту — це обмежувальні заходи, які передбачають регламентацію доступу та використання технічних засобів передачі та обробки інформації.

Організаційно-технічні заходи — це заходи, що забезпечують блокування можливих шляхів витоку інформації за допомогою спеціальних технічних засобів, розміщених у конструктивних елементах будівель і споруд, установках і технічних засобах, що забезпечують виробничо-трудову діяльність.

Технічні засоби - це заходи, що забезпечують використання під час виробництва спеціальних технічних засобів передачі та обробки конфіденційної інформації, захищених від побічного випромінювання.

Програмний захист – це система спеціальних програм, які входять до складу програмного забезпечення комп’ютерно-інформаційних систем і реалізують функції захисту інформації з обмеженим доступом від протиправних дій та програм для її обробки [18].

Програмне забезпечення захищає інформацію від несанкціонованого доступу, копіювання та знищення.

При використанні програмних засобів захисту інформації від несанкціонованого доступу вони виконують такі функції:

- Ідентифікація суб'єкта і об'єкта;
- розмежування доступу до джерел інформації
- Контроль та фіксація дій, спрямованих проти інформації та програм.

Захист інформації від копіювання забезпечується такими функціями:

- Ідентифікація середовища, в якому виконується програма;
- Аутентифікація середовища, з якого запускається програма;

- Реакція на запуск з неавторизованого носія;

- Видача завірених копій;

- стійкість до перевірки алгоритмів системи.

Заходи шифрування - це використання спеціальних пристроїв, програм або відповідних дій, які роблять передані сигнали абсолютно незрозумілими для сторонніх. Заходи шифрування гарантують, що інформація захищена таким чином, що у разі перехоплення та будь-якої обробки її можна вчасно розшифрувати, перш ніж її цінність буде втрачена. Для цього використовуються різні спеціалізовані засоби шифрування документів, голосових і телеграфних повідомлень.

Для створення моделей інформаційної безпеки використовується ряд спеціалізованих методів

- Порівняння - процес первинної оцінки знань, заснований на порівнянні елементів знання з відомими закономірностями і пошуку подібності між ними;

- Аналіз - процес розкладання інформації, представленої у вигляді об'єктів, подій і явищ, на складові елементи і детальне вивчення їх окремих характеристик. Провідну роль у цьому процесі відіграють свідомість і підсвідомість;

- Побудова моделей відомих об'єктів, процесів і явищ (ситуацій, видів діяльності) з окремих компонентів, передбачення їх розвитку в часі і прогнозування індивідуальної поведінки;

- Узагальнення - опис невідомого предмета чи явища як відомого з точки зору певних загальних властивостей. Узагальнення має як корисні, так і небезпечні елементи.

Корисний – уміння об’єднувати предмети та явища у великі групи за малими групами основних ознак. Проте об'єктивний стан цих об'єктів і явищ може спотворюватися через надмірне зменшення другорядних ознак в узагальнених моделях;

- Виключення – це процес зосередження уваги на відповідних аспектах особистого досвіду аналітика та виключення решти. Це дозволяє аналітику швидко знаходити необхідну форму відповіді в ситуаціях, що часто повторюються, зосереджуючись на відповідних частинах поточного досвіду. Ця функція дозволяє усунути непотрібні зовнішні подразники у свідомості;

- Абстрагування - відокремлення предмета, явища або елемента інформації від дійсності;

- Трансформація - перетворення сприйнятої інформації відповідно до створеної моделі. Трансформація лежить в основі уяви, передбачення та всіх видів творчої діяльності.

Загалом для забезпечення інформаційної безпеки під час проектування інформаційної інфраструктури підприємства та впровадження інформаційних систем підприємства має бути передбачено створення відповідної системи відстеження та протидії загрозам комерційній діяльності (системи захисту інформації). Загальна структура системи захисту інформації, яка відповідає вимогам, що вивчаються в дипломній роботі, представлена на рис. 3.2.

Рис. 3.2. Система інформаційної безпеки підприємства

Використовуючи новітні інформаційно-комунікаційні технології для управління інформаційною безпекою, компанії зможуть більш адекватно реагувати на різноманітні загрози та нові виклики. У довгостроковій перспективі підвищення інформаційної та IT-безпеки забезпечить стійкий розвиток японської економіки.

Тому питання захисту корпоративних інформаційних систем є надто серйозним, щоб ставитися до нього легковажно. Останнім часом сталася низка інцидентів, пов'язаних з порушенням інформаційної безпеки. Одним із прикладів є публічна доступність різноманітних баз даних про компанії та фізичних осіб. Теоретично в нашій країні існує законодавча база щодо захисту комерційної інформації, але її реалізація далека від досконалості. Поки що випадків покарання компаній за витік інформації чи спробу отримати конфіденційну інформацію не було.

Сучасна глобальна тенденція полягає в тому, що компанії готуються до ризиків для своїх інформаційних систем. Оскільки майже вся діяльність у сучасній економіці та бізнесі залежить від інформаційних систем, такі ризики можуть завдати значної шкоди компаніям, якщо вони матеріалізуються. Існує низка технічних, методологічних та організаційних бар’єрів, подолання яких дозволяє істотно знизити інформаційні ризики підприємств, а також інтегрувати такі ризики в системи управління інформаційною безпекою відповідно до вимог міжнародних стандартів.

Висновки до розділу 3

Формування системи управління інформаційної безпекою та її IT-підтримка є важливою складовою забезпечення ефективності процесів функціонування як окремих підприємств, так і економічного сектора України в цілому. При цьому стратегія управління інформаційною безпекою повинна органічно входити не лише до складу системи управління підприємством, а й задовольняти загальну стратегію розвитку інформаційних технологій відповідно до критеріїв системності та комплексності. Узагальнено, інформаційна безпека є

комплексним завданням, спрямованим на забезпечення безпеки інформаційних ресурсів, що передбачає встановлення загроз і зниження ризиків діяльності, організацію ефективної інформаційно та технічної підтримки управління цими процесами на основі використання сучасних інформаційно-комунікаційних технологій і технічних засобів.

Необхідність впровадження на підприємствах України стандартів з управління інформаційною безпекою продиктована вимогами Базельського комітету Basel II та рядом міжнародних стандартів, вимог законодавства ЄС. Тому система управління інформаційною безпекою, яка покликана забезпечити безпеку інформаційних ресурсів підприємств в цілому, повинна спиратись на національні законодавчі норми та стандарти з управління інформаційною безпекою, а також використовувати досвід кращих світових практик і міжнародних стандартів і рекомендацій.

Процес формування системи інформаційної безпеки підприємств України та затвердження відповідних стандартів зумовлено викликами сьогодення й активно розвивається, тому питання формування системи інформаційної безпеки як на рівні підприємств та організацій, так і на державному рівні є актуальними й потребують подальших досліджень.

ВИСНОВКИ

Інформаційна ера принесла кардинальні зміни в те, як багато професій виконують свої завдання. Завдання, які раніше виконували висококваліфіковані програмісти, тепер можуть виконувати нетехнічні спеціалісти середнього рівня. Водночас використання таких технологій створює ряд проблем для будь-якої організації та її керівників. Сьогодні компанії вживають різноманітних заходів для боротьби з несанкціонованим доступом і розголошенням комерційної інформації, а також для притягнення до відповідальності порушників. Метою даного дослідження є підвищення ефективності систем управління інформаційною безпекою організацій в сучасних умовах розвитку інформаційних технологій.

Процес впровадження та функціонування системи захисту інформації є комплексним завданням, спрямованим на забезпечення безпеки інформаційних ресурсів і актуальним для всіх підприємств, їх підрозділів та власників бізнес-процесів. В ході виконання роботи досліджено підхід до створення системи управління інформаційною безпекою підприємства та запропоновано методи підвищення її ефективності.

Результати цієї кваліфікаційної роботи такі:

1) Проведено аналіз систем управління інформаційною безпекою організацій;

2) Визначено ключові аспекти інформаційно-технологічної безпеки організації та їх вплив на здатність бізнесу виконувати свою місію.

3) Запропоновано модель інформаційних загроз у корпоративній інформаційній системі

4) Встановлено вимоги до створення системи управління інформаційною безпекою підприємства на основі українських галузевих стандартів;

5) Формальна система управління інформаційною безпекою організації;

6) Рекомендації щодо підвищення ефективності системи управління інформаційною безпекою організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про підприємства в Україні: Закон України від 27.03.1991 р. Закони України. Київ: 1996. Т.1.
2. Про інформацію: Закон України від 02.10.1992 р. Закони України. Київ: 1996. Т.4.
3. Основі законодавства України про охорону здоров'я: Закон України від 19.11.1992 р. Закони України. Київ: 1996. Т.4.
4. Про адвокатуру: Закон України від 19.12.1992 р. Закони України. Київ: 1996. Т.4.
5. Про науково-технічну інформацію: Закон України від 25.06.1993 р. Закони України. Київ: 1996. Т.5.
6. Про захист інформації в автоматизованих системах: Закон України від 5.07.1994 р. Закони України. Київ: 1997. Т.7.
7. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність. Навчальний посібник. Київ: Атіка, 2002. 240 с.
8. Близнюк І. Інформаційна безпека України та заходи її забезпечення Науковий вісник Національної академії внутрішніх справ України. 2003. № 5. С. 206 - 214
9. Братель О. Поняття та зміст доктрини інформаційної безпеки Право України. 2006. № 5. С.36 - 40
10. Бут В.В. Проблеми безпеки в інформаційній сфері сутність понять та їх термінологічне тлумачення Науковий вісник Національної академії внутрішніх справ України. 2003. № 5. С. 225 - 232.
11. Вертузаєв М.С., Попов А.Ф. Проблеми боротьби зі злочинністю в сфері комп'ютерної інформації Інформаційні технології та захист інформації. 1998. №1. Ст. 4 14.
12. Вступ до інформаційної культури та інформаційного права: Монографія. Ужгород: 2003. 240 с.
13. Гаврилов І. Розвиток інформаційного простору: нові можливості, нові загрози Національна безпека і оборона. 2001. № 1. С. 77 – 79

14. Гнатцов О. Політико-управлінські аспекти інформаційних ресурсів у системі забезпечення державної безпекиВісник Національної академії державного управління при Президентові України. 2004. № 3. С. 485 – 492

15. Горбатюк О.М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть Вісник Київського університету імені Т.Шевченка. 1999. Вип. 14: Міжнародні відносини. С. 46 – 48

16. Гуцалюк М. Інформаційна безпека у сучасному суспільстві Право України. 2005. № 7. С.71 – 73.

17. Гуцалюк М. Інформаційна безпека України: нові загрози Бізнес і безпека. 2003. № 5. С. 2 – 3

18. Інформатизація та відкритість влади як засоби демократизації суспільства. Зб. матеріалів «круглого столу» у Національному інституті стратегічних досліджень 17.12.2002 р. 1С, 2003.

19. Інформаційна безпека України: проблеми та шляхи їх вирішення Національна безпека і оборона. 2001. № 1. С. 60 – 69

20. Інформаційна безпека України: сутність та проблеми Стратегічна панорама. 1998. № 3 – 4.

21. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Монографія. Запоріжжя, 2001. 252 с

22. Інформаційне право. Навч.-метод. комплекс. Київ: 1998.

23. Інформаційне суспільство. Дефініції. Київ: 2002. 220 с

24. Інформаційний простір України Національна безпека і оборона. 2001. № 1. С. 3 - 15

25. Карпенко В. Інформаційний простір і національна безпека України Універсум. 2002. № 7 – 8. С. 49 – 52

26. Катренко А. Особливості інформаційної безпеки за міжнародними стандартами Альманах економічної безпеки. 1999. № 2. С. 15 – 17

27. Ковтун В.С. Інформаційні технології – небезпечний засіб поширення тероризму Безпека життєдіяльності. 2006. № 10. С. 39 – 44

28. Комп'ютерна злочинність: Навч. посібник. Київ: 2002.

29. Лапо А. Гуманітарні та технічні чинники підвищення інформаційної безпеки Вісник. 2007. № 2. С. 130 – 133

30. Ліщинська О. Соціально-правові основи інформаційної безпеки: Програма навчального спецкурсу Соціальна психологія. 2007. № 5. С. 163 – 178.

31. Медвідь Ф. Інформаційна безпека України в контексті становлення стратегії національної безпеки держави Юридичний Вісник України. 2008. № 43. С. 11

32. Михайлюк В.А. Безпека інформаційної сфери основа стійкого розвитку соціуму Безпека життєдіяльності. 2007. № 6. С. 15 – 16.

33. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності Віче. 2007. № 12. С. 23 – 25

34. Бабенко Л. К. Новые технологии электронного бизнеса и безопасности. М., 2001. 376 с.

35. Остроухов В. До проблеми забезпечення інформаційної безпеки України Політичний менеджмент. 2008. № 4. С. 135 – 141.

36. Попович В.М. Економіко-кримінологічна теорія детінізації економіки: Монографія. Ірпінь: Академія державної податкової служби України, 2001. 546 с.

37. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій Навч. посібник. Запоріжжя, 2002. 292 с

38. Сапєгін С. Ефективне управління паливним ринком потребує інформаційно-аналітичного забезпечення Національна безпека і оборона. 2006. № 3. С. 45 – 48

39. Система забезпечення інформаційної безпеки України Національна безпека і оборона. 2001. № 1. С. 16 – 28

40. Столбовський А. О. Нові інформаційні технології та економічна безпека України Актуальні проблеми економіки. 2004. № 8. С. 99 – 104.

41. Борсуковський Ю.В., Бурячок В.Л., Складанний П.М., Аналіз сучасних вимог до створення парольних політик корпоративних користувачів Сучасний захист інформації. 2016. №3

42. Семко В.В., Бурячок В.Л., Толюпа С.В., Складанний П.М. Модель управління захистом інформації в інформаційно-телекомунікаційній системі Львівська політехніка. 2015

43. Теплицький І. Інформаційна безпека як нова складова інформаційної культури Рідна школа. 2006. № 2. С. 63 – 64.

44. Хлевицький В. Інформаційна безпека як одна із основних складових національної безпеки України Євроатлантикінформ. 2006. № 1. С. 70 – 72

45. Цимбалюк В. Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальні кіберцивілізації) Підприємництво, господарство і право. 2004. № 3. С. 88 – 91

46. Цимбалюк В. С. Категорія «безпека» у новому Кримінальному кодексі України Новий Кримінальний кодекс України: питання застосування і вивчення. Матеріали міжнар. наук.-практ. конф. 25 – 26 жовтня 2001 р. – Х.; К., 2002. С 167 – 170

47. Чубарук Т. Проблеми законодавчого забезпечення інформаційної безпеки в Україні Право України. 2007 . № 9 . С. 67 – 69

48. Шилан Н.Н., Кривонос Ю.М., Бірюков М.Г. Комп'ютерні злочини та проблеми захисту інформації: навч. посіб. Луганськ, 1999.

49. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ Актуальні проблеми економіки. 2006. № 10. С. 220 – 225.