МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

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

ДИПЛОМНА РОБОТА

на тему:

ОРГАНІЗАЦІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

СТУДЕНТ: Романов Михайло Віталійович _____
(підпис)

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

НОРМОКОНТРОЛЕР: к.в.н., доц. Якименко Юрій Михайлович _____
(підпис)

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
Навчально-науковий інститут захисту інформації
Кафедра управління інформаційною та кібернетичною безпекою
Освітньо-кваліфікаційних рівень – бакалавр
Спеціальність «Кібербезпека»
Спеціалізація «Управління інформаційною та кібернетичною безпекою»

"ЗАТВЕРДЖУЮ"
Завідувач кафедри УІКБ
_____ С.В.Легомінова
(підпис)
“___”_____ 2020 р.

ЗАВДАННЯ

на дипломну роботу

студенту Романову Михайлу Віталійовичу

1. Тема роботи «Організація інформаційної безпеки на підприємстві», затверджена наказом по університету від “___” _____ 20__ р. № ____.
2. Термін здачі студентом оформленої роботи “__” _____ 20__ р.
3. Об’єкт дослідження: інформаційна безпека підприємства.
4. Предмет дослідження: організація інформаційної безпеки на підприємстві.
5. Мета дослідження полягає у визначенні шляхів удосконалення організації інформаційної безпеки на підприємстві.
6. Перелік питань, які мають бути розроблені:
1. Розглянути основні теоретичні засади забезпечення інформаційної безпеки підприємства.
2. Дослідити особливості організації інформаційної безпеки на сучасному підприємстві.
3. Визначити шляхи удосконалення організації інформаційної безпеки на підприємстві.
7. Дата видачі завдання “__” _____ 20__ р.

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання: «__» _____ 20__ р.

№ з/п	Етапи бакалаврської роботи	Термін виконання етапів	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	11.03.2020	
2.	Збір та аналіз літератури.	18.03.2020	
3.	Написання 1-го розділу роботи.	01.04.2020	
4.	Написання 2-го розділу роботи.	15.04.2020	
5.	Написання 3-го розділу роботи.	29.04.2020	
6.	Формулювання висновків за результатами проведеного дослідження.	06.05.2020	
7.	Оформлення роботи.	12.05.2020	
8.	Оформлення презентації.	14.05.2020	
9.	Отримання рецензії на роботу.	20.05.2020	
10.	Захист в ДЕК.	__.06.2020	

Студент М.В.Романов
(підпис)

Науковий керівник І.В.Мордас
(підпис)

РЕФЕРАТ

Дипломна робота присвячена дослідженню проблем інформаційної безпеки підприємства. Робота складається зі вступу, трьох розділів, висновків та списку використаних джерел, що містить 40 найменувань. Загальний обсяг роботи становить 83 аркуші, з яких 4 аркуша займає список використаних джерел.

Об'єктом дослідження є інформаційна безпека підприємства.

Метою роботи є надання визначення шляхів удосконалення організації інформаційної безпеки на підприємстві. Для цього у роботі використовуються методи системного аналізу, наукової абстракції, порівняння та ін.

Як результат у роботі проведено аналіз основних теоретичних засад забезпечення інформаційної безпеки підприємства; досліджено особливості організації інформаційної безпеки на сучасному підприємстві; визначено шляхи удосконалення організації інформаційної безпеки на підприємстві.

Галузь застосування. Розроблені підходи можуть бути використані при плануванні та реалізації системи інформаційної безпеки на підприємстві.

Ключові слова: ІНФОРМАЦІЙНА БЕЗПЕКА, ІНФРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА, ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, СИСТЕМА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС — автоматизована система;

ЕОМ — електронно-обчислювальна машина;

ІБ — інформаційна безпека

ІзОД — інформація з обмеженим доступом;

ІТ — інформаційні технології;

КС — комп'ютерна система;

КІС — комп’ютерна інформаційна система

КСЗІ — комплексна система захисту інформації;

НСД — несанкціонований доступ;

ОС — обчислювальна система;

ПЗ — програмне забезпечення;

ПЗІ — підрозділ захисту інформації;

РСО — режимно-секретний орган;

СЗІ — служба захисту інформації;

СЗІБ — система забезпечення інформаційної безпеки;

СКІБ — система керування ІБ;

ТЗІ — технічний захист інформації.

ВСТУП

Актуальність теми. В умовах економіки постіндустріального суспільства, інформація, що стосується усіх напрямків діяльності підприємства, стає найбільш цінним і дорогим ресурсом, а проблеми інформаційної безпеки – усе більш складними і практично значущими. Інформаційна безпека підприємства є однією із складових частин економічної безпеки, яка формує модель захищеності підприємства. Таким чином, в сучасних умовах наявність розвиненої системи інформаційної безпеки стає одним з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якої компанії.

Усе більш очевидною стає залежність загального рівня економічної безпеки підприємства від інформаційної складової. Розуміючи важливість інформаційного розвитку української держави та входження до світового інформаційного простору, законодавством України було задекларовано, що розвиток інформаційного суспільства в Україні та впровадження новітніх інформаційно-комунікаційних технологій в усі сфери суспільного життя визначається одним із пріоритетних напрямів державної політики.

Щодо поняття «інформаційна безпека підприємства» необхідно зазначити, що воно є надзвичайно актуальним на сучасному етапі розвитку інформаційних технологій, який супроводжується введенням інформаційних систем у всі сфери діяльності людини, постійною взаємодією підприємств на теренах саме інформаційного простору.

Мета і завдання дослідження. **Мета роботи** полягає у визначенні шляхів удосконалення організації інформаційної безпеки на підприємстві.

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

1. Провести аналіз основних теоретичних засад забезпечення інформаційної безпеки підприємства.

2. Дослідити особливості організації інформаційної безпеки на сучасному підприємстві.

3. Надати пропозиції щодо удосконалення методичної бази підприємства з питань інформаційної безпеки.

Об'єкт дослідження – інформаційна безпека підприємства. **Предмет дослідження** – організація інформаційної безпеки на підприємстві.

Методи дослідження. Для вирішення означеного вище наукового завдання в роботі використані методи системного аналізу, наукової абстракції, порівняння та ін.

Наукова новизна одержаних результатів. Розроблені підходи можуть бути використані при плануванні та реалізації системи інформаційної безпеки на підприємстві у контексті протидії загрозам.

Практичне значення одержаних результатів. Застосування напрацювань дадуть змогу здійснити обґрунтований вибір методів і засобів захисту інформації, інфраструктури та персоналу підприємства у відповідності до цілей, можливостей та ресурсів.

Розділ 1
ТЕОРЕТИЧНІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

1.1 Інформаційна складова в системі безпеки підприємства

Інформаційна складова полягає у здійсненні ефективного інформаційно-аналітичного забезпечення господарської діяльності підприємства.

Відповідні служби виконують при цьому певні функції, які в сукупності характеризують процес створення та захисту інформаційної складової економічної безпеки. До таких функцій належать:

1) збирання всіх видів інформації про діяльність того чи того суб'єкта господарювання;

2) аналіз одержуваної інформації з обов'язковим дотриманням загальноприйнятих принципів і методів;

3) прогнозування тенденцій розвитку науково-технологічних, економічних і політичних процесів;

4) оцінка рівня економічної безпеки за всіма складовими та в цілому, розроблення рекомендацій для підвищення цього рівня на конкретному суб'єкті господарювання;

5) інші види діяльності з розроблення інформаційної складової економічної безпеки.

На підприємство постійно надходять потоки інформації, що різняться джерелами їх формування. Виокремлюють інформацію:

- відкриту офіційну;
- вірогідну нетаємну, одержану через неформальні контакти працівників фірми з носіями такої інформації;
- вірогідну таємну, отриману через неформальні контакти працівників фірми з носіями такої інформації. Дослідження показують, що 90-

95% усієї необхідної інформації можна отримати легально, вивчаючи виступи працівників підприємства на конференціях, семінарах; відкриті публікації підприємства і його окремих працівників; експонати різних виставок, ярмарків, презентацій; дані товарних і фондових бірж, оголошення про наявні вакансії, конкурси на заміщення посади тощо.

Тому керівник підприємства повинен запровадити правові норми захисту таємниць, а також систему контролю за збереженням комерційної таємниці.

Розглянемо детальніше показники інформаційної складової безпеки підприємства:

Продуктивність інформації (Пін)

$$П_{ін} = \frac{П_{П}}{В_{т}}$$

де Пп - обсяг промислової продукції, грн.; В.т - витрати на придбання інформаційних ресурсів, грн.

Коефіцієнт інформаційної озброєності

$$К_{і.озб} = \frac{В_{т}}{Ч_{сп}} . 100\%, > 20\%,$$

де В.т - витрати на придбання інформаційних ресурсів,грн; $Ч_{сп}$- середньоспискова чисельність працівників, чол.

Коефіцієнт захищеності інформації

$$К_{з.ін} = \frac{В_{з.ін}}{В_{т}} . 100\%, \leq 20\%,$$

де $В_{з.ін}$ - витрати підприємства на захист інформаційних ресурсів, грн; В.т - витрати на придбання інформаційних ресурсів, грн.

Оперативна реалізація заходів з розроблення та охорони інформаційної складової економічної безпеки здійснюється послідовним виконанням певного комплексу таких робіт:

а) збирання різних видів необхідної інформації;

б) оброблення та систематизація добутої інформації;

в) аналіз цієї інформації;

г) захист інформаційного середовища підприємства, що традиційно охоплює:

- заходи захисту суб'єкта господарювання від промислового шпигунства з боку конкурентів чи інших юридичних і фізичних осіб;

- технічний захист приміщень, транспорту, кореспонденції, переговорів, різної документації від несанкціонованого доступу заінтересованих юридичних і фізичних осіб до закритої інформації;

- збирання інформації про потенційних ініціаторів промислового шпигунства та проведення необхідних запобіжних дій з метою припинення таких спроб;

- зовнішня інформаційна діяльність.

Рівень інформаційної складової економічної безпеки визначається використанням неповної, неточної і суперечливої інформації в процесі приймання управлінських рішень.

Як показники рівня інформаційної безпеки також визначають коефіцієнти:

- повноти інформації (Л), який обчислюють як відношення обсягу інформації, що є в розпорядженні особи, котра приймає рішення, до обсягу інформації, необхідної для прийняття цього рішення;
- точності інформації (К.), який визначають як відношення обсягу релевантної (достовірної) інформації до загального обсягу наявної інформації;
- суперечливої інформації (А) з відношення кількості незалежних свідчень на користь ухвалення рішення до загальної кількості незалежних свідчень у сумарному обсязі релевантної інформації.

Рівень інформаційної безпеки можна визначити як добуток коефіцієнтів

$$К_{іб} = К_в \cdot К_с \cdot К_н$$

Розрізняють три ступені інформаційної безпеки: Кв > 0,7 - високий; 0,3 < Кс < 0,7 - середній; Кн < 0,3 - низький.

Головною метою будь-якої системи інформаційної безпеки є гарантування стійкого функціонування об'єкта, запобігання загрозам його безпеки, захист законних інтересів замовника від протиправних посягань, запобігання розкраданню грошових коштів; розголошуванню, втратам, витоку, спотворенню і знищенню службової інформації; забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта. Система інформаційної безпеки має також сприяти підвищенню якості.

1.2 Основні загрози безпеці діяльності підприємства в інформаційній сфері

Сучасна література поняття **"інформаційна загроза"** розглядає як потенційну можливість певним чином порушити інформаційну безпеку, чи ступінь імовірності виникнення такого явища (події), наслідком якого можуть бути небажані впливи на інформацію, тоді як намагання реалізувати загрозу розглядається атакою, а той, хто починає таку спробу, — як зловмисник. Потенційні зловмисники називаються джерелами загрози. Успішність атаки може приводити до втрати інформацією однієї з критичних особливостей (конфіденційності, цілісності чи доступу до інформації).

Загрози ІБ – це сукупність умов і чинників, що створюють небезпеку життєво важливим інтересам компанії в інформаційній сфері. Дослідження причин виникнення загроз, їх характеристик, особливостей впливу на корпоративні мережі та інформаційні ресурси сприяє розробленню ефективних заходів їх захисту, спрямованих на забезпечення нормальної господарської діяльності компаній. Управління ІБ та стійкістю функціонування компаній залежить від глибини прогнозу соціально-економічних наслідків небезпечних ситуацій та своєчасного планування та

виконання низки запобіжних і захисних заходів.

Згідно з даними звіту "Глобальне дослідження інформаційної безпеки, 2018 рік", який 29 жовтня 2018 р. опублікувала компанія "Ернст енд Янг", для захисту компаній від загроз ІБ, які є наслідком дії наявних і впровадження нових ІТ, потрібно докорінно змінити підхід до забезпечення їх ІБ. Цей звіт (вже п'ятнадцятий за рахунком) є одним з найбільш повних досліджень в галузі ІБ, який базується на відповідях понад 1850 респондентів – керівників інформаційно-комунікаційних мереж і служб ІБ з 64 країн світу.

Хоча на сьогодні керівники практично всіх компаній поступово нарощують свій потенціал у вирішенні короткотермінових завдань [34], пов'язаних із проблемою забезпечення ІБ, але при цьому не приділяють уваги проблемам, вирішення яких є доцільним вже зараз для зниження загрози ІБ в майбутньому. Насамперед відчувається потреба в створенні надійної архітектури ІБ, про наявність якої зголосилися тільки 31 % респондентів і відзначили збільшення кількості випадків її порушення протягом останніх двох років. Тим не менш, в 63 % компаній така архітектура не створена, і тільки 16 % респондентів вважають, що їх система ІБ повністю відповідає потребам захисту власних корпоративних мереж та інформаційних ресурсів.

Це означає, що керівники служб ІБ мають прийняти як аксіому твердження про те, що звичайна оперативність реагування на сучасні загрози ІБ вже не є достатньою для їх попередження чи знешкодження з найменшими втратами. Швидкість і складність динаміки джерел загроз ІБ промислових компаній зростає з роками колосальними темпами. І без того непроста ситуація у сфері ІБ ускладнюється впливом ринків нових ІТ, кількість яких стрімко розвиваються, тривалою нестабільністю в економіці та політиці, офшорній діяльності багатьох промислових компаній і посиленням нормативних вимог у сфері ІБ.

Збільшення кількості загроз інформаційній безпеці. У багатьох керівників служб ІБ промислових компаній на сьогодні вже є розуміння того, що сама природа і характер ризиків втрат інформаційних ресурсів швидко міняються, а разом із збільшенням частоти появи загроз ІБ зростає і кількість порушень та інцидентів ІБ . Приблизно 77 % респондентів різних компаній підтвердили зростання ризику зовнішніх хакерських атак, проте вони не є єдиним джерелом занепокоєння для вирішення глобальних проблем ІБ, позаяк 46 % респондентів відзначають, що внутрішня уразливість інформаційних ресурсів також невпинно зростає за рахунок інсайдерів. Постійне зростання обсягу VoIP продуктів змушує керівників служби ІБ швидше реагувати на появу нових витоків конфіденційної інформації.

Компанія Sophos опублікувала "Дослідження загроз у сфері ІБ – 2017", в якому було проведено детальний аналіз подій в області IT безпеки за 2017 року та зроблено прогноз на 2018 рік. Зокрема, зазначалося, що 80 % хакерських атак у 2017 році використали переадресацію з нібито благонадійних сайтів різних організацій, а майже 18 % доменів – з експлойт Blackhole, які знаходилися в Росії. За словами фахівців цієї компанії, 2017 рік був роком нових програмних платформ і нових хакерських загроз. Якщо зовсім недавно основною операційною системою в світі була Windows, то тепер на зміну їй прийшла нова різноманітність програмних платформ. Розробники шкідливого ПЗ активно користуються цією ситуацією, придумуючи нові неприємні сюрпризи для працівників відділу IT та служби ІБ промислових компаній.

Незахищені комп'ютери схильні до атак різного шкідливого ПЗ, яке поширюється мережею Інтернет. Шкідливе ПЗ (англ. malware, malicious software – шкідлива програма, зловмисне ПЗ) – будь-яке ПЗ, призначене для отримання несанкціонованого доступу до обчислювальних ресурсів самого комп'ютера або до інформаційних ресурсів, які зберігаються на ньому,

призначене для несанкціонованого власником їх використання чи спричинення шкоди (нанесення збитку) власникові комп'ютера, інформації чи комп'ютерній мережі шляхом копіювання, спотворення даних, видалення або підміни інформації.

Термін "шкідлива програма" (malware – це скорочення від "malicious software") за трактуванням корпорації Microsoft зазвичай використовується як загальноприйнятий термін для позначення будь-якого ПЗ, спеціально створеного для того, щоб заподіювати збиток окремому комп'ютеру, серверу, або комп'ютерній мережі, незалежно від того, чи є воно вірусом, шпигунською програмою і т. д.

Шкідливі програми за нанесеним збитком поділяються на такі, що:

1) Створюють перешкоди в роботі зараженого комп'ютера: починаючи від відкриття-закриття піддону CD-ROM і закінчуючи знищенням даних і поломкою апаратного забезпечення; блокування антивірусних сайтів, антивірусного ПЗ і адміністративних функцій ОС з метою ускладнення їх лікування; саботаж виробничих процесів, керованих комп'ютером (цим відомий черв'як Stuxnet).

2) Виконують інсталяцію іншого шкідливого ПЗ: завантаження з мережі (downloader); розпаковування іншої шкідливої програми, що вже міститься усередині файлу (dropper).

3) Здійснюють крадіжку, шахрайство, здирство і шпигунство за користувачем. Для крадіжки може застосовуватися сканування жорсткого диска, реєстрація натиснень клавіш (Keylogger) і перенаправлення користувача на підроблені сайти, в точності повторюючи вихідні ресурси. Викрадання даних, які представляють цінність або таємницю. Крадіжка аккаунтів різних служб (електронної пошти, мессенджерів, ігрових серверів.). Аккаунти застосовуються для розсилання спаму, а через електронну пошту можна роздобути паролі від інших аккаунтів, водночас як віртуальне майно можна продати в MMOG (Massively multiplayer online game). Крадіжка

аккаунтів платіжних систем.

Шкідливе ПЗ створюють блокування комп'ютера, шифрування файлів користувача з метою шантажу і здирства грошових коштів (Ransomware[1]). Здебільшого після оплати комп'ютер або не розблоковується, або незабаром блокується другий раз. Шкідлива програма використовує телефонний модем для здійснення дорогих дзвінків, що спричиняє за собою значні суми в телефонних рахунках. Платне ПЗ, яке імітує, наприклад, антивірус, але нічого корисного для цього не робить (fraudware або scareware).

4) Виконують іншу незаконна діяльність: отримання несанкціонованого (і дармового) доступу до ресурсів самого комп'ютера або третіх ресурсів, доступних через нього, у т.ч. пряме управління комп'ютером (так званий backdoor). Організація на комп'ютері відкритих релеїв і загальнодоступних проксі-серверів. Заражений комп'ютер (у складі ботнета) може бути використаний для проведення DDoS-атак. Збирання адрес електронної пошти і поширення спаму, у т.ч. у складі ботнета. Накручування електронних голосувань, клацань по рекламних банерах. Генерування монет платіжної системи Bitcoin. Використання ефекту 25-го кадру для зомбування людини.

5) Записують файли, які не є істинно шкідливими, але здебільшого небажані: жартівливе ПЗ, тобто робить які-небудь речі, що непокоять користувача. Наприклад, програма Adware показує рекламу, а програма Spyware посилає через мережу Інтернет інформацію, несанкціоновану користувачем. Створюють видимість "отруєння" документів, які дестабілізують ПЗ, що відкриває їх (наприклад, архів розміром менше мегабайта може містити гігабайти даних, а при його архівуванні може надовго "зависнути" архіватор). Програми віддаленого адміністрування можуть застосовуватися як для того, щоб дистанційно вирішувати проблеми з комп'ютером, так і для зловмисних цілей. Rootkit (руткіт, від англ. root kit, тобто "набір root'а") програма або набір програм, призначений для

приховування слідів присутності зловмисника або шкідливого ПЗ від сторонніх очей

Інколи шкідливе ПЗ для власного "життєзабезпечення" встановлює додаткові утиліти: IRC-клієнти, програмні маршрутизатори, відкриті бібліотеки перехоплення клавіатури. Таке ПЗ шкідливим не є, але через те, що за ним часто знаходиться більш шкідлива програма, яка детектується антивірусами. Буває навіть, що шкідливим є тільки скрипт з одного рядка, а останні програми сповна легітимні.

Шкідливі програми за методом розмноження поділяються на:

1) Експлойт – теоретично нешкідливий набір даних (наприклад, графічний файл або мережевий пакет), що некоректно сприймається програмою, яка працює з такими даними. Тут шкоду наносить не сам файл, а неадекватна поведінку ПЗ з помилкою. Також експлойтом називають програму для генерування подібних "отруєних" даних.

2) Логічна бомба в програмі спрацьовує за певної умови, є невід'ємною від корисної програми-носія.

3) Троянська програма не має власного механізму розмноження.

4) Комп'ютерний вірус розмножується в межах комп'ютера і через змінні диски. Розмноження через локальну мережу можливо, якщо користувач сам викладе заражений файл в мережу. Віруси, водночас, поділяються за типом файлів, що заражаються (файлові, завантажувальні, макрофайлові, такі, що автозапускаються); за способом прикріплення до файлів (паразитні, супутні і такі, що перезаписують) і т.д.

5) Мережевий черв'як здатний самостійно розмножуватися мережею. Поділяється на IRC[2], поштові, такі, що розмножуються за допомогою експлойтів і т.д.

Шкідливе ПЗ може утворювати ланцюжки: наприклад, за допомогою експлойта на комп'ютері жертви розгортається завантажувач, який встановлює з мережі Інтернет черв'яка.

Міжнародна мережа центрів досліджень в галузі ІБ SophosLabs компанії Sophos на основі аналізу мережевого трафіку створила рейтинг країн з найбільшим і найменшим ризиками (індекс поширеності шкідливого ПЗ розрахований на основі кількості хакерських атак комп'ютерів за останні три місяці 2017 року) [19] :

- з найбільшим ризиком: Гонконг – 23,54 %; Тайвань – 21,26 %; Арабські Емірати – 20,78 %; Мексика – 19,81 %; Індія – 17,44 %.
- з найменшим ризиком: Норвегія – 1,81 %; Швеція – 2,59 %; Японія – 2,63 %; Великобританія – 3,51 %; Швейцарія – 3,81 %.

Фахівці компанії Sophos вважають, якщо до цього моменту безліч хакерських атак не завдавали істотної шкоди компаніям, то в 2017-му, з розвитком різних програмних платформ для тестування наборів експлойтів – шкідливого ПЗ, ситуація може кардинально змінитися – традиційні системи ІБ корпоративних мереж перестануть їх захищати від нових загроз. Деякі виробники подібних платформ навіть гарантують покупцям повернення коштів у разі невдачі їх продуктів. Внаслідок цього очікується збільшення кількості інцидентів, коли шахраї отримають доступ до корпоративних мереж і активно користуватимуться ними.

Також для 2018 р. в галузі ІБ було характерно:

- збільшення кількості критичних помилок для систем ІБ у налаштуваннях вебсерверів;
- зростання обсягів шкідливого ПЗ, яке важко аналізувати;
- поява інструментів для створення хакерських програм з новими сервісами; ● спрощення процесу виявлення експлойтів – шкідливого ПЗ;
- проблеми інтеграції, конфіденційності інформації та її безпеки.

Поява нових ІТ відкривають перед компаніями не тільки небачені можливості, але й піддають їх потенційним загрозам з невідомих раніше джерел Хмарні комп'ютерні технології як і раніше є головним джерелом інновацій в сучасному інформаційному середовищі: за останні декілька

років кількість компаній, які використовують хмарні обчислення, збільшилася майже удвічі. Тим не менше, 38 % таких компаній не вжили жодних заходів щодо зниження ризиків витоку інформації, зокрема не забезпечили більш строгого нагляду за управлінням контрактами з провайдерами, які надають послуги з хмарного оброблення даних, або застосування методів шифрування [24].

Ще однією новою ІТ, яка заслуговує на увагу, є мобільні пристрої для роботи в мережі Інтернет, технологічну досконалість яких, а також пов'язані з ними переваги для бізнесу, забезпечили стрімке зростання їх популярності. Станом на 2017 рік 44 % різних компаній давали змогу своїм працівникам використовувати корпоративні або особисті планшети (аналогічний показник за 2016 рік становив 20 %), за допомогою яких співробітники відправляли і отримували значні обсяги інформації, що істотно ускладнювало контроль за ІБ не тільки корпоративної мережі, але й всієї компанії загалом.

Керівники служб ІБ визнають, що мобільним технологіям потрібно приділяти більш пильну увагу. При цьому засоби забезпечення ІБ і спеціальне програмне забезпечення, яке б відстежувало трафік мобільних пристроїв, як і раніше досить рідко застосовуються на динамічному ринку мобільних технологій. Тільки 40 % різних компаній використовують той чи інший метод шифрування даних на мобільних пристроях

Зазвичай загроза є наслідком наявності вразливих місць у захисті інформаційних систем (таких, наприклад, як можливість доступу сторонніх осіб до критично важливого устаткування або помилки у програмному забезпеченні). Загроза інформації, що циркулює в інформаційній системі, залежить від її структури та конфігурації, технології оброблення інформації в ній, стану навколишнього фізичного середовища, а також дій персоналу.

Варто наголосити, що ряд загроз не слід вважати наслідком якихось помилок, прорахунків чи злого умислу, адже вони існують внаслідок самої

природи інформаційних систем (загроза відключення електрики чи її параметрів за допустимі межі існує через залежність апаратного забезпечення інформаційної системи від якісного електроживлення). Часто існують загрози заподіяння шкоди системам оброблення даних через фізичний вплив стихійних природних явищ, що не залежать від людини.

Зважаючи на це, розглянемо найбільш розповсюджені загрози, якими уразливі сучасні інформаційні системи, що дасть змогу вибрати найбільш економічні засоби забезпечення безпеки. Адже необізнаність у цій справі призведе до перевитрат коштів і, що ще гірше, до концентрації ресурсів там, де вони особливо й непотрібні, за рахунок послаблення справді вразливих напрямів.

Вивчаючи зміст поняття "загроза", бачимо, що за різних умов воно трактується по-різному. Зокрема, якщо фірма є відносно відкритою, то для неї не існує загроз конфіденційності, адже вся інформація є загальнодоступною, тоді як для більшості фірм нелегальний доступ є серйозною небезпекою. Тобто загрози, як і все в інформаційній безпеці, залежить від суб'єктів інформаційних відносин.

Беручи до уваги типову фірму, загрози її інформаційній безпеці можна класифікувати за такими критеріями:

• за аспектом інформаційної безпеки (доступність, цілісність, конфіденційність), на що спрямовані загрози передусім;

• за компонентами інформаційних систем, на які спрямовані загрози (дані, програми, апаратура, підтримуюча інфраструктура);

• за способом здійснення (випадкові/навмисні дії природного/ техногенного характеру);

• за розміщенням джерела загроз (всередині/ззовні інформаційної системи).

Тепер детальніше зупинимося на характеристиці вказаних загроз, критерієм яких є аспект інформаційної безпеки (доступність, цілісність, конфіденційність).

Найбільш розповсюдженими і небезпечними загрозами доступності є ненавмисні помилки постійних користувачів, операторів, системних адміністраторів та інших осіб, що обслуговують інформаційні системи. Саме такі помилки зазвичай і стають загрозами (неправильно введені дані чи помилка в програмі, що призвела до краху системи), іноді вони створюють слабкі місця, якими можуть скористатися зловмисники. Статистика свідчить, що близько 65 % втрат — наслідок ненавмисних помилок. Виходячи з цього, найбільш радикальний спосіб боротьби з ненавмисними помилками — максимальна автоматизація і строгий контроль.

На другому місці за розмірами збитків — крадіжки та підробки. За даними, що обертаються серед фахівців, у 2016 році внаслідок подібних протиправних діянь з використанням персональних комп'ютерів американським організаціям було завдано загальної шкоди у розмірі 1 млрд 882 млн дол. США. Можна припустити, що справжній розмір шкоди набагато більший, оскільки багато фірм зі зрозумілих причин приховують такі інциденти. У більшості розслідуваних випадків винуватцями виявлялися штатні співробітники фірм, добре обізнані з режимом роботи і заходами безпеки. Це ще раз переконує нас, що внутрішні загрози набагато небезпечніші за зовнішні.

Інші загрози доступності класифікують за компонентами інформаційних систем, на які спрямовані загрози:

• відмовлення користувачів;

• внутрішня відмова інформаційних систем;

• відмова підтримуючої інфраструктури.

Стосовно користувачів зазвичай розглядаються такі загрози:

• небажання працювати з інформаційною системою (найчастіше виявляється в разі потреби освоювати нові можливості і у випадку розбіжності

між запитами користувачів і фактичними можливостями та технічними характеристиками);

• неможливість працювати із системою через відсутність відповідної підготовки (низький рівень загальної комп'ютерної грамотності, невміння інтерпретувати діагностичні повідомлення, невміння працювати з документацією тощо);

• неможливість працювати із системою через відсутність технічної підтримки (неповнота документації, недолік довідкової інформації тощо).

Основними джерелами внутрішніх відмовлень є:

• відступ (випадковий або навмисний) від установлених правил експлуатації;

• вихід системи зі штатного режиму експлуатації через випадкові або навмисні дії користувачів або обслуговуючого персоналу (перевищення розрахункової кількості запитів, надмірний обсяг оброблюваної інформації тощо);

• відмовлення програмного й апаратного забезпечення;

• опромінення технічних засобів зондувальними сигналами, наслідком чого може стати викривлення чи знищення інформації, а у випадку сильного опромінення — вихід з ладу апаратури;

• загрози використання спеціальних методів і технічних засобів (фотографування, електронні закладки, що знищують або викривляють інформацію);

• знищення інформаційних даних;

• пошкодження або знищення апаратури.

Стосовно підтримуючої інфраструктури рекомендується розглядати такі загрози:

• порушення роботи (випадкове або навмисне) систем зв'язку, електроживлення, водо та/або теплопостачання, кондиціонування;

• пошкодження або знищення майна приміщень;

• неможливість або небажання обслуговуючого персоналу та/або користувачів виконувати свої обов'язки (громадські заворушення, аварії на транспорті, терористичний акт або його загроза, страйк тощо).

Досить небезпечними є так звані скривджені співробітники — нинішні і колишні. Як правило, вони прагнуть завдати шкоди фірмі-"кривдникові", наприклад:

• зіпсувати устаткування;

• вмонтувати логічну бомбу, що згодом зруйнує програми та/або дані;

• знищити дані.

Скривджена категорія співробітників (навіть ті, які вже не працюють, але знайомі з порядками на фірмі), може завдати чималої шкоди. А тому при звільненні таких співробітників варто стежити за тим, щоб їхні права доступу (логічного та фізичного) до інформаційних ресурсів анулювалися.

Багато говорять і пишуть також про хакерів, але загроза, що виходить від них, зазвичай перебільшується. Справді, майже кожен інтернет сервер декілька разів щодня піддається спробам проникнення; справді, іноді такі спроби виявляються вдалими; справді, інколи подібні дії пов'язані зі шпигунством. Однак загалом шкода від діяльності хакерів (порівняно з іншими загрозами) є не настільки значною. Імовірно, найбільше лякає непередбачуваність дій людей такого сорту. Уявіть собі, що в будь-який момент до вас у квартиру можуть забратися сторонні особи. Навіть якщо вони не мають злого наміру, а зайшли просто так, подивитися, приємного в цьому мало.

Багато говорять і пишуть про програмні віруси. Однак дотримання нескладних правил комп'ютерної гігієни зводить ризик зараження практично до нуля. Там де працюють, а не грають, кількість заражених комп'ютерів становить близько частки відсотка. Такими є основні загрози, на частку яких припадає левова частка втрат, що їх зазнають інформаційні системи.

Серйозну загрозу інформаційній безпеці становлять також **злочинні дії,** спрямовані на розкрадання, привласнення, підміну, підключення, ламання

(знищення), диверсію. Такі дії можуть здійснюватися до оброблення інформації чи в процесі її оброблення, з доступом до елементів інформаційної системи чи без нього, активно чи пасивно (тобто зі зміною стану системи чи без такого).

Джерелами названих вище загроз інформації можуть бути люди, апаратно-програмні засоби та середовище, що оточує інформаційну систему та її компоненти, що можуть впливати на інформацію ззовні (зовнішні джерела загроз) чи перебувати усередині інформаційної системи (внутрішні джерела загроз).

Зважаючи на це, до зовнішніх джерел загроз інформації відносять:

• діяльність розвідувальних і спеціальних служб;

• діяльність політичних, військових, фінансових та інших економічних структур, спрямована проти інтересів держави та бізнесу;

• злочинні дії окремих груп, формувань та фізичних осіб.

До внутрішніх джерел загроз відносять:

• протизаконну діяльність різних структур, угруповань та окремих осіб у сфері використання інформації з метою приховування правопорушень, заподіяння збитків законним інтересам інших юридичних чи фізичних осіб;

• порушення встановлених правил збирання, оброблення і передавання інформації.

1.3 Система забезпечення інформаційної безпеки підприємства

Інформаційна безпека - це стан захищеності інформаційного середовища, захист інформації являє собою діяльність щодо запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, тобто процес, спрямований на досягнення цього стану.

Метою реалізації інформаційної безпеки будь-якого об'єкта є побудова системи забезпечення інформаційної безпеки даного об'єкту [18].

Для побудови та ефективної експлуатації СЗІБ (система забезпечення інформаційної безпеки) необхідно:

- виявити вимоги захисту інформації, специфічні для даного об'єкта захисту;

- врахувати вимоги національного та міжнародного законодавства;

- використовувати напрацьовані практики (стандарти, методології) побудови подібних СЗІБ;

- визначити підрозділи, відповідальні за реалізацію та підтримку СЗІБ;

- рас проділити між підрозділами області відповідальності у здійсненні вимог СЗІБ;

- на базі управління ризиками інформаційної безпеки визначити загальні положення, технічні та організаційні вимоги, складові політики інформаційної безпеки об'єкта захисту;

- реалізувати вимоги політики інформаційної безпеки, впровадивши відповідні програмно-технічні засоби і способи захисту інформації;

- реалізувати систему менеджменту (управління) інформаційної безпеки (СМІБ);

- використовуючи систему управління організувати регулярний контроль ефективності СЗІБ і при необхідності перегляд і коригування СЗІБ.

Під системою безпеки будемо розуміти організовану сукупність спеціальних органів, служб, засобів, методів і заходів, що забезпечують захист життєво важливих інтересів особистості, підприємства і держави від внутрішніх і зовнішніх загроз (рис. 1.1) [21].

Метою системи захисту інформації підприємства є:

- запобігання витоку, розкраданню, втраті, перекручуванню, підробці інформації;
- запобігання загрозам безпеці особистості, підприємства, суспільства, держави;

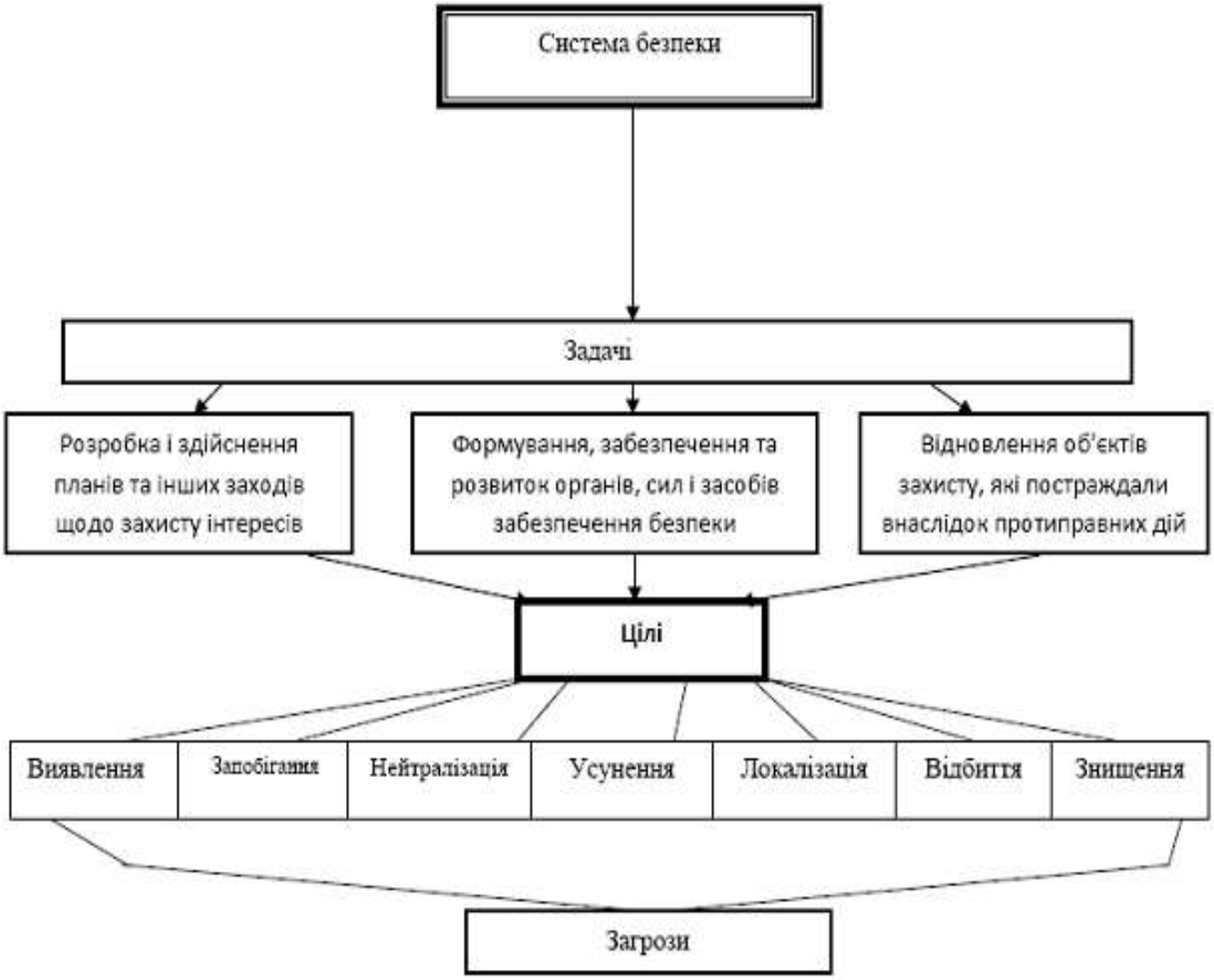

Рис. 1.1. Функціональна система інформаційної безпеки

- запобігання несанкціонованим діям щодо знищення, модифікації, перекручування, копіювання, блокування інформації;
- запобігання іншим формам незаконного втручання в інформаційні ресурси й системи, забезпечення правового режиму документованої інформації як об'єкта власності;
- захист конституційних прав громадян на збереження особистої таємниці й конфіденційності персональних даних, що існують в інформаційних системах;
- збереження конфіденційності документованої інформації відповідно до законодавства.

Для грамотної побудови й експлуатації системи захисту необхідно дотримуватись таких принципів її застосування:

- простота захисту;
- прийнятність захисту для користувачів;
- підконтрольність системи захисту;
- постійний контроль за найбільш важливою інформацією;
- дроблення конфіденційної інформації на складові елементи, доступ до яких мають різні користувачі;
- мінімізація привілеїв доступу до інформації;
- установка пасток для провокування несанкціонованих дій;
- незалежність системи керування для користувачів;
- стійкість захисту в часі й за несприятливих обставин;
- глибина захисту, його дублювання й перекриття;
- особлива персональна відповідальність осіб, що забезпечують безпеку інформації;
- мінімізація загальних механізмів захисту.

Алгоритм створення системи захисту конфіденційної інформації такий:

- визначення об'єктів захисту;
- виявлення загроз і оцінка їхньої ймовірності;
- оцінка можливої шкоди;
- огляд застосовуваних засобів захисту, визначення їхньої недостатності;
- визначення адекватних заходів захисту;
- організаційне, фінансове, юридичне та ін. види забезпечення засобів захисту;
- впровадження засобів захисту;
- контроль;

- моніторинг і коригування впроваджених засобів.

1. Начальник служби захисту інформації призначається наказом керівника підприємства. Він очолює групу компетентних співробітників, які висловлюють свої пропозиції щодо обсягу, рівня й способів забезпечення збереженості конфіденційної інформації.

2. Керівник групи, маючи відповідну кваліфікацію в цій сфері, із залученням окремих фахівців формує попередній список відомостей, які надалі ввійдуть в «Перелік відомостей, що становлять конфіденційну інформацію підприємства».

3. Керівник групи на основі цього списку визначає й подає на узгодження необхідні до захисту об'єкти (устаткування для обробки й обігу інформації, програмне забезпечення, комунікації для передання конфіденційних даних, носії інформації, персонал, допущений до роботи з використанням комерційної й іншої таємниці).

4. Аналізуються наявні засоби захисту відповідних об'єктів, визначається ступінь їхньої недостатності, неефективності, фізичного й морального зношування.

5. Вивчаються зафіксовані випадки спроб несанкціонованого доступу до захищених інформаційних ресурсів і розголошення інформації.

6. На основі досвіду підприємства, з використанням методу моделювання ситуацій група фахівців виявляє можливі шляхи несанкціонованих дій зі знищення інформації, її копіювання, модифікації, перекручування, використання й т. п. Загрози ранжуються за ступенем значимості й класифікуються за видами впливу.

7. На основі зібраних даних оцінюється можлива шкода підприємству від кожного виду загроз, що стає визначальним фактором для категорування відомостей в «Переліку» за ступенем важливості, наприклад, для службового користування, конфіденційно, суворо конфіденційно.

8. Визначаються сфери обігу кожного виду конфіденційної

інформації: за носіями, територією поширення, допущеними користувачами. Для вирішення цього завдання група залучає керівників структурних підрозділів, вивчає їхні побажання.

9. Група проводить підготовку до введення зазначених засобів захисту.

Висновки до першого розділу

З позиції економічного підходу, загальний збиток інформаційної безпеки підприємства складається з двох складових частин: прямого і непрямого збитку. Прямий збиток інформаційної безпеки підприємства виникає внаслідок витоку конфіденційної інформації. Непрямий збиток - втрати, які несе підприємство у зв'язку з обмеженнями на поширення інформації, в установленому порядку віднесеної до категорії конфіденційної. Опис збитку, що наноситься підприємству в результаті витоку конфіденційної інформації, грунтується на його кількісних і якісних показниках, які базуються на одному з принципів засекречування інформації (віднесення її до категорії конфіденційної) - принципі обгрунтованості. Він полягає у встановленні (шляхом експертних оцінок) доцільності засекречування конкретних відомостей, а також ймовірних наслідків цих дій, з урахуванням розв'язуваних підприємством задач і поставлених цілей.

Введення обмежень на поширення інформації (у зв'язку з її засекречуванням або віднесенням до категорії конфіденційної) призводить і до позитивних, і до негативних наслідків. До основних позитивних наслідків слід віднести запобігання можливого прямого збитку інформаційної безпеки підприємства через витік інформації, що захищається. Негативні наслідки пов'язані з наявністю (ймовірним зростанням) непрямого збитку або витрат у вигляді витрат на захист інформації та величини упущеної вигоди, яка може бути отримана при її відкритому розповсюдженні.

При розробці необхідних, засобів, методів і заходів, що забезпечують захист інформації, необхідно враховувати велику кількість різних факторів.

Інформація, будучи предметом захисту, може бути представлена на різних технічних носіях. Її носіями можуть бути люди з числа користувачів і обслуговуючого персоналу. Інформація може піддаватися обробці в комп'ютерних системах, передаватися по каналах зв'язку і відображатися різними пристроями. Вона може розрізнятися за своєю цінністю. Об'єктами, що підлягають захисту, де може перебувати інформація, є не тільки комп'ютери і канали зв'язку, але й приміщення, будівлі та прилегла територія. Істотно різнитися може кваліфікація порушників, а також використовувані способи і канали несанкціонованого доступу до інформації.

Таким чином, основними принципами забезпечення інформаційної безпеки є наступні:

Системності.

Комплексності.

Безперервності захисту.

Розумної достатності.

Гнучкості управління і застосування.

Відкритості алгоритмів і механізмів захисту.

Простоти застосування захисних заходів і засобів.

За способами здійснення всі заходи забезпечення безпеки комп'ютерних систем підрозділяють на:

правові (законодавчі);

морально-етичні;

організаційно-адміністративні;

фізичні;

апаратно-програмні.

Розділ 2
ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА СУЧАСНОМУ ПІДПРИЄМСТВІ

2.1 Нормативно-правове регулювання інформаційної безпеки діяльності підприємства

Для забезпечення повноцінного правового та організаційного захисту інформації необхідно розробити низку документів, а саме:

- положення стосовно конфіденційної інформації підприємства;
- перелік документів підприємства, які містять конфіденційну інформацію;
- інструкцію щодо захисту конфіденційної інформації у інформаційній системі підприємства;
- пропозиції стосовно внесення змін в Статут підприємства;
- пропозиції стосовно внесення змін в трудовий договір, контракт із керівником і колективний договір;
- угоду зі співробітником стосовно нерозголошення конфіденційної інформації підприємства;
- обов’язки співробітника стосовно нерозголошення конфіденційної інформації після звільнення з підприємства;
- пропозиції стосовно внесення змін в Правила внутрішнього розпорядку підприємства (в частині регламентації конкретних засобів фізичного захисту інформації та питань режиму);
- пропозиції стосовно внесення змін в посадовий (штатний) розклад підприємства (штату Служби із захисту інформації);
- пропозиції стосовно внесення доповнень в посадові інструкції всього персоналу;

- відомість ознайомлення працівників підприємства з Положенням стосовно конфіденційної інформації й Інструкцію стосовно захисту конфіденційної інформації у інформаційній системі підприємства;
- план проходження занять з персоналом стосовно збереження та нерозголошення конфіденційної інформації підприємства;
- пропозиції стосовно внесення змін до структури співбесіди при прийомі на роботу (уточнення обов'язків інформаційного характеру з останніх місць роботи кандидатів);
- пропозиції стосовно внесення доповнень в стандартні договори з контрагентами.

Саме вищезазначені документи відіграють важливу роль в забезпеченні інформаційної безпеки підприємства.

Документаційне забезпечення захисту починається із внесення доповнень в Статут підприємства: «Підприємство самостійно має право встановлювати обсяг відомостей, які становлять комерційну й іншу таємницю, яка охороняється законом, та порядок її захисту. Підприємство, з метою захисту свого економічного суверенітету, має право також вимагати від персоналу, контрагентів, партнерів та інших юридичних і фізичних осіб, установ та організацій забезпечення нерозголошення конфіденційної інформації підприємства на підставі контрактів, договорів та інших необхідних документів».

Для розробки усіх документів, що стосуються роботи із конфіденційною інформацією, необхідно, у першу чергу, розробити основний документ – «Положення про конфіденційну інформацію».

Форми всіх документів, які регулюють захист конфіденційної інформації, затверджуються наказом керівника підприємства. Положення ж є головним документом підприємства, який регламентує всі питання обігу конфіденційної інформації. Усі базові моменти, пов'язані з цим процесом, містяться саме в даному документі.

Положення містить основні обов'язки працівників стосовно забезпечення збереженості конфіденційної інформації. Щоб посилити цю складову системи захисту інформації необхідно доводити персоналу його обов'язки також у формі включення у посадові інструкції та додатково видавати спеціальні пам'ятки. І все це повинно відбуватися виключно під розпис.

Обов'язковим додатком до Положення має бути Перелік документів, які містять конфіденційну інформацію підприємства. Його наявність на підприємстві носить принциповий характер, адже неможливо вимагати від співробітників нерозголошення абстрактної конфіденційної інформації, наприклад, як іноді вказують в зобов'язальних документах: «зберігати службові відомості, ноу-хау, ділові секрети». Захищається лише документована інформація, а тому, потрібно якомога конкретніше описувати всі групи та види конфіденційної документації підприємства.

За основу для встановлення необхідного контролю над доступом до конфіденційної інформації підприємства береться, як правило, класифікація інформації за критерієм – рівень конфіденційності, залежно від змісту та можливих наслідків у разі зловживань або втрати інформації.

Основні види інформації за категоріями конфіденційності розподіляються приблизно наступним чином.

Найнижчий гриф конфіденційності «ДСК» ставлять на телефонні довідники, де містяться окремі дані про партнерів або кадровий склад. Цей гриф також ставлять на журнали реєстрації, службове листування, документи, що регламентують діяльність (розпорядження, накази, заяви, доповідні й т. д.).

У категорії документів з грифом "КОНФІДЕНЦІЙНО" містяться ті, де є інформація стосовно окремих аспектів ділових угод за короткостроковий проміжок часу; розгорнуті відомості стосовно персоналу компанії; стосовно поточної фінансової діяльності; дані про клієнтуру, що не надаються третім (стороннім) особам підприємства.

Гриф "СУВОРО КОНФІДЕНЦІЙНО" присвоюють документам, які

містять дані стосовно ділових угод з клієнтами або партнерами підприємства, стосовно підсумків діяльності за довгостроковий період часу. Крім того, цей гриф надають документам, які стосуються найважливіших аспектів комерційної діяльності підприємства, стратегії діяльності, документам, які містять детальну інформацію стосовно фінансового становища підприємства.

Класифікації за критерієм – рівень конфіденційності – підлягають усі документи підприємства відповідно до плану заходів стосовно забезпечення його безпеки. Питання стосовно присвоєння грифу вирішується розробником документа за участі начальника ПЗІ. Якщо цінність інформації через які-небудь причини знижується, знижується і гриф документа.

Окремої уваги також заслуговує питання і про терміни дії наявних грифів конфіденційності. Строк таємності, зазвичай, визначається автором документа, виконавцем, або особою, що підписує чи затверджує документ за узгодженням з керівником ПЗІ. Строк може вказуватися в вигляді періоду грифа, від дати закінчення грифа, настання конкретної події, на яку орієнтований документ, або напису «безстроково». В деяких випадках рішення стосовно зняття грифу залишається за начальником ПЗІ.

Наступний документ, який входить до складу документації з впровадження, – це **угода з співробітником (зобов'язання співробітника) стосовно нерозголошення конфіденційної інформації підприємства,** що співробітник підписує при прийомі на роботу [9].

Угода містить:

- зобов'язання стосовно збереження конфіденційної інформації підприємства;
- право співробітника на службову інформацію;
- відповідальність співробітника за порушення своїх зобов'язань.

Перед підписанням зобов'язання доцільним є також ознайомлювати кандидатів з витягами із законодавства, які обґрунтовують (коротко) правовий захист та санкції за неправомірне використання інформації, у тому числі – і

кримінально-правові.

Продовженням обов'язків працівника стосовно нерозголошення інформації є його «Заява про підтвердження зобов'язань стосовно нерозголошення конфіденційної інформації при звільненні з підприємства».

Документ не є бездоганним із юридичної точки зору, так як після звільнення трудові відносини, у межах яких діють зобов'язання працівника, припиняються. Однак доцільно пропонувати працівнику, який звільняється, підписати таку заяву: по його реакції можна буде оцінити реальну значущість для конкретної людини даних нею обіцянок. В той же час, в разі завдання збитків підприємству, з причини розголошення звільненим працівником конфіденційних відомостей підприємства, таке зобов'язання, скоріше за все, буде прийнято судом як додатковий доказ провини колишнього працівника. Крім того, про такий випадок можна буде з чистим сумлінням повідомляти його новому роботодавцеві.

Ставлення партнерів і контрагентів до таємниці підприємства варто виявляти самому підприємству.

Для цього необхідно внести у всі стандартні форми договірної документації підрозділи/розділи стосовно конфіденційності:

Кожна із сторін погодилася вважати текст цього договору, а також увесь обсяг інформації, який передається сторонами одна одній у процесі виконання зобов'язань, які виникають з даного договору, конфіденційною інформацією другої сторони.

Сторони зобов'язуються в будь-який спосіб не розголошувати (робити доступною третім особам, окрім випадків наявності у третіх (сторонніх) осіб відповідних повноважень в силу прямої дії закону, чи випадків, коли інша сторона у письмовій формі дасть згоду стосовно надання конфіденційної інформації, яка обумовлена відповідно до п. 1 цього договору, третім (стороннім) особам) конфіденційну інформацію другої сторони, до якої було одержано доступ при укладанні цього договору та в процесі виконання

зобов'язань, які виникають з нього.

Дані зобов'язання виконуються сторонами у межах терміну дії договору та протягом одного року після закінчення дії договору, якщо інше не буде обумовлене.

Кожна зі сторін зобов'язується відшкодовувати іншій стороні у повному обсязі всі збитки, які заподіяні останній у результаті розголошення її конфіденційної інформації у порушення пп. 1-3 даного договору.

Клієнт (постачальник і ін.) не вправі використовувати своє становище як сторона (за даним договором) у цілях та інтересах третіх (сторонніх) осіб.

Сторони договору зобов'язуються негайно попереджувати одна одну про виникнення некерованих процесів або факторів, що можуть призвести до порушення конфіденційності сторін договору.

Служба захисту інформації на підприємстві вживає заходи стосовно збереження комерційної таємниці підприємства шляхом максимального обмеження кількості осіб, які мають доступ до неї, фізичної збереженості документів, які містять такі відомості, оброблювання інформації з грифом конфіденційності на захищених комп’ютерах, внесення вимог стосовно конфіденційності конкретної інформації у договори з внутрішніми й зовнішніми партнерами й інших заходів відповідно до рішення керівництва.

Всі роботи з документами, які містять конфіденційну інформацію, повинні регламентуватися положенням про конфіденційне діловодство.

Обробка і захист конфіденційних документів повинні передбачати:

- порядок визначення інформації, яка містить комерційну таємницю, та строків дії відповідних грифів конфіденційності;
- систему допуску співробітників, відряджених та фізичних осіб до відомостей, які становлять комерційну таємницю підприємства;
- забезпечення збереження документів на магнітних і паперових носіях з грифом конфіденційності;
- зобов’язання осіб, що допущені до відомостей, які становлять

комерційну таємницю підприємства;

- принципи організації та проведення контролю за дотриманням режиму при роботі із відомостями, які становлять комерційну таємницю підприємства;
- відповідальність за розголошення відомостей та втрату документів, які містять комерційну таємницю. Допуск працівників до відомостей, які становлять комерційну таємницю підприємства, здійснюється Генеральним директором та Начальником ПЗІ.

Начальник ПЗІ, який відповідальний за підбор осіб, які допускаються до відомостей з грифом конфіденційності, зобов'язаний забезпечувати контроль за тим, аби до цих відомостей мали доступ лише ті особи, яким дані відомості необхідні для виконання службових обов'язків на підприємстві [9].

2.2 Організаційна структура та основні функції підрозділу інформаційної безпеки на підприємстві

Для забезпечення працездатності та ефективності розробленої системи захисту інформації на підприємстві потрібно створити спеціальний відділ в структурі підприємства, який буде займатися даними питаннями, – ПЗІ (підрозділ (або ж служба) захисту інформації).

Метою створення ПЗІ (підрозділу захисту інформації) є організаційне забезпечення завдань управління комплексною системою захисту інформації (КСЗІ) на підприємстві та здійснення постійного контролю за її функціонуванням [9].

На ПЗІ покладається завдання стосовно виконання робіт із визначення вимог щодо захисту інформації в АІС (автоматизованій інформаційній системі) підприємства, проектування, розроблення та модернізації КСЗІ (комплексної системи захисту інформації), із експлуатації, обслуговування та підтримки її працездатності, а також контролю за станом захищеності інформації в АІС.

Правову основу для створення та діяльності ПЗІ становлять Закони України: “Про державну таємницю”, “Про захист інформації в АС”, Положення стосовно технічного захисту інформації в Україні, Положення стосовно забезпечення режиму секретності у процесі обробки інформації, яка становить державну таємницю, у автоматизованих системах, інші юридичні (нормативно-правові акти), які стосуються питань захисту інформації, міжнародні, державні та галузеві стандарти, розпорядчі і інші документи. ПЗІ, як правило, здійснює діяльність у відповідності до “Плану захисту інформації”, перспективних, календарних та інших планів робіт, які затверджені керівником або заступником керівника підприємства.

Для здійснення окремих заходів стосовно захисту інформації в АІС, які пов’язані із напрямком діяльності інших структурних підрозділів підприємства, керівник або заступник керівника підприємства своїм наказом визначає перелік, терміни виконання та підрозділи для здійснення цих робіт.

ПЗІ у своїй роботі взаємодіє із підрозділами підприємства (службою охорони, РСО тощо), а також із державними органами, організаціями та установами, які займаються питаннями захисту інформації. В разі потреби, до здійснення робіт можуть бути залучені зовнішні організації, які володіють ліцензіями на відповідний вид діяльності в сфері захисту інформації.

До завдань ПЗІ належить:

- забезпечення безпеки інформації персоналу та структурних підрозділів підприємства у процесі інформаційної діяльності і взаємодії між собою та у взаємовідносинах із зовнішніми закордонними і вітчизняними організаціями;
- дослідження технологій обробки інформації з метою визначення можливих каналів витоку і інших загроз безпеці інформації, формування моделі загроз, розробка політики безпеки інформації та визначення заходів, які спрямовані на її реалізацію;

- організація і координація робіт, які пов’язані із захистом інформації на підприємстві (необхідність захисту визначається чинним законодавством), а також підтримка необхідного рівня захисту інформації, ресурсів та технологій;
- розробка проектів нормативних та розпорядчих документів, які чинні в межах підприємства, згідно з якими повинен бути забезпечений захист інформації на підприємстві;
- організація робіт стосовно створення та використання КСЗІ на усіх етапах життєвого циклу АІС;
- участь в організації і забезпеченні професійної підготовки та підвищенні кваліфікації персоналу і користувачів АІС стосовно питань захисту інформації; а також формування в персоналу і користувачів АІС на підприємстві розуміння необхідності виконання вимог чинного законодавства (нормативно-правових актів і розпорядчих документів, які стосуються сфери захисту інформації на підприємстві);
- організація забезпечення виконання персоналом та користувачами АІС вимог чинного законодавства (нормативно-правових актів і розпорядчих документів, які стосуються сфери захисту інформації на підприємстві) й проведення контрольних перевірок стосовно їх виконання, а також забезпечення визначених політикою інформаційної безпеки властивостей інформації (конфіденційність, цілісність, доступність) під час створення й експлуатації АІС;
- своєчасне виявлення й знешкодження загроз для ресурсів АІС, причин та умов, що спричиняють (можуть призвести до) порушення її функціонування й розвитку; створення механізму і умов оперативного реагування на будь-які загрози безпеці інформації та інші прояви негативних наслідків та тенденцій у функціонуванні АІС;

- ефективне попередження (знешкодження) загроз для ресурсів АІС шляхом комплексного запровадження правових, організаційних, морально-етичних, фізичних, технічних та інших заходів стосовно забезпечення безпеки інформації; керування засобами захисту інформації, а також керування доступом користувачів та працівників до ресурсів АІС, контроль з боку персоналу ПЗІ за їхньою роботою, оперативне оповіщення про спроби несанкціонованого доступу до ресурсів АІС підприємства;
- реєстрація, збір, обробка та зберігання даних про всі події у системі, які мають те чи інше відношення до безпеки інформації на підприємстві; створення умов для максимального можливого відшкодування і локалізації збитків, які завдаються через неправомірні (несанкціоновані) дії фізичних та юридичних осіб, вплив зовнішнього середовища та інші чинники, а також зменшення (нейтралізація) негативного впливу наслідків у результаті порушення безпеки функціонування АІС.
- своєчасне виявлення загроз інформації, що захищається, причин та умов їхнього виникнення і реалізації;
- виявлення і максимально можливе перекриття потенційно можливих каналів та методів несанкціонованого доступу до конфіденційної інформації підприємства;
- відпрацьовування механізмів оперативного реагування з боку підприємства на загрози, а також використання юридичних, організаційних, економічних, соціально-психологічних, інженерно-технічних методів і засобів виявлення та нейтралізації джерел загроз безпеці підприємства;
- організація спеціального діловодства, яке виключає несанкціоноване отримання конфіденційної інформації.

Керівник (начальник) ПЗІ є новою штатною одиницею на підприємстві. На цю посаду варто брати професіонала-фахівця у галузі захисту інформації, який добре розуміється на юридичній стороні цієї проблеми, має досвід керування й координації роботи аналогічних

підрозділів (служб). Вимогами на таку посаду є: вища професійна освіта та стаж роботи у галузі захисту інформації не менш, ніж 5 років, знання законодавства у даній сфері, принципів та методів планування захисту.

Керівник (начальник) ПЗІ повинен виконувати такі функції:

- розробляти політику забезпечення захисту інформації та забезпечувати її реалізацію;
- нести відповідальність за функціонування ПЗІ та забезпечення захисту конфіденційної інформації на підприємстві;
- здійснювати планування та безпосереднє керування роботою ПЗІ, нести відповідальність (персональну) за виконання відповідною службою покладених на неї задач та завдань, неухильне виконання працівниками (підлеглими) своїх посадових обов'язків та правил внутрішнього трудового розпорядку на підприємстві;
- брати особисту участь в проведенні найбільш складних заходів стосовно забезпечення захисту інформації на підприємстві;
- розробляти плани дій в надзвичайних ситуаціях та регулярно проводити навчання з працівниками;
- керувати проведенням службових розслідувань на підприємстві;
- організовувати взаємодію ПЗІ із іншими підрозділами підприємства;
- розробляти інструкції стосовно роботи з комерційною таємницею підприємства для персоналу, який допущений до роботи з відповідними документами на підприємстві;
- організовувати розробку рекомендацій стосовно удосконалювання функціонування ПЗІ на підприємстві;
- здійснювати керівництво відділом охорони на підприємстві;
- крім того, виконувати юридичні функції: розробка, оновлення та ведення основних документів у частині закріплення у них вимог забезпечення

захисту й безпеки конфіденційної інформації на підприємстві.

Керівник (начальник) ПЗІ відповідає за:

- організацію відповідних робіт стосовно захисту інформації в АІС, ефективність захисту інформації у відповідності до діючого законодавства (нормативно-правових актів);
- своєчасну розробку та виконання “Плану захисту інформації у автоматизованій системі”;
- належне виконання співробітниками ПЗІ функцій, завдань та обов'язків, які зазначені у відповідному Положенні, посадових інструкціях працівників, а також планових заходів стосовно захисту інформації, які затверджені керівником підприємства;
- координацію діяльності підрозділів та служб підприємства, які займаються питаннями захисту інформації;
- побудова системи навчання працівників та користувачів АІС стосовно питань захисту інформації на підприємстві;
- виконання (особисто) і працівниками ПЗІ розпоряджень та наказів керівника підприємства, правил трудового внутрішнього розпорядку, встановленого на підприємстві режиму, правил охорони праці і протипожежної безпеки.

Співробітники ПЗІ відповідають за:

- дотримання вимог нормативних документів, які визначають порядок організації робіт стосовно захисту інформації, інформаційних технологій та ресурсів;
- повноту і якість розроблення та впровадження організаційно-технічних заходів стосовно захисту інформації в АІС, точність і достовірність одержаних результатів та висновків стосовно питань, які належать до компетенції ПЗІ;

- додержання термінів проведення інспекційних, контрольних, перевірочних і інших заходів стосовно оцінки стану захищеності інформації у АІС, які включено до плану робіт ПЗІ;
- правомірність та якість документального оформлення результатів роботи окремих етапів створення КСЗІ та документального оформлення результатів проведених перевірок;
- ряд інших питань персональної відповідальності, що покладені на керівника і співробітників ПЗІ відповідно до специфіки та особливостей діяльності підприємства.

Взаємодія ПЗІ (підрозділу захисту інформації) із іншими підрозділами підприємства й зовнішніми організаціями.

ПЗІ проводить свою діяльність у взаємодії із науковими, виробничими й іншими організаціями, державними органами та установами, які займаються питаннями захисту інформації.

Всі заходи стосовно захисту інформації в АІС повинні бути узгоджені ПЗІ із заходами режимно-секретної та охоронної діяльності інших підрозділів підприємства.

Отже, ПЗІ взаємодіє, узгоджує свою роботу та встановлює зв’язки із:

- РСО підприємства;
- службою охорони підприємства;
- адміністрацією АІС і іншими структурними підрозділами підприємства, діяльність яких стосується захисту інформації чи її автоматизованою обробкою;
- зовнішніми організаціями, що є партнерами, постачальниками, виконавцями робіт або користувачами;
- підрозділами служб безпеки іноземних підприємств (які є для даного підприємства партнерами, постачальниками, виконавцями робіт, користувачами) або їхніми представництвами (на договірних чи інших засадах);

- колом інших суб’єктів діяльності в сфері захисту інформації.

Керівники ж відповідних підрозділів підприємства мають своєчасно інформувати ПЗІ про зміни та пересування у складі технічних засобів, за допомогою яких обробляється ІзОД.

Взаємодію із іншими підрозділами підприємства стосовно питань, які не пов’язані із захистом інформації безпосередньо, ПЗІ здійснює у відповідності із наказами або (та) розпорядженнями керівника підприємства.

Підрозділ (служба) програмно-апаратного захисту інформації.

Основними цілями захисту інформації, що обробляється та зберігається в комп’ютерах, є:

1. запобігання витоку та втраті інформації, втручанню та перехопленню зловмисника на усіх рівнях обробки даних та для всіх об'єктів захисту;

2. забезпечення цілісності даних на усіх етапах їхнього збереження та перетворення засобів програмного забезпечення.

Основні завдання підрозділу:

- запобігання витоку конфіденційної інформації за рахунок ПЕМВ (побічних електромагнітних випромінювань);
- запобігання НСД (несанкціонованому доступу) до інформації;
- захист інформації від вірусів (комп'ютерних);
- захист інформації від збоїв в системі живлення;
- захист інформації від копіювання;
- програмний захист всіх каналів передачі даних.

Підрозділ (служба) інженерно-технічного захисту інформації.

В загальному, інженерно-технічний захист інформації призначено для активно-пасивних протидій методам та засобам технічної розвідки та формування рубежів охорони будинків, приміщень, устаткування, території за допомогою комплексу технічних засобів, який містить:

- споруди інженерного (фізичного) захисту від проникнення третіх

(сторонніх) осіб на територію, у приміщення й будинки;

- засоби захисту каналів (технічних) витоку інформації при роботі комп’ютерів, засобів зв'язку, офісного устаткування та інших приладів при проведенні нарад, бесід із співробітниками й відвідувачами;
- засоби захисту приміщень й будинків від візуальних засобів розвідки (технічної);
- засоби забезпечення охорони територій, приміщень й будинків;
- засоби протипожежної охорони;
- заходи й технічні засоби, які запобігають винесенню персоналом з територій, приміщень й будинків документів, дискет, дисків й інших носіїв інформації.

Підрозділ (служба) конфіденційного діловодства.

Основні завдання:

- зберігання й обробка конфіденційних документів;
- контроль за системою конфіденційного документообігу.

На не дуже великих підприємствах доцільно організувати ПЗІ у такому складі:

- керівник (начальник) ПЗІ;
- співробітник, який займається програмно-апаратним захистом;
- працівник, який займається інженерно-технічним захистом.

Завдання та функції конфіденційного діловодства можна покласти на вже наявних працівників, яким на даний час доручено створення та обробку документів, які містять конфіденційну інформацію на підприємстві.

Штатний розклад та структура ПЗІ (підрозділу захисту інформації). ПЗІ є штатним структурним підрозділом підприємства з питань ТЗІ, який безпосередньо підпорядкований керівнику підприємства чи заступнику керівника підприємства, який відповідає за забезпечення безпеки інформації на підприємстві.

Штатність або позаштатність ПЗІ на підприємстві визначається керівництвом підприємства. А структура, її склад та чисельність ПЗІ визначається фактичними потребами підприємства з метою виконання вимог політики безпеки і захисту інформації й затверджується керівництвом підприємства.

Склад і чисельність ПЗІ повинні бути достатніми для виконання всіх завдань стосовно захисту інформації. А з метою ефективного функціонування та керування захистом інформації ПЗІ повинен мати штатний розклад, що включає перелік функціональних обов'язків всіх співробітників, необхідні вимоги до рівня їхніх знань і навичок. Штат ПЗІ повинен комплектуватися спеціалістами, що мають технічну освіту (вищу, спеціальну середню, спеціальні курси підвищення кваліфікації в галузі ТЗІ тощо) й практичний досвід роботи, володіють навиками стосовно розробки, впровадження і експлуатації КСЗІ, й засобів захисту інформації, а також навиками реалізації організаційних, технічних й інших заходів стосовно захисту інформації, знаннями та вмінням застосовувати норми діючого законодавства (нормативно-правові документи) в сфері захисту інформації на підприємстві.

Функціональні обов'язки працівників визначаються переліком й характером завдань, що покладаються на ПЗІ керівником підприємства. У залежності від обсягів й особливостей завдань ПЗІ, до його складу можуть входити спеціалісти (деякі групи спеціалістів, підрозділи і ін.) різного фаху: фахівці стосовно питань захисту інформації підприємства від витоку технічними каналами; фахівці стосовно питань захисту каналів зв'язку та комутаційного обладнання, налагодження й керування активним мережевим обладнанням; фахівці стосовно питань адміністрування і контролю засобів захисту, керування базами даних захисту та системами доступу; фахівці стосовно питань захищених технологій оброблення інформації.

За посадами працівники ПЗІ можуть поділятися на дані категорії (за критерієм – рівень ієрархії) [9]:

- керівник (начальник) ПЗІ;
- адміністратори захисту АІС (безпеки системи, безпеки баз даних тощо);
- спеціалісти служби захисту інформації.

Для роботи ПЗІ потрібно підготувати ряд нормативних документів, а саме:

- положення про ПЗІ (підрозділ захисту інформації);
- інструкцію стосовно безпеки конфіденційної інформації підприємства;
- перелік відомостей, які становлять конфіденційну інформацію підприємства;
- інструкцію стосовно роботи з конфіденційною інформацією підприємства;
- посадові інструкції співробітників ПЗІ (підрозділу захисту інформації);
- інструкцію стосовно забезпечення пропускного режиму на підприємстві;
- пам'ятку працівникові (службовцеві) стосовно збереження конфіденційної інформації.

2.3 Управління інцидентами інформаційної безпеки у процесі здійснення підприємством господарської діяльності

Завдання керування інцидентами ІБ в даному контексті – це постійне неперервне забезпечення безпеки інформаційного забезпечення бізнес-процесів на потрібному рівні шляхом обробки будь-яких подій з реагування на події, що є несприятливими відносно політики інформаційної безпеки (ПІБ). З точки зору оператора телекомунікацій чи сервіс-провайдера (постачальника ІТ-послуг),

процес керування інцидентами ІБ сприяє інтеграції аспектів безпеки в ІТМ чи ІТ-інфраструктуру. Під час експлуатації системи керування ІБ (СКІБ) процес керування інцидентами ІБ є постачальником даних для аналізу функціонування подібних систем, оцінки ефективності використовуваних заходів зниження ризиків і планування поліпшень в роботі системи.

Таким чином, керування інцидентами ІБ є однією з найважливіших частин загальної проблеми керування ІБ, а систему керування інцидентами ІБ можна розглядати як підсистему СКІБ, що взаємопов’язана з системами керування якістю та послугами.

В міжнародній практиці вже розроблено велику кількість нормативно-методологічних документів, які в тому чи іншому аспекті регламентують процеси керування інцидентами ІБ. В даній статті розглянуто лише стандарти та технічні звіти ISO/IEC, які об’єднані єдиним підходом та безпосередньо пов’язані з керуванням інцидентами або відіграють визначну роль у вирішенні даного науково-практичного завдання.

Міжнародна нормативно-методологічна база з керування інцидентами ІБ.

У світі розробка стандартів, технічних звітів, керівництв та рекомендацій в галузі ІБ проводиться безперервно; послідовно публікуються проекти і версії стандартів, присвячених тим чи іншим аспектам ІБ на різних стадіях узгодження і затвердження. Деякі стандарти поетапно заглиблюються і деталізують у вигляді сукупності взаємозв'язаних концепціями і структурами груп стандартів. Розробка нормативних документів з ІБ, повністю або частково присвячених керуванню інцидентами ІБ, здійснюється низькою спеціалізованих міжнародних організацій і консорціумів, таких як, наприклад: CERT, ISO, IEC, IETF, ITU-T, IEEE, OMG, SANS Institute, X/Open тощо. Значна робота щодо стандартизації питань ІБ, зокрема керування інцидентами, проводиться спеціалізованими організаціями і на національному рівні, в першу чергу в США – NIST,

CMU/SEI; Німеччині та Великобританії – BSI. Все це дозволило сформувати обширну нормативно-методологічну базу у вигляді міжнародних, національних та галузевих стандартів, а також нормативних і керівних матеріалів, що регламентують діяльність в сфері керування інцидентами ІБ. Проте, як свідчить сучасна практика, найважливішу роль в світі відіграють стандартиISO.

Стандарти ISO серій 9000, 17799, 20000, 27000 описують правила створення систем керування різними процесами та гармонійно поєднуються один з одним. Усі вони, як основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього. Крім цього, стандарти зазначених серій використовують єдину модель PDCA як структуру життєвого циклу всіх процесів системи менеджменту.

Основні нормативно-методологічні документи ISO/IEC, які в тому чи іншому аспекті регламентують процеси керування інцидентами ІБ, наведені в таблиці 2.1 (також див. список літератури).

Як свідчить світова практика стандарт ISO/IEC 17799 на сьогодні став найпоширенішим інструментом створення СКІБ, стандартом де-факто щодо керування ІБ. Відмітимо, що попередня версія ISO/IEC 17799 від 2000 року офіційно прийнята в Україні як ДСТУ ISO/ IEC 17799:2000. ISO/IEC 17799 – це збірка практичних рекомендацій, яка дає деталізоване керівництво щодо розробки, впровадження та оцінки заходів керування ІБ, а також загальні принципи побудови СКІБ. В цьому ж документі визначено наступні терміни, які є базовими для даного дослідження:

подія інформаційної безпеки - встановлений прояв стану системи, служби або мережі, вказуючий на можливе порушення політики інформаційної безпеки або збій заходів безпеки, або невідома до даного моменту ситуація, яка може бути пов'язана з безпекою.

Таблиця 2.1.

Нормативно-методологічні документи ISO/IEC, що стосуються керування інцидентами

№ п/п	Позначення документу	Назва документу	Рік
1	ISO/IEC 27001	Information technology. Security techniques. Information security management systems. Requirements.	2005
2	ISO/IEC TR 18044	Information technology. Security techniques. Information security incident management.	2004
3	ISO/IEC 20000	ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice.	2005

інцидент інформаційної безпеки - ознаками інциденту інформаційної безпеки є поодинокі або послідовні небажані або несподівані події інформаційної безпеки, які мають значну вірогідність компрометації ділових операцій і загрожують інформаційній безпеці.

Розділ 13 ISO/IEC 17799 присвячено керуванню інцидентами ІБ. В ньому розглянуто наступні питання. Повідомлення про події і слабкі місця ІБ. Виявлення користувачами подій і слабких місць ІБ, пов'язаних з інформаційними системами, має гарантувати можливість ухвалення своєчасних корегуючих дій. Має бути впроваджений формальний порядок повідомлення про події і порядок ескалації. Всіх співробітників, контрагентів і користувачів третіх сторін слід поінформувати про порядок повідомлення щодо різних типів подій і слабких місць, які можуть мати вплив на безпеку активів організації. Дані особи зобов'язані негайно повідомляти про будь-які події і слабкі місця ІБ, використовуючи певну точку контакту.

Про події ІБ потрібно повідомляти за допомогою прийнятних каналів керування настільки швидко, наскільки це можливо. Слід затвердити формальний порядок повідомлення про події ІБ, разом з порядком реагування на інциденти і порядком ескалації. В цих порядках потрібно описати дії, що мають бути здійснені при отриманні повідомлення про подію ІБ. Слід встановити точку контакту для повідомлень про події ІБ. Слід забезпечити обізнаність всієї організації про дану точку контакту, її постійну доступність і здатність адекватно і своєчасно реагувати.

Порядок повідомлення має включати:

- прийнятні процеси зворотного зв'язку для забезпечення повідомлення осіб, що повідомляють про події ІБ, про результати після обробки і закриття проблеми;
- форми повідомлення про події ІБ для підтримки процесу повідомлення і нагадування особі про всі необхідні дії уразі події ІБ;
- правильна поведінка у разі події ІБ, тобто: негайний запис всіх важливих подробиць (наприклад, тип невідповідності або порушення, збій, повідомлення на екрані, дивна поведінка); не виконання будь-яких самостійних дій, але негайне повідомлення в точку контакту; посилання на встановлений формальний дисциплінарний процес вживання заходів до співробітників, контрагентів або користувачів, третіх сторін, що здійснюють порушення безпеки.

Приклади подій та інцидентів ІБ: втрата обслуговування, устаткування або засобів обслуговування; системні збої або перевантаження; людські помилки; невідповідність політикам або керівництву; порушення заходів фізичної безпеки; некеровані системні зміни; збої програмного або апаратного забезпечення; порушення доступу.

При дотриманні заходів щодо конфіденційності, інформація про інциденти ІБ може використовуватися в тренінгах з підвищення обізнаності користувачів як приклади того, що може трапитися, як реагувати на такі

інциденти і як уникати їх в майбутньому. Для забезпечення можливості належного поводження з інцидентами ІБ може існувати необхідність збору доказів негайно після їх появи.

Збої або інша аномальна поведінка системи можуть свідчити про атаку на безпеку або дійсно порушення безпеки, тому слід завжди повідомляти про них, як про події ІБ.

Всіх співробітників, контрагентів і користувачів, третіх сторін, що використовують інформаційні системи і послуги, слід зобов'язати звертати увагу і повідомляти про будь-які помічені або передбачувані слабкі місця ІБ в системах або послугах. Механізм повідомлення повинен бути якомога легким та зручним. Слід проінформувати всіх, що ні за яких обставин не можна намагатися перевіряти і демонструвати передбачуване слабке місце. Випробування слабких місць можна тлумачити як потенційне неправомірне використання системи, що може також привести до пошкоджень інформаційної системи або служби і до юридичної відповідальності особи, що виконує перевірку.

Керування інцидентами і вдосконаленнями ІБ Забезпечення застосування послідовного і ефективного підходу до керування інцидентами ІБ.

Слід впровадити обов'язки та порядок ефективної невідкладної обробки подій і слабких місць ІБ. Як реакцію на них слід застосовувати процес безперервного вдосконалення, відстежування , оцінки та повного керування інцидентами ІБ. Для забезпечення відповідності юридичним вимогам слід збирати докази. Для забезпечення швидкого, ефективного і організованого реагування на інциденти ІБ слід затвердити обов'язки і порядок керування. Для виявлення інцидентів ІБ, окрім повідомлення про події і слабкі місця ІБ, слід використовувати відстежування систем та вразливостей.

Необхідно розглянути наступні рекомендації щодо порядкукерування інцидентами ІБ:

- слід затвердити порядок поводження з різними типами інцидентів ІБ, включаючи: збої інформаційних систем; шкідливий код; відмову в обслуговуванні; помилки через неповні або неточні дані; порушення конфіденційності та цілісності; неправомірне використання інформаційних систем;
- на додаток до звичайних планів реагування на непередбачені обставини, порядок має також охоплювати: аналіз та ідентифікацію причин інциденту; обмеження розповсюдження; планування і впровадження корегуючих дій; зв'язок з особами, відповідальними за процес відновлення після інциденту або задіяними в даний процес; повідомлення увідповідні державні органи;
- при необхідності, слід збирати і захищати протоколи (audit trails) та інші подібні докази;
- слід ретельно та формально керувати заходами щодо відновлення після порушень ІБ та виправлення збоїв системи; порядок повинен забезпечувати: дозвіл доступу до виробничих чи технологічних систем і даних тільки чітко встановленому і уповноваженому персоналу; докладне документування всім вжитим надзвичайним заходам; повідомлення керівництву про надзвичайні заходи і їх організований розгляд; підтвердження цілісності систем бізнесу та засобів керування з мінімальною затримкою.

Цілі керування інцидентами ІБ слід погоджувати з керівництвом, а також слід забезпечити розуміння співробітників, що відповідають за керування інцидентами ІБ, пріоритетів організації щодо поводження з інцидентами ІБ.

Інциденти ІБ можуть виходити за рамки організації і держави. Для реагування на такі інциденти зростає потреба в координації реагування та в обміні інформацією стосовно інцидентів із зовнішніми організаціями.

Вивчення інцидентів ІБ. Слід впровадити механізми вимірювання та відстежування типів і об'єму інцидентів ІБ, а також витрат. Для розпізнавання інцидентів, що повторюються, або інцидентів з високим рівнем дії слід

використовувати інформацію оцінки інцидентів ІБ. Оцінка інцидентів ІБ може вказати на потребу в збільшенні або доповненні засобів керування з метою зниження частоти, збитків та витрат майбутніх проявів інцидентів, або для прийняття до уваги при перегляді політики безпеки.

Збір доказів.

Якщо після інцидентів ІБ відносно людини або організації вживаються заходи, що передбачають судовий розгляд (як цивільних, так і кримінальних), слід збирати, зберігати і представляти докази з метою відповідності нормам, що стосуються доказів, прийнятим у відповідній юрисдикції. Слід розробити внутрішній порядок, якого слід дотримуватися при зборі і представленні доказів з метою застосування дисциплінарних заходів в організації. Загалом, правила обробки доказів охоплюють: допустимість доказів – чи дійсно доказ може використовуватися в суді; вагомість доказів: якість і повнота доказів. Для забезпечення допустимості доказів організація має переконатися у відповідності її інформаційної системи якому-небудь опублікованому стандарту або зведенню правил зі збору допустимих доказів.

Вагомість доказів, що надаються, має відповідати прийнятним вимогам. Для забезпечення вагомості доказів ряд переконливих підтверджень має показувати якість і повноту засобів керування, що використовуються для правильного і послідовного захисту доказів (тобто, доказів керування процесами) протягом періоду, коли зберігався і оброблявся доказ, що підлягає відновленню. Загалом, такий ряд переконливих підтверджень може бути встановлений за наступних умов:

- для паперових документів: оригінал збережений надійно із записом особи, що знайшла документ, де і коли документ був знайдений і хто засвідчив виявлення; гарантії відсутності підробок оригіналів мають надаватися розслідуванням;
- для інформації на комп'ютерних носіях: дзеркальні образи або копії (залежно від відповідних вимог) будь-яких змінних носіїв, інформацію на

жорстких дисках або в пам'яті слід одержати для забезпечення доступності; слід зберігати протоколи всіх дій протягом процесу копіювання, процес повинен проходити при свідках; оригінальні носії і протокол (якщо це неможливо, принаймні, один дзеркальний образ або копію) слід надійно зберігати і не чіпати.

Будь-яку роботу до розслідування слід виконувати тільки на копіях доказового матеріалу. Слід захищати цілісність всієї доказової бази. Контролювати копіювання доказового матеріалу повинні надійні співробітники. Також слід протоколювати інформацію про те, коли і де був виконаний процес копіювання, хто виконував копіювання і які інструменти і програми використовувалися.

Коли подія ІБ виявляється вперше, може бути не очевидно, чи дійсно випадок закінчиться судовим розглядом. Тому існує небезпека навмисного або випадкового знищення необхідного доказу раніше, ніж усвідомлена серйозність інциденту. При будь-якому припущенні судового позову бажано відразу привернути юриста або правоохоронні органи і отримати пораду щодо необхідних доказів.

Доказ може виходити за рамки організації і/або за підвідомчі межі. В таких випадках слід переконатися, що організація має право збирати необхідну інформацію як докази. Для максимізації можливостей ухвалення доказів у відповідній юрисдикції слід також розглядати вимоги різних юрисдикцій.

Стандарт ISO/IEC 27001 конкретно звертає увагу на необхідність створення процедури керування інцидентами ІБ. В рамках даного стандарту висуваються загальні вимоги щодо побудови СКІБ, що відносяться у тому числі і до процесів керування інцидентами ІБ. Згідно з ISO/IEC 27001 для обробки подій і інцидентів ІБ необхідно організувати процес реагування на інциденти. Основними завданнями процесу реагування на інциденти ІБ є:

- координація реагування на інцидент ІБ;
- підтвердження / спростування факту виникнення інциденту ІБ;

- забезпечення збереження і цілісності доказів виникнення інциденту ІБ, створення умов для накопичення і зберігання точної інформації про інциденти ІБ, що мали місце, про корисні рекомендації;
- мінімізація порушень порядку роботи і пошкодження даних ІТ-системи, відновлення в найкоротші терміни працездатності компанії при її порушенні в результаті інциденту;
- мінімізація наслідків порушення конфіденційності, цілісності і доступності інформації ІТ-систем;
- захист прав компанії, встановлених законом; створення умов для порушення цивільної або кримінальної справи проти зловмисників;
- захист репутації компанії і її ресурсів;
- швидке виявлення і/або попередження подібних інцидентів в майбутньому;
- навчання персоналу компанії діям до виявлення, усунення наслідків і запобігання інцидентам ІБ.

В рамках ISO/IEC 27001 висуваються наступні вимоги до процесу реагування на інциденти ІБ, які повністю відповідають вищерозглянутим рекомендаціям щодо керування інцидентами ІБ у ISO/IEC 17799:

Моніторинг і аналіз СКІБ Організація має виконати наступне:

- своєчасно ідентифікувати невдалі та успішні інциденти ІБ;
- допомогти у виявленні подій ІБ і, таким чином, запобігти інцидентам ІБ шляхом використання індикаторів.

Висновки до другого розділу

Ефективність захисту інформації в ІС досягається лише в тому випадку, якщо забезпечується її надійність на всіх об'єктах і елементах системи, що можуть бути піддані погрозам із боку зовнішнього середовища.

Об'єкт захисту — такий структурний компонент системи, у якому знаходиться або може знаходитися інформація, яка підлягає захисту.

Система захисту інформації (СЗІ) — комплекс організаційних заходів і програмно-технічних (у тому числі криптографічних) засобів забезпечення безпеки інформації в автоматизованих системах.

Кожний співробітник незалежно від свого службового становища або ступеня спорідненості з керівником підприємства повинен володіти тільки тією інформацією, якому йому необхідна для роботи. Намагайтеся діяти так, аби заходи щодо захисту інформації не заважали рекламній політиці та комерційній діяльності вашої фірми.

Несистематична та неістотна підготовка до реагування та обробки інцидентів ІБ призводить до того, що на практиці реагування виявляється хаотичним, невпорядкованим та неефективним, істотно ускладнюючи відновлення бізнес-процесів (технічної експлуатації, менеджменту якості, надання послуг тощо) і через це – потенційно підсилює завданий збиток. Без своєчасної реакції на інциденти ІБ та усунення їхніх наслідків неможливо ефективне функціонування СКІБ.

Суть методологічно-правильного процесу керування інцидентами ІБ – це чітке визначення ролей та розподіл відповідальності щодо якісного та своєчасного реагування на інциденти ІБ.

Розділ 3
ШЛЯХИ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

3.1 Створення комплексної системи захисту інформації на підприємстві

Необхідність побудови КСЗІ.

Згідно з чинним законодавством України і вимогами окремих нормативних документів Законів України "Про захист інформації в інформаційно-телекомунікаційних системах" і "Про захист персональних даних" захисту інформації обов'язково підлягає: інформація, яка є власністю держави, чи інформація із обмеженим доступом, вимоги стосовно захисту якої встановлені вітчизняним законодавством, у т.ч. персональні дані усіх громадян.

Комплексна система захисту інформації – це сукупність організаційних та інженерно-технічних заходів, що спрямовані на забезпечення захисту певної інформації від розголошення, витоку та несанкціонованого доступу. Організаційні заходи, у свою чергу, є обов'язковою складовою компонентою побудови будь-якої КСЗІ. Щодо інженерно-технічних заходів, то вони здійснюються у міру необхідності [20].

Організаційні заходи захисту інформації включають у себе побудову концепції інформаційної безпеки підприємства, а також:

- створення посадових інструкцій для користувачів і обслуговуючого персоналу;

- складання правил адміністрування компонентів інформаційної системи, зберігання, розмноження, обліку, знищення носіїв інформації та ідентифікації користувачів;

- формування планів дій у випадку появи спроб несанкціонованого доступу до ІР (інформаційних ресурсів) системи, виходу із ладу засобів захисту та виникнення надзвичайної ситуації;

- навчання вимогам та правилам інформаційної безпеки користувачів.

В разі необхідності, у рамках проведення організаційних заходів захисту інформації може бути створено на підприємстві службу інформаційної безпеки, проведено реорганізацію системи діловодства і зберігання необхідних документів.

Інженерно-технічні заходи захисту інформації – це сукупність спеціальних технічних засобів і їх використання з метою захисту інформації. Вибір тих чи інших інженерно-технічних заходів залежить, як правило, від рівня захищеності інформації, що необхідно забезпечити на підприємстві.

Інженерно-технічні заходи, які проводяться для захисту інформаційних ресурсів підприємства, можуть включати також використання міжмережевих екранів, захищених підключень, розмежування потоків інформації поміж сегментами мережі, використання методів та засобів шифрування й захисту від несанкціонованого доступу.

В разі необхідності, у рамках здійснення інженерно-технічних заходів, може відбуватися установка у приміщеннях системи контролю й управління доступом, системи охоронно-пожежної сигналізації.

Окремі приміщення можуть бути облаштовані засобами захисту від витоку мовної (акустичної) інформації.

Суб'єкти КСЗІ

В процес створення КСЗІ, як правило, залучаються такі сторони:

- підприємство, для якого здійснюється побудова КСЗІ (Замовник);

- підприємство, що здійснює заходи стосовно побудови КСЗІ (Виконавець);

- Адміністрація Держспецзв'язку (Адміністрація Державної служби спеціального зв'язку і захисту інформації України) (Контролюючий орган);

- організація, яка у разі необхідності залучається Виконавцем або Замовником для виконання деяких робіт стосовно створення КСЗІ (Підрядник);

- організація, яка здійснює експертизу (державну) КСЗІ (Організатор експертизи).

Об'єкти захисту КСЗІ

Отже, об'єктом захисту КСЗІ виступає інформація, у будь-якому її вигляді та формі подання. Матеріальними носіями такої інформації є сигнали. За своєю фізичною природою інформаційні сигнали можна поділити на такі види: електромагнітні, електричні, акустичні, а також їхні комбінації [20].

Сигнали ж можуть бути представлені в формі електромагнітних, механічних і інших видів коливань, причому інформація, що підлягає захисту, розташована в їхніх змінних параметрах.

В залежності від природи, такі інформаційні сигнали поширюються у певних фізичних середовищах. Середовища, у свою чергу, можуть бути твердими, рідинними і газовими. Наприклад, повітряний простір, різноманітні конструкції будівель, з'єднувальні лінії та струмопровідні елементи, заземлення й інші.

В залежності від виду й форми подання інформаційних сигналів, що циркулюють у ІТС (інформаційно-телекомунікаційній системі), у тому числі й в АС (автоматизованих системах), при побудові КСЗІ можуть бути використані різні засоби захисту інформації.

Етапи побудови КСЗІ [10].

У процесі побудові КСЗІ можна виокремити наступні етапи:

- Обстеження інформаційної інфраструктури підприємства (Замовника).
- Підготовка організаційно-розпорядчої документації.
- Розробка "Технічного завдання стосовно створення КСЗІ".
- Формування "Плану захисту інформації".
- Створення "Технічного проекту стосовно побудови КСЗІ".

- Приведення інформаційної інфраструктури підприємства (Замовника) у відповідність із "Технічним проектом стосовно побудови КСЗІ".

- Розробка "Експлуатаційної документації стосовно КСЗІ".

- Впровадження КСЗІ.

- Випробування КСЗІ.

- Здійснення державної експертизи КСЗІ та отримання "Атестата відповідності".

- Обслуговування та підтримка КСЗІ.

1. Обстеження інформаційної інфраструктури підприємства (Замовника).

Для кожної конкретної інформаційно-телекомунікаційної системи (ІТС) структура, склад і вимоги до побудови КСЗІ визначаються властивостями інформації, яка обробляється, класом автоматизованої системи (АС) і умовами її експлуатації. Спеціалісти Виконавця здійснюють обстеження (аудит) ІТС Замовника. При цьому, проводиться аналіз архітектури системи, її топології та складових елементів. Також типізуються користувачі системи, визначаються типи інформації, яка обробляється у ІТС.

За результатами виконання 1-го етапу Виконавцем розробляються такі документи:

- акт обстеження ІТС (вміщує опис, архітектуру ІТС й принципи її побудови);

- перелік об'єктів ІТС, які підлягають захисту, та затверджуються Замовником.

2. Підготовка організаційно-розпорядчої документації.

Спеціалісти Виконавця аналізують організаційно-розпорядчі документи Замовника та нормативно-правові документи в області захисту інформації, які впливають на діяльність Замовника. Зазвичай, до організаційно-розпорядчих документів відносяться: організаційна структура, штатний розпис, положення

про відділи та посадові інструкції співробітників, які пов'язані із експлуатацією ІТС, документи, які регламентують доступ до ІТС й так далі.

У результаті проведеного аналізу Виконавець, у відповідності до нормативної бази, яка діє в Україні, в галузі захисту інформації, здійснює підготовку проектів документів, що визначають організаційну структуру КСЗІ (проект наказу стосовно створення КСЗІ, проект положення стосовно служби захисту інформації, проекти процедур і посадових інструкцій і ін.), що затверджує Замовник.

3. Розробка "Технічного завдання стосовно створення КСЗІ".

Спеціалісти Виконавця розробляють та погоджують з Замовником документ "Технічне завдання стосовно створення КСЗІ", що визначає усі основні вимоги до КСЗІ та можливих варіантів реалізації складових елементів системи. Після узгодження "Технічного завдання стосовно створення КСЗІ" з Замовником, цей документ узгоджується із Контролюючим органом.

В ТЗ містяться вимоги до функціонального складу та порядку розробки й впровадження технічних засобів, що забезпечують безпеку інформації у процесі її обробки в ІТС (у обчислювальній системі), а також вимоги до фізичних, організаційних та інших заходів захисту, що реалізуються за межами обчислювальної системи ІТС у доповнення до комплексу технічних та програмних засобів захисту конкретної інформації.

"Технічне завдання стосовно створення КСЗІ" може формуватися для ІТС, які створюються вперше, а також у процесі модернізації ІТС, які вже існують, у вигляді окремого підрозділу ТЗ стосовно створення ІТС, частково окремого ТЗ чи доповнення до ТЗ стосовно створення ІТС.

4. Формування "Плану захисту інформації".

Відповідно до результатів виконання 2-го етапу, а саме, базуючись на переліку об'єктів ІТС, які підлягають захисту, Виконавець формує комплекс документів "План захисту інформації", який повинен включати:

- документ " Модель порушника (Модель загроз інформації)";

- документ "Політика безпеки інформації підприємства»;

- документ "Положення стосовно Служби захисту інформації".

Всі вищезазначені документи затверджуються Замовником.

5. Створення "Технічного проекту стосовно побудови КСЗІ".

Після узгодження з Контролюючим органом "Технічного завдання стосовно створення КСЗІ" Виконавець розробляє комплекс документів "Технічний проект стосовно побудови КСЗІ". "Технічний проект стосовно побудови КСЗІ" є комплектом документів, куди входить частина документів, які розроблені на попередніх етапах та ряд нових документів, у яких описано, як саме буде створюватися, експлуатуватися й, у разі потреби, модернізуватися КСЗІ. "Технічний проект стосовно побудови КСЗІ" створюється на підставі та відповідно до "Технічного завдання стосовно створення КСЗІ". У процесі розробки проекту КСЗІ приймаються і обґрунтовуються проектні рішення, що дають можливість реалізувати всі вимоги технічного завдання, забезпечити взаємодію і сумісність різних структурних компонентів КСЗІ, а також різноманітних заходів та способів захисту інформації. У результаті створюється пакет робочої та експлуатаційної документації, яка необхідна для проведення пусконалагоджувальних робіт, забезпечення тестування, випробувань і управління КСЗІ на підприємстві.

6. Приведення інформаційної інфраструктури підприємства (Замовника) у відповідність із "Технічним проектом стосовно побудови КСЗІ".

Особливістю 6-го етапу є те, що в момент ухвалення рішення стосовно створення КСЗІ невідомою є вартість даного етапу як для Замовника, так й для Виконавця. Зважаючи на великий можливий перелік виконання робіт, на даному етапі також існує велика ймовірність залучення до його виконання Підрядників.

На даному етапі можуть бути виконані будівельні, монтажні, пусконалагоджувальні роботи, роботи, які пов'язані з встановленням

необхідних технічних чи криптографічних засобів захисту інформації та засобів фізичного захисту структурних елементів ІТС (встановлюється необхідне програмне забезпечення і устаткування, засоби контролю доступу, охоронна та пожежна сигналізації) й таке інше.

7. Розробка "Експлуатаційної документації стосовно КСЗІ".

На даному етапі Виконавець КСЗІ формує пакет документів "Експлуатаційна документація стосовно КСЗІ", який включає:

- інструкції стосовно експлуатації КСЗІ та її елементів;
- правила та положення стосовно проведення тестування й аналізу роботи КСЗІ;
- процедури регламентного обслуговування КСЗІ;
- керівництво адміністраторів й користувачів;
- формуляр КСЗІ ІТС на підприємстві.

8. Впровадження КСЗІ.

На даному етапі Виконавець (або Підрядник під наглядом Виконавця) здійснює усі пусконалагоджувальні роботи, навчає та інструктує персонал Замовника стосовно правил і режимів експлуатації КСЗІ.

Включає перелік таких заходів:

- організація захисту інформації від НСД (несанкціонованого доступу);
- організація захисту інформації від комп’ютерних вірусів;
- розробку програми та методики попередніх випробувань;
- здійснення попередніх випробувань.

Після реалізації даного етапу впроваджена КСЗІ ІТС готова до подальшого випробування на підприємстві.

9. Випробування КСЗІ.

На даному етапі Замовник за активної підтримки Виконавця проводить випробування (попередні) КСЗІ, з метою відповідності положенням, які визначені в "Технічному завданні стосовно створення КСЗІ" та підтвердження результативності її роботи. У процесі попередніх випробувань виконуються

тестові завдання та контролюються отримані результати, що і є індикатором працездатності створеної КСЗІ.

За результатами випробування КСЗІ робиться висновок стосовно можливості представлення КСЗІ до державної експертизи. У процесі попередніх випробувань перевіряються працездатність створеної КСЗІ та відповідність її вимогам ТЗ.

У процесі дослідної експлуатації:

- відпрацьовують технології оброблення інформації, управління засобами захисту, облік машинних носіїв інформації, розмежування доступу користувачів ІТС до її ресурсів й автоматизованого контролю за діями таких користувачів ІТС;

- користувачі ІТС і співробітники служби захисту інформації набувають практичних навиків стосовно використання програмно-апаратних та технічних засобів захисту інформації, вивчають та засвоюють вимоги організаційних й розпорядчих документів стосовно питань розмежування доступу до інформаційних ресурсів і технічних засобів;

- здійснюється (за потреби) доопрацювання наявного програмного забезпечення, додаткове налагодження та конфігурація комплексу засобів й методів захисту інформації від НСД (несанкціонованого доступу);

- здійснюється (за потреби) корегування робочої й експлуатаційної документації.

Відповідно до результатів дослідної експлуатації приймається рішення стосовно готовності КСЗІ ІТС до представлення до державної експертизи.

10. Здійснення державної експертизи КСЗІ та отримання "Атестата відповідності" складається з таких етапів:

- підготовка КСЗІ до здійснення державної експертизи у Адміністрації Держспецзв'язку й супроводу експертних випробувань;

- узгодження із Адміністрацією Держспецзв'язку результатів експертизи та видача Замовникові Атестата відповідності КСЗІ.

Державна експертиза здійснюється із метою визначення відповідності КСЗІ ІТС "Технічному завданню стосовно створення КСЗІ", вимогам документації (нормативної) після захисту інформації та визначення можливості введення КСЗІ ІТС в експлуатацію.

У процесі створення КСЗІ Підприємства до функцій ПЗІ належать:

- визначення переліку відомостей, що підлягають захисту у процесі їх обробки, інших об’єктів захисту у ІТС, класифікація інформації за критерієм вимог до її конфіденційності чи важливості для підприємства, необхідних рівнів захищеності необхідної інформації, визначення порядку виведення/введення, використання та розпорядження інформації в ІТС;
- розробка й коригування моделі загроз та моделі захисту інформації в ІТС, політики безпеки інформації в ІТС;
- визначення та формування вимог до КСЗІ ІТС;
- організація та координація робіт стосовно проектування й розробки КСЗІ, безпосередня участь в проектних роботах стосовно створення КСЗІ ІТС;
- підготовка технічних пропозицій, рекомендацій стосовно запобігання витоку інформації, насамперед, технічними каналами і попередження спроб НСД (несанкціонованого доступу) до інформації у процесі створення КСЗІ ІТС;
- організація робіт та участь у випробуваннях КСЗІ ІТС, здійсненні її експертизи;
- вибір підприємств-виконавців робіт стосовно побудови КСЗІ ІТС, здійснення контролю за додержанням встановленого порядку проведення робіт стосовно захисту інформації, у взаємодії із службою охорони підприємства та РСО, погодження основних технічних та розпорядчих документів, які супроводжують процес побудови КСЗІ (технічне завдання, технічний та робочий проекти, програма та методика випробувань, плани робіт і ін.);

- участь в розробці нормативних документів, які чинні та функціонують в межах підприємства та ІТС, та які передбачають відповідальність (дисциплінарну) за порушення вимог стосовно безпеки інформації і встановлених правил експлуатації КСЗІ ІТС;
- участь в розробці нормативних документів, які чинні в межах підприємства та ІТС, та якими встановлюються правила доступу користувачів ІТС до її ресурсів, визначаються порядок, норми, правила стосовно захисту інформації й здійснення контролю за їх додержанням (наказів, рекомендацій, інструкцій, положень та ін.).

У процесі експлуатації КСЗІ до функцій ПЗІ належать:

- організація процесу керування КСЗІ ІТС;
- розслідування випадків порушень політики безпеки, непередбачених та небезпечних подій, здійснення аналізу причин, які призвели до них, супроводження бази даних таких подій;
- здійснення заходів у випадку виявлення спроб несанкціонованого доступу до ресурсів ІТС, порушенні правил експлуатації методів та засобів захисту інформації чи інших дестабілізуючих факторів та чинників;
- забезпечення контролю цілісності методів та засобів захисту інформації й оперативне реагування на вихід їх з ладу чи порушення режимів функціонування;
- здійснення керування доступом до ресурсів ІТС (розподілення між користувачами ІТС необхідних реквізитів стосовно захисту інформації – паролів, ключів, привілеїв та ін.);
- актуалізація та супроводження бази даних захисту інформації (класифікаційні мітки об’єктів, матриці доступу, ідентифікатори користувачів та ін.);
- спостереження за функціонуванням КСЗІ і її компонентів (реєстрація та аудит подій в ІТС, моніторинг подій та ін.);

- підготовка пропозицій стосовно удосконалення порядку захисту інформації в ІТС, забезпечення впровадження нових технологій захисту та модернізації КСЗІ;
- організація й проведення заходів стосовно модернізації, тестування, швидкого відновлення функціонування КСЗІ після відмов, збоїв, аварій ІТС чи КСЗІ;
- участь у роботах стосовно модернізації ІТС – узгодження пропозицій стосовно введення до складу ІТС нових компонентів, нових функціональних режимів обробки інформації і завдань, заміна засобів обробки інформації та ін.;
- забезпечення супроводження та актуалізації еталонних, резервних та архівних копій програмних компонентів КСЗІ, а також їхнього зберігання та тестування;
- проведення аналітичного оцінювання поточного стану та рівня безпеки інформації в ІТС (прогнозування виникнення нових загроз та їх врахування у моделі загроз, обґрунтування необхідності її коригування, аналіз відповідності технологій обробки інформації та реалізованої політики безпеки інформації в ІТС поточній моделі загроз тощо);
- інформування власників інформації стосовно технічних можливостей захисту інформації в ІТС та типових правил, які встановлені для персоналу та користувачів ІТС;
- негайне втручання у процес роботи ІТС у випадку виявлення атаки на КСЗІ та проведення в таких випадках робіт стосовно викриття порушників;
- регулярне подання звітів керівництву підприємства (власника/ розпорядника) ІТС стосовно виконання користувачами ІТС вимог із захисту інформації;

- аналіз відомостей стосовно технічних засобів захисту інформації так званого «нового покоління», обґрунтування пропозицій стосовно придбання засобів захисту такої інформації на підприємстві;
- контроль за виконанням персоналом та користувачами ІТС вимог, норм, інструкцій, та правил стосовно захисту інформації у відповідності до визначеної на підприємстві політики безпеки інформації, в тому числі контроль над забезпеченням режиму секретності у випадку обробки в ІТС інформації, яка складає державну таємницю;
- контроль за дотриманням порядку, охорони та зберігання документів (носіїв інформації), що містять відомості, які підлягають захисту;
- розробка та реалізація спільно із РСО підприємства комплексних заходів стосовно безпеки інформації у результаті проведення заходів стосовно науково-технічного, інформаційного та економічного співробітництва із іноземними підприємствами, а також у результаті проведення нарад, переговорів і ін., здійснення їхнього інформаційного та технічного забезпечення [10].

3.2 Пропозиції щодо удосконалення методичної бази підприємства з питань інформаційної безпеки

Важливою умовою забезпечення економічної та інформаційної безпеки підприємства являється створення ефективних спеціалізованих підрозділів, ціллю яких є інформаційна діяльність.

У одних фірмах – це інформаційно-аналітичний відділ, в інших – відділ маркетингу, на який керівництво фірми разом з іншими покладає і інформаційно-аналітичні завдання, в третіх — відділ комерційної розвідки. Часто все залежить від рівня розуміння керівництвом фірми ступеня важливості інформаційно-аналітичної роботи для безпеки всіх сторін діяльності будь-якої комерційної структури та фінансових можливостей

самого підприємства [2].

У цьому контексті, головним завданням будь-якого з даних підструктурних елементів являється збір релевантної бази даних і обробка різноманітної інформації щодо:

- економічного стану фірми, регіону, своєї країни, країн, в яких є партнери;
- політичної ситуації в регіоні і країні; морально-психологічного клімату в колективі;
- конкурентів і дієвості використовуваних методів конкуренції (добросовісною і недобросовісною);
- кримінальні структури і можливі терористичні погрози;
- визначення цільових завдань по перевірці потенційних партнерів, клієнтів, конкурентів;
- розробки програм протидії промисловому шпигунству, терористичним погрозам і іншим методам недобросовісної конкуренції;
- розробки програм дезінформації конкурентів:

через засоби масової інформації;

через інформаційно-телекомунікаційні канали;

через постачальників, суміжників, партнерів, клієнтів;

шляхом організації псевдо сприйняття конфіденційної інформації.

При цьому, слід зважати і на те, що захист інформації слід здійснювати поетапно, а саме:

1 етап — визначення масштабів розповсюдження й аналіз рівня і типу загроз;

2 етап — розроблення технологій та формування системи захисту інформаційно-методичного забезпечення;

3 етап — реалізація плану цільового захисту інформації;

4 етап — контролювання, коригування та керування системою захисту

інформації.

На першому етапі здійснюється аналіз об’єктів захисту інформації, ситуаційного плану, умов функціонування Підприємства, оцінити ймовірність прояву загроз та очікувану шкоду від їх реалізації, підготувати дані для побудови окремої моделі загроз.

Джерелами загроз може бути діяльність розвідок інших суб’єктів господарювання, а також навмисні або ненавмисні дії юридичних і фізичних осіб.

На другому етапі розробляється план захисту інформації, що містить організаційні, первинні технічні та основні технічні заходи захисту, визначити зони безпеки інформації.

Рівень захисту інформації означується системою кількісних та якісних показників, які забезпечують розв’язання завдання захисту інформації на основі норм та вимог захисту інформації.

Мінімально необхідний рівень захисту інформації забезпечують обмежувальними і фрагментарними заходами протидії найнебезпечнішій загрозі.

На третьому етапі слід реалізувати організаційні, первинні технічні та основні технічні заходи захисту, установити необхідні зони безпеки інформації, провести атестацію технічних засобів забезпечення інформаційної діяльності, технічних засобів захисту інформації, робочих місць (приміщень) на відповідність вимогам безпеки інформації. Засоби захисту інформації можуть функціонувати автономно або спільно з технічними засобами забезпечення інформаційної діяльності у вигляді самостійних пристроїв або вбудованих у них складових елементів. На четвертому етапі необхідна організація проведення обстеження об’єктів інформаційної діяльності підприємства. Метою обстеження об’єктів інформаційної діяльності підприємства є визначення об’єктів захисту, виявлення загроз, їхній аналіз та побудова окремої моделі загроз [7].

Визначення вимог до економічної інформації підприємницьких структур слід вважати важливою передумовою для побудови раціональних інформаційних потоків при зниженні витрат на їх формування та підвищення ефективності управління. В умовах переходу до ринкової системи господарювання значно розширилось коло користувачів економічної інформації, яка характеризує результати роботи підприємницьких організацій. Це не тільки підвищило актуальність питань, пов’язаних із визначенням вимог до економічної інформації, а й зумовило необхідність вирішення нових завдань у сфері інформаційного забезпечення, визначення інформаційних ризиків і шляхів їх зниження.

Раціональна система інформаційного забезпечення підприємницької організації повинна відповідати таким вимогам:

1) з позицій держави — забезпечувати об’єктивність даних, на основі яких здійснюються розрахунки макроекономічних показників, розрахунки з державою, включаючи систему оподаткування; використання природних ресурсів, трудових ресурсів, дотримання встановлених екологічних норм і нормативів;

2) з боку споживачів продукції, робіт, послуг — якість товару, ціни, безпека в користуванні;

3) з позицій інвесторів — фінансовий стан підприємства, величина ризику при вкладанні капіталів у розвиток підприємницької структури, її перспективи і стратегія розвитку;

4) з позицій акціонерів — величина прибутків, величина дивідендів, перспективи розвитку підприємства;

5) з позицій контролюючих органів — дотримання чинного законодавства з питань здійснення підприємницької діяльності;

6) з позицій постачальників сировинно-матеріальних ресурсів — фінансова стабільність підприємства, його платоспроможність на поточний час і в перспективі;

7) з позицій найманих працівників підприємств — оплата праці, стабільність фінансового стану, перспективи розвитку;

8) з позицій менеджерів і адміністрації — забезпечення повної достовірної інформації, необхідної для прийняття обґрунтованих управлінських рішень [35].

Підвищення ефективності підприємницької діяльності на основі забезпечення повноти і достовірності економічної інформації передбачає реалізацію заходів у напрямах адаптації підприємницьких управлінських структур у відповідності з міжнародними стандартами, зниження підприємницьких ризиків на основі забезпечення повноти і достовірності економічної інформації.

Отже, оскільки головними завданнями реалізації технологій управління економічною безпекою є: 1) забезпечення найефективнішого функціонування промислового підприємства; 2) найпродуктивнішої діяльності операційної системи за умов раціонального використання різних видів ресурсів; 3) забезпечення певного рівня ефективності менеджменту персоналу та якості господарських процесів; 4) нарощування стратегічного потенціалу; 5) збалансований розвиток. Відтак, перманентний захист інформаційно-методичної бази даних і постійне уточнення напрямів підвищення рівня інформаційної безпеки уможливить досягнення визначених завдань і забезпечення економічних інтересу суб’єкта господарювання.

Висновки до третього розділу

Об’єктивним є визнати, що макроекономічна динаміка параметрів розвитку промисловості не відповідає вимогам як до ефективності її функціонування та суспільним очікування, так і до достатності забезпечення рівня економічної безпеки в цілому та інформаційної,

зокрема. Це зумовлене неспроможністю держави формування системи регулювання економікою, а також можливістю адаптації до мінливих умов функціонування реального сектору:

а) використовуваних заходів забезпечення захисту інформаційно-методичної безпеки,

б) механізмів усунення загроз від перманентного протікання економічних, соціальних, технологічних та політичних криз в нашому «державному утворенні».

Маючи на меті розробку ключових алгоритмів системи безпеки у сфері підприємництва, доцільно розглянути основні інститути цієї системи, а саме:

— внутрішньобанківські засоби та системи економічної безпеки у сфері кредитних відносин;

— організаційно-правові форми, структуру та принципи страхової справи як фактора зниження ризиків у сфері підприємництва;

— інші види гарантій щодо зниження ризиків у сфері фінансово-господарської діяльності;

— захист інформації з обмеженим доступом, її правовий режим.

Як висновок треба зазначити, що кваліфікований підхід до побудови системи захисту інформації в сучасних інформаційно-комунікаційних системах та мережах має на увазі конкретну оцінку ймовірності вияву кожної загрози. Таким чином, кожній інформаційній системі, в залежності від конкретних умов його роботи, потрібна персональна система захисту інформації.

Побудова захищеної інформаційної системи можлива лише на аудиторських умовах спеціально залученими фахівцями і фірмами, що мають ліцензію на вказаний характер діяльності. Розглянувши загальні поняття, напрями та засоби захисту інформації в сучасних інформаційно-комунікаійних ситсемах та мережах, потрібно зазначити, що комплексний захист інформації

має в своєї основі використання фізичних, законодавчих, організаційних та програмно-технічних засобів захисту. Такі засоби повинні забезпечувати ідентифікацію та аутентифікацію користувачів, розподіл повноважень доступу до системи, реєстрацію та облік спроб несанкціонованого доступу. Всі ці заходи в комплексі, як правило, спрямовані на чіткий розподіл відповідальності при роботі персоналу з інформацією, створення декількох рубежів контролю, запобігання навмисному або випадковому знищенню та модифікації інформації.

ВИСНОВКИ

Отже в результаті проведеного дослідження з’ясовано, що проблема забезпечення інформаційної безпеки (ІБ) будь-якої компанії є надзвичайно актуальною на сучасному етапі розвитку інформаційних технологій (ІТ), яка супроводжується постійними інформаційними загрозами – як зовнішніми, так і внутрішніми. Тому керівники служб ІБ мають прийняти як аксіому твердження про те, що звичайна оперативність реагування на сучасні загрози ІБ вже не є достатньою для їх попередження чи знешкодження з найменшими втратами.

Встановлено, що поява нових ІТ відкривають перед компаніями не тільки небачені можливості, але й піддають їх потенційним загрозам з невідомих раніше джерел. Хмарні комп'ютерні технології як і раніше є головним джерелом інновацій в сучасному інформаційному середовищі: за останні декілька років кількість компаній, які використовують хмарні обчислення, збільшилася майже удвічі.

Виявлено, що заплановане збільшення бюджету на удосконалення системи ІБ виявиться ефективним тільки в разі належного розподілу обов'язків між відповідальними за прийняття рішень. У багатьох компаніях питанням забезпечення ІБ як і раніше займаються інформаційно-технологічні відділи. Оскільки забезпечення ІБ починає виходити за рамки традиційних можливостей ІТ, в даний час потрібно приймати рішення про вибір дещо інших інструментів, процесів і методів моніторингу джерел загроз ІБ, оцінювання ефективності роботи персоналу служби ІБ, пошуку прогалин у системі ІБ, що і визначає потребу перерозподілу відповідальності.

Інформаційна безпека підприємства на практиці включає сукупність напрямів, методів, засобів і заходів, що знижують вразливість інформації і перешкоджають несанкціонованому доступу до інформації, її розголошенню або витоку. Елементами цієї системи є: правовий, організаційний, інженерно-

технічний захист інформації, а основною її характеристикою **- комплексність.**

Структура системи, склад і зміст елементів, їх взаємозв'язок залежать від об'єму і цінності інформації, що захищається, характеру можливих загроз безпеки інформації, необхідної надійності захисту і вартості системи.

Слід зазначити, що ключовим фактором, у забезпеченні інформаційної безпеки підприємства є його персонал. Основними заходами при роботі з яким є: проведення аналітичних процедур при прийомі і звільненні; навчання і інструктаж практичним діям по захисту інформації; контроль за виконанням вимог по захисту інформації, стимулювання відповідального відношення до збереження інформації та ін.

Не менш важливим є питання **економічного обгрунтування** витрат на захист інформації. Адже чим вище рівень захищеності інформації, тим за інших рівних умов, буде нижче розмір можливих збитків, але тим вищою буде вартість захисту. Оптимальний розміром витрат на захист буде такий, при якому забезпечується рівень захищеності, що дорівнює мінімуму загальних витрат. Вартість збитків визначається двома параметрами: ймовірністю реалізації різних загроз інформації; вартістю (важливістю) інформації, захищеність якої може бути порушена під впливом різних загроз. У зв'язку зі складністю дати кількісну оцінку збитків (сума втрат або розмір недоотриманого прибутку) причиною яких може бути витік, або втрата інформації, що захищається, в даний час найбільш доцільним є підхід на основі експертних оцінок. За даними висновків експертів можуть бути отримані статистично стійкі оцінки можливого збитку.

Захист інформаційних ресурсів підприємства є одним з ключових завдань в умовах підвищення рівня внутрішніх і зовнішніх загроз інформаційної безпеки, що можуть безпосередньо вплинути на його фінансову діяльність і стійкість на ринку. Щоб зберегти бізнес, розвиватися і бути конкурентоспроможним, підприємствам необхідно створити ефективну систему управління інформаційною безпекою. **Сутність викладеного дає**

підстави стверджувати, що в сучасних умовах, без належного захисту інформаційного середовища підприємства не можливо забезпечити його безпеку в цілому.

Сьогодні спеціалізовані фірми пропонують широкий спектр засобів захисту інформаційних систем з урахуванням їх вартості та функціональних можливостей. Найбільш прийнятним підходом при виборі того чи іншого варіанту є дотримання принципу «розумної достатності», суть якого полягає в тому, що визначальними при проектуванні політики інформаційної безпеки повинні бути: розмір підприємства, його ресурсні та фінансові можливості, поточний рівень інформаційної безпеки, стадія функціонування фірми.

Як результат, можна виділити такі підсистеми ефективного захисту інформації на підприємстві:

1. Підсистема антивірусного захисту шлюзів входу в мережу Інтернет, файлових серверів, робочих місць користувачів, централізованого управління, періодичного оновлення антивірусних баз даних.
2. Підсистема управління контролем доступу та ідентифікацією в інформаційній системі.
3. Підсистема міжмережного екранування, яка дозволяє реалізувати безпеку міжмережної взаємодії через використання програмних і програмно-апаратних міжмережних екранів.
4. Підсистема криптографічного захисту, яка гарантує безпеку передачі інформації завдяки шифруванню даних.
5. Підсистема забезпечення цілісності інформації та програмного середовища шляхом застосування відповідних засобів для фіксації та контролю стану програмного комплексу, управління зберіганням даних для резервного копіювання та архівування.

6. Підсистема захисту від інсайдерів, яка контролює дії порушників, реалізує інформаційну безпеку при управлінні доступом і реєстрації.

7. Підсистема захисту систем управління базами даних.

8. Підсистема виявлення вторгнень і спроб несанкціонованого доступу до інформаційних ресурсів підприємства. Підсистема забезпечує реалізацію захисних заходів з протидії атакам хакерів і поширенню спаму.

9. Підсистема захисту мобільних пристроїв.

10. Підсистема моніторингу подій інформаційної безпеки, яка дозволяє своєчасно виявляти загрози інформаційній системі та оперативно реагувати на них.

Постійна робота в сфері підтримки інформаційної безпеки на належному рівні є необхідною умовою ефективності підприємницької діяльності. І тільки комплексна система може гарантувати досягнення максимальної ефективності захисту інформації, тому що системність забезпечує необхідні складові захисту й установлює між ними логічний і технологічний зв'язок, а комплексність, що вимагає повноти цих складових, всеохоплення захисту, забезпечує її надійність.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Богуш В. М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: «МК-Прес», 2015. – 432с.
2. Братель О. Поняття та зміст доктрини інформаційної безпеки / О. Братель // Право України. – 2017. – № 5. – С. 36-40.
3. Березюк Л. П. Организационное обеспечение информационной безопасности [Текст]: навч. посібник / Л. П. Березюк. – Хабаровськ: ДВГУПС, 2012. – 188 с.
4. ГОСТ 28147-89 "Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования".
5. ГОСТ 34.10-95 "Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма".
6. ГОСТ 34.11-95 "Информационная технология. Криптографическая защита информации. Функция хэширования".
7. Гуцалюк М. Інформаційна безпека України: нові загрози / М. Гуцалюк // Бизнес и безопасность. – 2013. – № 5. – С. 2-3.
8. Домарев В. В. Безопасность информационных технологий. Системный подход: – К.: ООО «ТИД «ДС», 2014. – 992 с.
9. Домарев В. В. Створення підрозділу захисту інформації [Електронний ресурс]. – Доступний з http://www.trn.ua/articles/2101/
10. Етапи побудови КСЗІ [Електронний ресурс]. – Доступний з http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi
11. Закон України "Про інформацію".
12. Закон України "Про ліцензування певних видів господарської діяльності".
13. Закон України "Про захист персональних даних".

14. Закон України "Про доступ до публічної інформації".
15. Закон України "Про державний контроль за міжнародними передачами товарів військового призначення та подвійного використання".
16. Захаров Е. Информационная безопасность или опасность отставания [Текст] / Е. Захаров // Права людини. – 2010. – № 1 . – С. 3-5.
17. Игнатьев В. А. Информационная безопасность современного коммерческого предприятия [Текст] : монографія / В. А. Игнатьев. – Старий Оскол: ООО «ТНТ», 2015. – 448 с.
18. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1 / С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с..
19. Компании ищут способы оперативного реагирования на современные угрозы и больше не могут обеспечивать информационную безопасность путем решения отдельных задач [Электронный ресурс]. – Доступный с http://www.ey.com/RU/ru/Newsroom/News-rele-ases/Press-Release---2017-10-29-2
20. Комплексна система захисту інформації (КСЗІ) [Електронний ресурс]. – Доступний з http://altersign.com.ua/korysna-informacija/pobudova-kszi/etapy-pobudovy-kszi
21. Корнюшин П.Н. Информационная безопасность / П.Н. Корнюшин, С.С. Костерин. – Владивосток: ТИДОТ ДВГУ, 2013. – 154 с.
22. Маракова І. Захист інформації [Текст] : підручник / І. Маракова, А. Рибак, Ю. Ямпольский – Одеса : ОдНПУ, 2011. – 164 с.
23. Матиев Д. Средства защиты информации: проблема выбора и соответствия / Д. Матиев [Електронний ресурс]. – Доступний з http://bankir.ru/publikacii/s/sredstva-zaschiti-informacii-problema-vibora-i-sootvetstviya-5386161/
24. Мониторинг утечек информации [Электронный ресурс]. – Доступный с http://www. infowatch.ru/analytics/leaks_monitoring

25. Положення про порядок здійснення криптографічного захисту інформації в Україні, затверджене Указом Президента України від 22.05.98 № 505.
26. Постанова Кабінету Міністрів України від 25.05.2011 № 616 "Про затвердження Положення про Державний реєстр баз персональних даних та порядок його ведення".
27. Постанова Кабінету Міністрів України від 14.11.2000 № 1698 "Про затвердження переліку органів ліцензування".
28. Постанова Кабінету Міністрів України від 29.10.2000 № 1755 "Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу".
29. Постанова Кабінету Міністрів України від 04.07.2001 № 756 "Про затвердження переліку документів, які додаються до заяви про видачу ліцензії для окремого виду господарської діяльності".
30. Постанова Кабінету Міністрів України від 25.05.2011 № 543 "Про затвердження переліків послуг у галузі криптографічного захисту інформації (крім послуг електронного цифрового підпису) та криптосистем і засобів криптографічного захисту інформації, господарська діяльність щодо яких підлягає ліцензуванню".
31. Положення про порядок проведення експертизи в галузі експортного контролю, затверджене постановою Кабінету Міністрів України від 15.07.97 № 767.
32. Правила проведення робіт із сертифікації засобів захисту інформації, затверджені наказом Держспоживстандарту та Адміністрації Держспецзв'язку від 25.04.07 № 75/91 та зареєстровані у Мін`юсті 14.05.07 № 498/13765.
33. Про основні засади інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 9 січня 2007 року // Офіційний вісник України.
34. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко [Електронний ресурс]. –

Доступний з http://nbuv.gov.ua/portal/ Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf

35. Чубарук Т. Проблеми законодавчого забезпечення інформаційної безпеки в Україні / Т. Чубарук // Право України. – 2017. – № 9. – С. 67-69.
36. Щербина В. М. Інформаційне забезпечення економічної безпеки підприємств та установ [Текст] / В. М. Щербина // Актуальні проблеми економіки. – 2016. – № 10. – С. 220-225.
37. ISO/IEC 17799:2005. Information technology. Security techniques. Code of practice for information security management.
38. ISO/IEC 27001:2005. Information technology. Security techniques. Information security management systems. Requirements.
39. ISO/IEC TR 18044:2004. Information technology -Security techniques - Information security incident management/
40. ISO/IEC 20000:2005. Information technology. Service management. Part 2: Code of practice/