МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації
(назва факультету, інституту)

Систем інформаційного та кібернетичного захисту
(назва кафедри)

"На правах рукопису"

«До захисту допущено»
Завідувач кафедри
Шуклін Г.В.
(підпис) (ініціали, прізвище)
“____” _____ 2021р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 Кібербезпека
(код та назва спеціальності)

на тему: Підвищення рівня системи захисту інформації на підприємстві

Студент групи СЗДМ – 61 Вдовиченко Олексій Віталійович _____
(шифр групи) (прізвище, ім’я, по батькові) (підпис)

Керівник к.т.н., Ахрамович Володимир Миколайович _____
(вчені ступінь та звання, прізвище, ініціали) (підпис)

Нормоконтроль: Гребенніков А.Б. _____
(вчені ступінь та звання, прізвище, ініціали) (підпис)

Київ – 2021

ЗАТВЕРДЖУЮ»

Завідувач кафедри

_____ Шуклін Г.В.
(підпис) (ініціали, прізвище)

“__” _____ 2021р.

ЗАВДАННЯ

на атестаційну роботу магістра

студенту Вдовиченко Олексію Віталійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи: Підвищення рівня системи захисту інформації на підприємстві

Затверджена наказом по університету від “__”_____ 2021р. №_____

2. Термін здачі студентом оформленої роботи “____”_____2021р.

3. Об’єкт дослідження: підприємство ЗАТ «БКІ»

4. Предмет дослідження: системи захисту інформації

5. Мета роботи: підвищення рівня системи захисту інформації на підприємстві

6. Перелік питань, які мають бути розроблені:

7. Перелік публікацій: Ахрамович В.М., Вдовиченко О.В. – Метод розрахунку захисту персональних даних від довіри між користувачами та інтенсивності передавання данних у соціальних мережах

8. Перелік ілюстративного матеріалу:

9. Дата видачі завдання “__” _____ 2021 р.

Керівник _____ Ахрамович В. М.
(підпис) (ініціали, прізвище)

Завдання прийняв до виконання _____ Вдовиченко О.В.
(підпис) (ініціали, прізвище)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	**Примітка**
1	Підбір науково-технічної літератури	05.10.2021	Вик.
2	Обґрунтування актуальності теми роботи	17.10.2021	Вик.
3	Написання першого розділу роботи	22.10.2021	Вик.
4	Написання другого розділу роботи	28.10.2021	Вик.
5	Написання третього розділу роботи	03.11.2021	Вик.
6	Написання висновків по роботі	18.11.2021	Вик.
8	Підготовка демонстраційних матеріалів	25.11.2021	Вик.
9	Підготовка доповіді	05.12.2021	Вик.
10	Захист в ДЕК	18.01.2022	

Студент _____ Вдовиченко О.В.
(підпис) (ініціали, прізвище)

Керівник роботи _____ Ахрамович В. М.
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Мета випускної кваліфікаційної роботи: у цій дипломній роботі розглянуто питання, пов'язані з розробкою системи захисту інформації на підприємстві. У ході виконання роботи було проведено аналіз інформаційних засобів захисту інформації, в результаті якого виявлено склад джерел та носіїв інформації, проведено категорування інформації, виявлено можливі канали витоку інформації.

Завдання випускної кваліфікаційної роботи: в рамках аудиту інформаційної безпеки було проаналізовано поточну діяльність підприємства з питань захисту інформації, проведено оцінку інформаційної системи організації, в якій циркулює конфіденційна інформація; були виявлені недоліки системи захисту, способи усунення яких представлені в роботі.

У результаті виконання дипломної роботи було розроблено комплексну систему захисту інформації, було проведено підбір технічних та програмно-апаратних засобів.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

НСД – несанкціонований доступ

ЗЗКІ – засоби захисту конфіденційної інформації

АС – автоматизована система

КІ – кредитна історія

БКІ – бюро кредитних історій

КІ – кредитна історія

СЗІ - система захисту інформації

ПРД – правила розмежування доступу

ЦП – цифровий підпис

ПЗ – програмне забезпечення

НЕП – некваліфікований електронний підпис

ЗМІСТ

ВСТУП

У сучасному світі складно уявити організацію роботи людини, підприємства без застосування автоматизованих систем та процесів. При цьому кожен розробник намагається зробити свою систему більш простою та зручною у використанні, оскільки конкуренція на цьому ринку досить велика. Щороку сфера інформаційних технологій розвивається все швидше. Дедалі більше піддаються автоматизації різні виробничі процеси. Також неухильно зростає і кількість користувачів мережі Інтернет. І, звичайно, нині рідкісна система, навіть найпростіша, яка функціонує без використання ресурсів мережі Інтернет.

Крім зовнішніх впливів на безпеку (пограбування, зламування) організації існує загроза витоку інформації по інформаційних каналах зв'язку. Становиться недостатнім лише зовнішнє забезпечення безпеки. З'являється все більше різних фірм, що виробляють однакові послуги, зростає і конкуренція. У таких умовах кожен керівник зацікавлений у забезпеченні цілісності, доступності та конфіденційності інформації щодо діяльності організації. Для вирішення таких завдань з'явився цілий напрямок, пов'язаний з розробкою комплексного підходу до забезпечення безпеки інформаційних ресурсів різних рівнях. Комплексне забезпечення захисту інформації дозволяє запобігти максимальній кількості загроз.

Особливе місце у списку автоматизованих систем займають ті, що обробляють конфіденційну інформацію. Нині АС розділені на три групи, кожної з яких відповідають своїм клас захищеності [1].

1. Перша група включає АС, що мають на увазі безліч користувачів. У таких АС одночасно обробляється та/або зберігається інформація різних рівнів конфіденційності. Доступ користувачів до інформаційних ресурсів обмежений. Група містить п'ять класів: 1Д, 1Г, 1В, 1Б, 1А.
2. Друга група включає автоматизовані системи, в яких користувачі мають ті самі права доступу до всієї інформаційної бази автоматизованої системи. Інформація обробляється та/або зберігається на носіях різного рівня конфіденційності. Група містить два класи: 2Б, 2А.

3. Третя група включає автоматизовані системи, де працює один користувач. Користувач має доступ до всієї інформаційної бази системи. Інформація розміщена на носіях одного рівня конфіденційності. Група містить два класи: 3Б, 3А.

Для якісного та коректного забезпечення безпеки необхідний детальний аналіз роботи АС, що включає розбір всіх процесів, уразливостей, можливих загроз при НСД.

Тому для даної роботи головною метою є розробка системи захисту інформації для закритого акціонерного товариства «Бюро кредитних історій». Для вирішення поставленого завдання потрібне проведення наступних робіт [2]:

1. Аналіз наявної системи захисту інформації ЗАТ «БКІ».

1.1. Аудит системи захисту інформації ЗАТ «БКІ»..

1.2. Опис існуючих інформаційних ресурсів ЗАТ «БКІ»..

1.3. Аналіз загроз та вразливостей системи захисту інформації ЗАТ «БКІ»..

1.4. Аналіз ризиків системи захисту інформації ЗАТ «БКІ»..

2. Проектування.

2.1. Розробка концепції системи захисту інформації (політики та процедури системи).

2.2. Розробка моделі системи безпеки.

2.3. Технічне проектування, розробка документації.

3. Використання.

Реалізувавши всі перераховані вище дії, вдасться побудувати комплексну систему захисту інформації. Система буде включати технічні та програмні компоненти, що дозволить попередити максимальну кількість загроз.

Необхідно проводити своєчасне оновлення всіх засобів, що входять до складу системи, стежити за коректною роботою всіх компонентів, запобігати можливим збоям у роботі.

Таким чином, система захисту інформації є комплексом програмних і технічних засобів, організаційних заходів та правових норм, спрямованих на

протидію різного виду загрозам інформації, що захищається, інформаційним системам та користувачам.

У цій роботі буде розглянуто умовну організацію ЗАТ «БКІ»., яка ґрунтується на реальному підприємстві . З метою збереження комерційної таємниці назва цього підприємства розголошуватися не може.

1. ОСНОВНІ ПОНЯТТЯ ЗАХИСТУ ІНФОРМАЦІЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Сучасні методи обробки, передачі та зберігання інформації сприяють появі загроз, пов'язаних з можливістю втрати, спотворення та розкриття конфіденційної інформації. Тому забезпечення захисту інформації комп'ютерних систем та мереж є одним із провідних напрямків розвитку інформаційних технологій.

Нижче наведено основні визначення захисту інформації та інформаційної безпеки комп'ютерних систем та мереж з урахуванням визначень «Захист інформації. Основні терміни та поняття».

Захист інформації — організаційні заходи, спрямовані на запобігання витоку конфіденційної інформації та небажаних впливів на інформацію, що захищається.

Захист інформації від витоку — організаційні та технічні заходи, спрямовані на запобігання неконтрольованому поширенню/копіюванню конфіденційної інформації внаслідок її розголошення.

Захист інформації від розголошення – організаційні технічні заходи, спрямовані на запобігання несанкціонованого доступу до конфіденційної інформації розголошення її суб'єктам, які мають права доступу до цієї інформації.

Система захисту інформації - сукупність суб'єктів та об'єктів конфіденційної інформації, технічних та програмних засобів захисту інформації. Така система створюється і функціонує відповідно до правил і норм, що встановлюються відповідними керівними актами в галузі захисту інформації.

Сучасна автоматизована система обробки конфіденційної інформації є складною системою, що складається з великої кількості компонентів різного ступеня автономності, які пов'язані між собою і обмінюються даними. Практично кожен компонент може зазнати зовнішнього впливу або вийти з ладу. Компоненти АС можна розбити на такі групи [3]:

1. Апаратні засоби - комп'ютери та їх складові (процесори, монітори, термінали, периферійні пристрої – дисководи, принтери, контролери, кабелі, лінії зв'язку тощо).
2. Програмне забезпечення - різні програми, утиліти та т.д.
3. Дані - різна інформація, що зберігається на дисках, дискетах, у журналах тощо.
4. Персонал - користувачі системи та обслуговуючі співробітники.

Для безпеки всіх компонентів АС необхідний комплексний підхід до розробки системи захисту конфіденційної інформації. Так само не варто забувати і про засоби захисту, що використовуються в процесі побудови системи. Всі ЗЗК повинні бути сертифіковані[4]

1.1. Сертифікація засобів захисту конфіденційної інформації

Засоби захисту конфіденційної інформації, що використовуються при організації системи захисту інформації, обов'язково мають бути сертифіковані відповідно до державних стандартів.

Сертифікація - процес зіставлення засобів захисту з державними стандартами, і подальша видача підтвердження при успішному тестуванні [5].

Сертифікація засобів захисту інформації щодо вимог безпеки та захисту інформації — організаційні заходи щодо підтвердження властивостей технічних та програмних засобів захисту інформації відповідно до вимог державних стандартів. Відповідно до вимог чинного законодавства, обов'язковій сертифікації підлягають засоби захисту наступної інформації [6]:

1. Відомості, що становлять державну таємницю.

Державна таємниця – відомості, що перебувають під захистом держави, у сфері її військової, зовнішньополітичної, економічної, розвідувальної, контррозвідувальної та оперативно-розшукової областей. Поширення таких даних може завдати шкоди безпеці.

2. Державні інформаційні ресурси.

Державні інформаційні ресурси — ресурси, що перебувають у власності держави.

3. Персональні дані.

Персональні дані — будь-яка інформація, що прямо чи опосередковано відноситься до суб'єкта конфіденційної інформації.

Сертифікація здійснюється з метою:

- створення умов для діяльності організацій і підприємців на єдиному товарному ринку України, а також для участі в міжнароднім економічнім, науково-технічнім співробітництві й міжнародній торгівлі;
- сприяння споживачам у компетентному виборі продукції;
- захисту споживача від несумлінності виготовлювача (продавця, виконавця);

- контролю безпеки продукції для навколишнього середовища, життя, здоров’я й майна;
- підтвердження показників якості продукції, заявлених виготовлювачем.

Сертифікація може мати обов’язковий і добровільний характер.

Учасниками процесу сертифікації є:

1. Заявники – ті, хто прагне одержати сертифікат відповідності. Заявниками можуть бути продавці продукції, виконавці продукції.
2. Орган по сертифікації;
3. Центральний орган сертифікації – орган, що очолює сертифікацію однорідної продукції (необов’язковий учасник).
4. Органи з сертифікації засобів захисту інформації – ті, хто проводить сертифікацію певної продукції.
5. Іспитові лабораторії – лабораторії сертифікаційних випробувань певної продукції. В основні обов’язки органа по сертифікації входить:

1. Створення системи сертифікації;
2. Вибір способу підтвердження відповідності засобів захисту інформації;
3. Визначення переліку засобів захисту, для яких необхідна сертифікація;
4. Установлення правил акредитації центральних органів систем сертифікації, органів по сертифікації засобів захисту інформації, іспитових лабораторій і проведення відповідних акредитацій;
5. Видача сертифікатів і ліцензій на застосування знака відповідності;
6. Ведення реєстру сертифікованих засобів і учасників сертифікації;
7. Здійснення контролю й нагляду за дотриманням учасниками сертифікації правил сертифікації й за сертифікованими засобами захисту інформації;
8. Розгляд апеляції з питань сертифікації;
9. Періодична публікація інформації про сертифікацію;
10. Організація підготовки й атестації експертів-аудиторів;
11. Призупинення, продовження або скасування дії виданих сертифікатів.

Органи сертифікації:

1. Беруть участь у визначенні схеми проведення сертифікації засобів захисту інформації з урахуванням пропозицій заявника;

2. Уточнюють вимоги, на відповідність яким проводяться сертифікаційні випробування;

3. Рекомендують заявникові іспитовий центр (лабораторію);

4. Затверджують програми й методики проведення сертифікаційних випробувань;

5. Проводять експертизу технічної, експлуатаційної документації на засоби захисту інформації й матеріалів сертифікаційних випробувань;

6. Оформляють експертний висновок по сертифікації засобів захисту інформації й представляють їх у державний орган по сертифікації;

7. Організують, при необхідності, попередню перевірку (атестацію) виробництва засобів захисту інформації;

8. Беруть участь в акредитації іспитових центрів (лабораторій) і органів по атестації об'єктів інформатизації;

9. Організують інспекційний контроль над стабільністю характеристик сертифікованих засобів захисту інформації й беруть участь в інспекційному контролі над діяльністю іспитових центрів (лабораторій);

10. Зберігають документацію (оригінали) засобів захисту інформації про сертифікацію;

11. Клопочуться перед державним органом по сертифікації про припинення або скасування дії виданих сертифікатів;

12. Формують і актуалізують фонд нормативних і методичних документів, необхідних для сертифікації, беруть участь у їхній розробці;

13. Представляють заявникові необхідну інформацію із сертифікації.

Іспитові центри (лабораторії) у межах установленої області акредитації:

1. Здійснюють добір зразків засобів захисту інформації для проведення сертифікаційних випробувань;

2. Розробляють програми й методики сертифікаційних випробувань, здійснюють сертифікаційні випробування засобів захисту інформації, оформляють протоколи сертифікаційних випробувань і технічні висновки;

3. Маркірують сертифіковані засоби захисту інформації знаком відповідності в порядку, установленому правилами системи сертифікації;

4. Беруть участь в атестації виробництва сертифікуємих засобів захисту інформації.

Іспитові центри (лабораторії) відповідають за повноту випробувань засобів захисту інформації, вірогідність, об'єктивність і необхідну точність вимірів, своєчасну перевірку засобів вимірів і атестацію іспитового встаткування.

Органи сертифікації засобів захисту інформації й іспитові лабораторії проходять процедуру акредитації на право проведення робіт із сертифікації, у ході якої державний орган по сертифікації перевіряє їхню здатність на проведення даних робіт і видає дозвіл.

Сертифікація проводиться на матеріально-технічній базі акредитованих іспитових лабораторій. В окремих випадках можливе проведення випробувань на базі заявника при належному контролі з боку органа сертифікації.

Виготовлювачі зобов'язані сповіщати орган по сертифікації, який видав сертифікат на їхню продукцію, про зміни в технології виготовлення або складі сертифікованого засобу захисту інформації.

Процедура сертифікації включає:

1. Подачу й розгляд заявки на проведення сертифікації (продовження терміну дії) засобу захисту інформації в орган по сертифікації. Заявка оформляється на бланку заявника й засвідчується печаткою. Державний орган призначає орган по сертифікації й іспитову лабораторію, після чого заявник відправляє туди сертифікуємий засіб захисту інформації.

2. Сертифікаційні випробування засобів захисту інформації й (при необхідності) атестацію їх виробництва. Терміни проведення випробувань установлюються на договірній основі між заявником і лабораторією. За результатами випробувань оформляється висновок, який відправляється в орган по сертифікації й заявникові. Експертизу результатів випробувань, оформлення, реєстрацію й видачу сертифіката й ліцензії на право використання знака відповідності. На підставі висновку іспитової лабораторії орган сертифікації робить висновок і відправляє його в орган по сертифікації. Після присвоєння

сертифікату реєстраційного номера, його одержує заявник. Термін дії сертифіката – 3 роки.

3. Здійснення державного контролю й нагляду, інспекційного контролю над дотриманням правил обов'язкової сертифікації й за сертифікованими засобами захисту інформації. За результатами контролю Державний орган по сертифікації може призупинити або анулювати сертифікат у наступних випадках:

- зміни на законодавчому рівні, що стосуються вимог до засобів захисту інформації, методам випробувань і контролю;
- зміна технології виготовлення, конструкції (складу), комплектності засобів захисту інформації й системи контролю їх якості;
- невиконання вимог технології виготовлення, контролю й випробувань засобів захисту інформації;
- невідповідність сертифікованих засобів захисту інформації технічним умовам або формуляру, виявлене в ході державного або інспекційного контролю;
- відмова заявника в допуску (прийманні) осіб, уповноважених здійснювати державний контроль і нагляд, інспекційний контроль над дотриманням правил сертифікації й за сертифікованими засобами захисту інформації.

4. Інформування про результати сертифікації засобів захисту інформації;

5. Розгляд апеляцій. Апеляція подається в орган по сертифікації й розглядається в місячний термін за участю незалежних експертів і зацікавлених сторін.

Органи по сертифікації й іспитові лабораторії відповідають за виконання своїх функцій, забезпечення схоронності інформації обмеженого доступу, матеріальних цінностей, наданих заявником, а також за дотримання авторських прав розроблювача при випробуваннях його засобів захисту інформації.

Під сертифікацією засобів захисту інформації розуміється діяльність по підтвердженню відповідності цих засобів вимогам державних стандартів або інших нормативних документів по захисту інформації.

До засобів захисту інформації відносяться технічні, криптографічні, програмні й інші засоби, призначені для захисту відомостей, що становлять державну таємницю, засоби, у яких вони реалізовані, а також засобу контролю ефективності захисту інформації. Обов'язкової сертифікації підлягають засобу, у тому числі іноземного виробництва, призначені для захисту інформації, що становить державну таємницю, і іншої інформації з обмеженим доступом, а також засоби, використовувані в керуванні екологічно небезпечними об'єктами.

Атестаційні випробування припускають проведення наступних перевірок:

- перевірка стану технологічного процесу автоматизованої обробки персональних даних в ІСПД;
- перевірка ІСПД на відповідність організаційно-технічним вимогам по захисту інформації;
- випробування ІСПД на відповідність вимогам по захисту інформації від несанкціонованого доступу.

Результатом атестації є:

- Протокол атестаційних випробувань;
- Висновок за результатами атестаційних випробувань;
- Атестат відповідності на ІСПД (видається у випадку позитивного висновку);
- Акт про передачу СЗПД у промислову експлуатацію (у випадку наявності позитивного висновку за результатами атестаційних випробувань ІСПД).

Організаційну структуру системи сертифікації утворюють:

- центральний орган системи сертифікації (очолює систему сертифікації однорідних засобів захисту інформації);
- державний орган по сертифікації засобів захисту інформації;
- органи по сертифікації засобів захисту інформації (проводять сертифікацію засобів захисту інформації);
- іспитові лабораторії (проводять сертифікаційні випробування засобів захисту інформації);

- заявники (розроблювачі, виготовлювачі, постачальники, споживачі засобів захисту інформації).

Відповідно до Положення про порядок здійснення криптографічного захисту інформації в Україні, затвердженим Указом Президента України від 22.05.98 № 505/98, Департамент спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України (далі по тексту ДСТСЗІ) є державним органом України, який організовує всі роботи, пов'язані із сертифікацією засобів КЗІ на відповідність вимогам до забезпечення безпеки інформації.

Орган по сертифікації засобів КЗІ (ОС КЗІ) створений у структурі ДСТСЗІ відповідно до спільного наказу Служби безпеки України й Комітету України з питань стандартизації, метрології й сертифікації від 24.09.99 №202/213. Відповідно до спільного наказу Служби безпеки України й Державного комітету стандартизації, метрології й сертифікації України від 6 грудня 2000 р. №247/695 змінене найменування ОС КЗІ на "Орган по сертифікації засобів захисту інформації ДСТСЗІ СБ України (далі по тексту ОС СЗІ)".

ОС СЗІ акредитований Національним агентством по акредитації України в Системі Укрсепро - атестат акредитації № UA 4.001. 112 від 27.12.02. Дійсний до 26.12.05 ОС СЗІ є незалежним від розроблювачів, виробників, постачальників і споживачів засобів КЗІ в області закріпленої за ним акредитації, що унеможливлює надання на його співробітників тиску, здатного вплинути на їхні висновки або результати робіт.

Область акредитації ОС СЗІ включає засоби криптографічного захисту інформації – криптографічні системи, апаратні, програмні, апаратно-програмні або інші засоби, призначені для реалізації КЗІ, у тому числі й використовувані для генерації, виготовлення й тестування криптографічних ключів.

Роботи із сертифікації проводяться на підставі договорів, ув'язнених ОС СЗІ з організаціями й підприємствами.

ОС СЗІ на договірній основі проводить:

- роботи із сертифікації засобів КЗІ;
- роботи з обстеження й атестації виробництва сертифікуємих засобів КЗІ;

- технічний нагляд за виробництвом сертифікованих засобів;
- визнання сертифікатів відповідності.

Вартість робіт визначається відповідно до Правил визначення вартості робіт із сертифікації продукції й послуг, затвердженими наказом Держстандарту України від 10.03.99 №100 і зареєстрованими в Міністерстві юстиції 31.03.99 за №194/3487.

Основні функції ОС СЗІ визначаються Положенням про Орган по сертифікації СЗІ.

Іспитові лабораторії (центри) засобів КЗІ в Системі Укрсепро виконують такі функції:

- з доручення органа по сертифікації засобів КЗІ проводять випробування продукції й відповідають за повноту випробувань і вірогідність результатів, готовлять і пред'являють в ОС СЗІ протоколи випробування;
- з доручення органа по сертифікації беруть участь у проведенні обстеження й атестації виробництва, технічного нагляду за виробництвом сертифікованих засобів КЗІ.

Сертифікаційні випробування засобів КЗІ проводяться іспитовими лабораторіями (МУЛ) на відповідність вимогам діючим в Україні стандартів і нормативних документів на засоби КЗІ по методиках, розроблених МУЛ і погодженим ДСТСЗІ СБ України.

Заявники:

- мають договори на проведення робіт із сертифікації продукції з органом по сертифікації СЗІ й іспитовими лабораторіями;
- здійснюють підготовку виробництва й вживають заходів по забезпеченню стабільності характеристик засобів КЗІ, які впливають на забезпечення вимог до безпеки інформації;
- негайно повідомляють в орган по сертифікації СЗІ про всі зміни в технології, конструкції (складі) засобів КЗІ, які можуть вплинути на характеристики сертифікованих засобів КЗІ й на їхню стабільність;

- здійснюють доробку сертифікованих засобів КЗІ при виявленні їх невідповідності вимогам нормативних документів.

Орган по сертифікації засобів захисту інформації Державного науково дослідного інституту спеціальному зв’язку й захисту інформації при Адміністрації Державної служби спеціальному зв’язку й захист інформації України уповноважен Госпотребстандартом України (наказ від 03 липня 2008 року № 208) на виконання робіт із сертифікації продукції й послуг у державній Системі сертифікації Укрсепро.

1.1. Ліцензування у сфері захисту інформації

Інститут ліцензування є одним із провідних інститутів у системі регулювання господарської діяльності, що набув важливого значення з набуттям статусу ринкової економіки в Україні.

Регламентується законом України «Про ліцензування певних видів господарської діяльності» Відомості Верховної Ради України (ВВР) 2000, 36с. та постановами Кабінету Міністрів України від 14.11.2000 №1698 "Про затвердження переліку органів ліцензування";

постанова Кабінету Міністрів України від 20.11.2000 №1719 "Про запровадження ліцензії єдиного зразка для певних видів господарської діяльності";

постанова Кабінету Міністрів України від 29.11.2000 №1755 " Про термін дії ліцензії на провадження певних видів господарської діяльності, розміри і порядок зарахування плати за її видачу";

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";

Ліцензійні умови провадження господарської діяльності, пов’язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту інформації. Затверджено спільним наказом Держпідприємництва та Департаментом СТСЗІ СБ України від 29.12.2000 р. №89/67. Зареєстровано в Міністерстві юстиції України 20.01.2001 р. №50/5241.

Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб. Затверджено наказом ДСТСЗІ СБ України від 23.02.2002 № 9 , зареєстровано в Міністерстві юстиції України 13.03.2001 за № 245/6533.

Ліцензуванням у сфері захисту інформації називається діяльність, яка полягає у передачі/отриманні прав на проведення різних робіт у галузі захисту інформації.

Ліцензія – дозвіл на право проведення робіт у галузі безпеки та захисту інформації. Ліцензія видається на певні види діяльності та дійсна протягом 3 років, після закінчення яких здійснюється її перевірка у порядку, встановленому для видачі ліцензії.

Ліцензія видається в тому випадку, коли підприємство/організація або компанія, що подала заявку на отримання ліцензії, має всі необхідні умови для ліцензування. Зокрема, необхідно мати виробничу та експериментальну базу, нормативну та методичну документацію, мати науково та інженерно-технічних співробітників[7].

Безсумнівно, ліцензія є важливим засобом управлінського впливу, «окремі права й обов'язки з'являються у громадян лише у зв'язку з наявністю ненормативного акта, яким є акт – дозвіл». Необхідність істотного розширення інституту ліцензування багатьох видів діяльності в Україні, була обумовлена змінами в характері впливу держави на суспільні відносини, що складаються в сфері економіки.

Основним законодавчим актом, який регулює ліцензування в Україні є Закон України «Про ліцензування певних видів господарської діяльності» від 1 червня 2000 року. Цей Закон визначає види господарської діяльності, що підлягають ліцензуванню, порядок їх ліцензування, встановлює державний контроль у сфері ліцензування, відповідальність суб'єктів господарювання та органів ліцензування за порушення законодавства у сфері ліцензування.

Відповідно до статті 1 даного Закону ліцензування – це видача, переоформлення та анулювання ліцензій, видача дублікатів ліцензій, ведення ліцензійних справ та ліцензійних реєстрів, контроль за додержанням ліцензіатами ліцензійних умов, видача розпоряджень про усунення порушень ліцензійних умов, а також розпоряджень про усунення порушень законодавства у сфері ліцензування.

Основні поняття ліцензування містить також Господарський кодекс України. Відповідно до ч. 3 ст. 14 ліцензія – це документ державного зразка, який засвідчує право суб'єкта господарювання – ліцензіата на провадження зазначеного в ньому виду господарської діяльності протягом визначеного строку за умови виконання ліцензійних умов. Поняття ліцензування не є однозначним, у зв'язку з цим можна виділити такі його особливості: ліцензійна діяльність відноситься до системадержавно – виконавчих відносин, змістом яких є організація діяльності громадян і юридичних осіб у тих сферах діяльності, де потрібне неухильне виконання параметрів і визначеної правової поведінки.

Ліцензійна діяльність має свої принципи організації управлінського впливу, до яких належать:

1. Обмеження державного втручання в діяльність соціальних інститутів.
2. Демонополізація професійної діяльності, зацікавленість громадян у виконанні адміністративних умов ліцензійної діяльності
3. Координація держави і громадян при реалізації програм управління
4. Спеціалізація управлінського впливу
5. Професійна компетентність.

Ліцензування виступає формою контролю за набуттям спеціального правового статусу, фактичним виконанням обов'язкових ліцензійних умов, припиненням діяльності як суб'єкта ліцензійних правовідносин, а також формою контролю за правомірністю використання обмежених ресурсів; ліцензування – це особливий адміністративно – правовий режим «порядок регулювання, який виражений у комплексі правових засобів, що характеризують особливий зв'язок взаємодіючих між собою дозволів, заборон, позитивних зобов'язань, що створюють особливу спрямованість правового регулювання», що у даному випадку пов'язано з одержанням суб'єктом спеціального правового статусу, у структурі якого переважають обов'язки, визначені органами виконавчої влади, які добровільно виконуються суб'єктом ліцензування; норми, що регулюють систему ліцензування, охоплюють однорідні, тісно пов'язані відносини в межах однієї галузі, тобто складають

самостійний адміністративно - правовий інститут; імперативні розпорядження і заборони для ліцензійних видів діяльності, встановлені не в приватному порядку і не «заради здійснення інтересів особи, якій адресована правова норма, а заради чужого інтересу», тобто в публічних цілях; за порушення ліцензійних умов ліцензіат несе особливу адміністративну відповідальність, аж до анулювання ліцензії; названі змістовні ознаки знаходяться в діалектичній єдності з їх юридичною формою, і ліцензія з юридичного боку являє собою юридичний документ органу державного управління, що підтверджує право на здійснення визначених видів діяльності з дотриманням законодавства України і ліцензійних умов, що не суперечать чинному законодавству. Інститут ліцензування є комплексним, оскільки містить у собі норми адміністративного і цивільного права, де наявність ліцензії є підставою для виникнення правоздатності і майнових відносин при здійсненні окремих видів діяльності.

Суб'єктами відносин, що виникають у зв'язку з ліцензуванням, є, з одного боку, суб'єкт господарювання, а з іншого боку – орган ліцензування.

Суб'єкт господарювання – зареєстрована в установленому законодавством порядку юридична особа незалежно від її організаційно-правової форми та форми власності, яка провадить господарську діяльність, крім органів державної влади та органів місцевого самоврядування, а також фізична особа – суб'єкт підприємницької діяльності. Орган ліцензування орган виконавчої влади, визначений Кабінетом Міністрів України, або спеціально уповноважений виконавчий орган рад для ліцензування певних видів господарської діяльності. Суб'єкт господарювання, що має намір провадити певний вид господарської діяльності, що ліцензується, особисто або через уповноважений ним орган чи особу звертається до відповідного органу ліцензування із заявою встановленого зразка про видачу ліцензії. Орган ліцензування приймає рішення про видачу ліцензії або про відмову її видачі

Термін не пізніше ніж десять робочих днів дати надходження заяви про видачу ліцензії та документів, що додаються до заяви, якщо спеціальним законом, що регулює відносини певних сферах господарської діяльності, не передбачений інший Термін видачі ліцензії на окремі види діяльності.

Орган ліцензування: забезпечує виконання законодавства сфері ліцензування; затверджує спільно із спеціально уповноваженим органом питань ліцензування ліцензійні умови провадження певного виду господарської діяльності і та порядок контролю за їх додержанням, крім випадків, передбачених цим Законом; видає та переоформлює ліцензії, видає дублікати ліцензій на певний вид господарської діяльності, приймає рішення про визнання ліцензій недійсними; здійснює в межах своєї компетенції контроль за додержанням ліцензіатами ліцензійних умов; видає розпорядження про усунення порушень ліцензійних умов; анулює ліцензії на певний вид господарської діяльності; формує веде ліцензійний реєстр.

Орган ліцензування, яким центральний орган виконавчої влади, що здійснює передбачені цією статтею повноваження, може делегувати їх своїм структурним територіальним підрозділам.

Повноваження органу ліцензування не можуть бути делеговані іншим особам, в тому числі створеним органом ліцензування. Орган ліцензування не може доручати іншим особам визначати спроможність суб'єктів господарювання виконувати ліцензійні умови згідно поданими документами. Фінансування органу ліцензування здійснюється за рахунок коштів Державного бюджету України або місцевого бюджету. Відповідно до ст. Закону ліцензійні умови є нормативно-правовим актом, положення якого встановлюють кваліфікаційні, організаційні технологічні та інші вимоги для провадження певного виду господарської діяльності.

Суб'єкт господарювання зобов'язаний провадити певний вид господарської діяльності, що підлягає ліцензуванню, відповідно до встановлених для цього виду діяльності ліцензійних умов. Ліцензійні умови щодо видів господарської діяльності, для провадження яких необхідні спеціальні знання включаються кваліфікаційні вимоги до працівників суб'єктів господарювання юридичних осіб та (або) до фізичних осіб суб'єктів підприємницької діяльності.

В разі якщо для провадження певних видів господарської діяльності, що підлягають ліцензуванню, необхідні особливі вимоги щодо будівель,

приміщень, обладнання, інших технічних засобів, такі вимоги включаються до ліцензійних умов.

Ліцензійні умови та порядок контролю за їх додержанням затверджуються спільним наказом спеціально уповноваженого органу з питань ліцензування та органу ліцензування.

Ліцензійні умови та зміни до ліцензійних умов підлягають оприлюдненню порядку, встановленому законодавством, і набирають чинності через десять днів дати державної реєстрації нормативно-правового акта, якщо ньому непередбачений пізніший Термін набрання чинності.

1.2. Методи та засоби захисту інформації

Можна виділити основні засоби створення СЗІ [8]:

1. Системний підхід до побудови системи захисту інформації, такий підхід включає оптимальне поєднання програмних, апаратних, фізичних та інших засобів захисту.
2. Принцип сталого розвитку системи. Цей принцип є одним із основних в організації системи захисту інформації. Способи злому конфіденційної інформаціїї постійно розвиються захищеності інформаційної системи може бути статичним. Динамічний процес, який полягає в аналізі та реалізації найбільш раціональних методів, способів та шляхів перетворення системи захисту.
3. Поділ і зведення повноважень щодо доступу до інформації, що захищається, до мінімуму.
4. Повний контроль та реєстрація спроб НДД. Необхідність ідентифікації та аутентифікації кожного користувача та контролю його дій з подальшим відзначенням фактів здійснення різних дій у спеціалізованих журналах. Також обмеження щодо здійснення будь-якої дії в інформаційній системі без його попередньої реєстрації.
5. Забезпечення надійності системи захисту, тобто неможливість зниження рівня надійності у разі виникнення в системі збоїв, відмов, навмисних дій зломщика або ненавмисних помилок користувачів.
6. Контроль за коректною роботою системи.
7. Забезпечення економічного обґрунтування використання системи. Це виявляється у тому, що можливі збитки від несанкціонованого доступу до конфіденційної інформації під час реалізації загроз значно перевищують вартість розробки та експлуатації СЗІ [9].

Підсумовуючи, можна сказати, що побудова СЗІ досить тривалий і трудомісткий процес. Необхідно враховувати безліч аспектів розробки та реалізації системи.

Так само не варто забувати і про засоби захисту конфіденційної інформації, що використовуються. Вони мають бути обов'язково сертифіковані та розроблені лише органами, що мають ліцензію на даний вид діяльності.

На Рис.1 представлена схема взаємодії компонентів СЗІ. Можна зробити висновок, що така система завжди перебуває у динамічному стані.

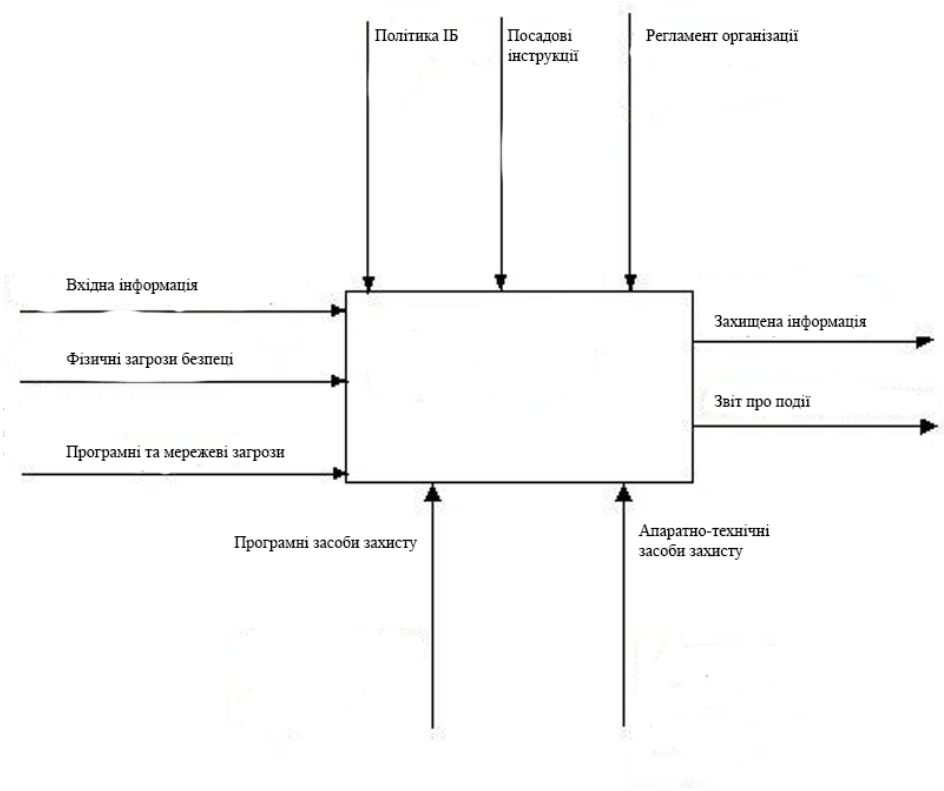

Рис. 1.1 Схема організації СЗІ

Аудит стану інформаційної безпеки на підприємстві являє собою експертне обстеження основних аспектів інформаційної безпеки, їх перевірку на відповідність певним вимогам. У деяких випадках під аудитом інформаційної безпеки мається на увазі перевірка захищеності окремих елементів інформаційної інфраструктури підприємства (сегментів його мережі, окремих серверів, баз даних, Інтернет-сайтів і т.п.) і надійності засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень і т. п.).

Однак ми надалі виходимо з того, що аудит інформаційної безпеки є комплексним (по можливості, вичерпним) дослідженням всіх аспектів

інформаційної безпеки (як технічних, так і організаційних) в контексті всієї господарської діяльності підприємства з урахуванням діючої політики інформаційної безпеки, об'єктивних потреб підприємства і вимог, що пред'являються третіми особами (державою, контрагентами тощо).

Розрізняють два основних види аудиту: внутрішній (що проводиться винятково силами співробітників підприємства) і зовнішній (здійснюваний сторонніми організаціями).

Цілями аудиту можуть бути:

- встановлення ступеня захищеності інформаційних ресурсів підприємства, виявлення недоліків і визначення напрямів подальшого розвитку системи захисту інформації;
- перевірка керівництвом підприємства та іншими зацікавленими особами досягнення поставлених цілей у сфері інформаційної безпеки, виконання вимог політики безпеки;
- контроль ефективності вкладень в придбання засобів захисту інформації та реалізацію заходів щодо забезпечення інформаційної безпеки;
- сертифікація на відповідність загальновизнаним нормам і вимогам у сфері інформаційної безпеки (зокрема, на відповідність національним та міжнародним стандартам).

Одним із стратегічних завдань, що вирішуються при проведенні аудиту інформаційної безпеки та отриманні відповідного сертифіката, є демонстрація надійності підприємства, його здатності виступати в якості сталого партнера, здатного забезпечити комплексний захист інформаційних ресурсів, що може бути особливо важливо при здійсненні операцій, що передбачають обмін конфіденційною інформацією, що має велику вартість.

У тому випадку, якщо аудит є внутрішнім, групу аудиторів необхідно сформувати з числа таких фахівців, які самі не є розробниками і адміністраторами використовуваних інформаційних систем і засобів захисту інформації та не мали відношення до їх впровадження на даному підприємстві.

Як правило, підприємство може вдаватися до допомоги зовнішніх аудиторів з метою:

- підвищення об’єктивності, незалежності та професійного рівня перевірки;
- отримання висновків про стан інформаційної безпеки та відповідності міжнародним стандартам від незалежних аудиторів.

Компанії, що спеціалізуються на проведенні аудитів, можуть здійснювати перевірки стану інформаційної безпеки на відповідність таким загальновизнаним стандартам і вимогам, як:

- ISO 15408: Common Criteria for Information Technology Security Evaluation (Загальні критерії оцінки безпеки інформаційних технологій);
- ISO 17799 (BS 7799): Code of Practice for Information Security Management (Практичні правила управління інформаційною безпекою);
- BSI \ IT: Baseline Protection Manual (Керівництво базового рівня щодо захисту інформаційних технологій Агентства інформаційної безпеки Німеччини);
- COBIT: Control Objectives for Information and related Technology (Основні цілі для інформаційних і пов’язаних з ними технологій);

Вимогам Керівних документів СБУ, системи СЕПТО чи інших державних органів та інших документів (таких як SAC, COSO, SAS 55/78).

При цьому організація, що здійснює зовнішній аудит, повинна відповідати певним вимогам:

- мати право (ліцензію) на видачу висновків про відповідність певним вимогам (наприклад, акредитацію UKAS - United Kingdom Accreditation Service);
- співробітники повинні мати право доступу до інформації, що становить державну таємницю (якщо така інформація є на підприємстві, що перевіряється);
- володіти необхідними програмними та апаратними засобами для вичерпної перевірки наявної у підприємства програмного і апаратного забезпечення.

Основними етапами проведення аудиту є:

- ініціювання проведення аудиту;
- безпосередньо здійснення збору інформації та проведення обстеження аудиторами;
- аналіз зібраних даних і вироблення рекомендацій;
- підготовка аудиторського звіту та атестаційного висновку.

Аудит повинен бути ініційований керівництвом підприємства з досить чітко сформульованої метою на певному етапі розвитку інформаційної системи або системи забезпечення інформаційної безпеки підприємства (наприклад, після завершення одного з етапів впровадження). У разі якщо аудит не є комплексним, на початковому етапі необхідно визначити його безпосередні кордони:

- перелік обстежуваних інформаційних ресурсів та інформаційних систем (підсистем);
- перелік будівель, приміщень і територій, в межах яких проводитиметься аудит;
- основні загрози, засоби захисту від яких необхідно піддати аудиту;
- елементи системи забезпечення інформаційної безпеки, які необхідно включити в процес перевірки (організаційне, правове, програмно-технічне, апаратне забезпечення);

Основна стадія - проведення аудиторського обстеження та збір інформації - як правило, має включати в себе:

- аналіз наявної політики інформаційної безпеки та іншої організаційної документації;
- проведення нарад, опитувань, довірчих бесід і інтерв’ю з співробітниками підприємства;
- перевірку стану фізичної безпеки інформаційної інфраструктури підприємства;
- технічне обстеження інформаційних систем - програмних і апаратних засобів (інструментальна перевірка захищеності).

Перш ніж приступити власне до аудиту інформаційної безпеки, аудиторам (зокрема, якщо проводиться зовнішній аудит) необхідно ознайомитися зі структурою підприємства, його функціями, завданнями та основними бізнес-процесами, а також з наявними інформаційними системами (їх складом, функціональністю, процедурами використання та роллю на підприємстві). На початковому етапі аудитори приймають рішення про те, наскільки глибоко і детально будуть досліджені окремі елементи інформаційної системи та системи захисту інформації. Також необхідно заздалегідь скоординувати з користувачами інформаційних систем процедури перевірки та тестування, що вимагають обмеження доступу користувачів (такі процедури по можливості повинні проводитися в неробочий час або в періоди найменшого завантаження інформаційної системи).

Якісний аналіз діючої на підприємстві політики безпеки є відправною точкою для проведення аудиту. Одне з перших завдань комплексного аудиту - встановлення того, якою мірою діюча політика відповідає об’єктивним потребам даного підприємства в безпеці, чи можуть дії в рамках даної політики забезпечити необхідний рівень захищеності інформації і засобів її обробки, зберігання та передачі. Це, в свою чергу, може вимагати проведення додаткової оцінки значущості основних інформаційних активів підприємства, їх уразливості, а також існуючих ризиків і загроз.

Аналіз політики також може включати оцінку таких її характеристик, як:

- повнота і глибина охоплення всіх питань, а також відповідність змісту політик нижнього рівня цілям і завданням, встановленим в політиках верхнього рівня;
- зрозумілість тексту політики для людей, які не є технічними фахівцями, а також чіткість формулювань і неможливість їх подвійного тлумачення;
- актуальність всіх положень і вимог політики, своєчасність обліку всіх змін, що відбуваються в інформаційних системах і бізнес-процесах.

Після перевірки основних положень політики безпеки в процесі аудиту можуть бути вивчені (перевірені) діючі класифікації інформаційних ресурсів

за ступенем критичності та конфіденційності, а також інші документи, що мають відношення до забезпечення інформаційної безпеки:

- організаційні документи підрозділів підприємства (положення про відділи, посадові інструкції);
- інструкції (положення, методики), що стосуються окремих бізнес-процесів підприємстві;
- кадрова документація, зобов'язання про нерозголошення відомостей, дані співробітниками, свідоцтва про проходження навчання, професійної сертифікації, атестації та ознайомленні з діючими правилами;
- технічна документація і призначені для користувача інструкції для різних використовуваних програмних і апаратних засобів (як розроблених самим підприємством, так і придбаних у сторонніх постачальників): міжмережевих екранів, маршрутизаторів, операційних систем, антивірусних засобів, систем управління підприємством і т.п.

Основна робота аудиторів у процесі збору інформації полягає у вивченні фактично застосованих заходів щодо забезпечення захисту інформаційних активів підприємства, таких як:

- організація процесу навчання користувачів прийомам і правилам безпечного використання інформаційних систем;
- організація роботи адміністраторів інформаційних і телекомунікаційних систем і систем захисту інформації (правильність використання програмних і апаратних засобів адміністрування, своєчасність створення і видалення облікових записів користувачів, а також налаштування їх прав в інформаційних системах, своєчасність заміни паролів і забезпечення їх відповідності вимогам безпеки, здійснення резервного копіювання даних, ведення протоколів усіх вироблених у процесі адміністрування операцій, вжиття заходів при виявленні несправностей і т.п.);
- організація процесів підвищення кваліфікації адміністраторів інформаційних систем і систем захисту інформації;
- забезпечення відповідності необхідних (у відповідності з політикою безпеки і посадовими обов'язками) прав користувачів інформаційних систем і

фактично наявних;

- організація призначення і використання спеціальних прав в інформаційних системах підприємства;
- організація робіт і координації дій при виявленні порушень інформаційної безпеки та відновленні роботи інформаційних систем після збоїв і нападів (практичне виконання "аварійного плану");
- заходи, що вживаються антивірусного захисту (належне використання антивірусних програм, облік всіх випадків зараження, організація
- роботи з усунення наслідків заражень і т.п.);
- забезпечення безпеки придбаних програмних і апаратних засобів (наявність сертифікатів та гарантійних зобов'язань, підтримка з боку постачальника при усуненні виявлених недоліків і т.п.);
- забезпечення безпеки самостійно розроблюваного програмного забезпечення (наявність необхідних вимог у проектній документації інформаційних систем, якість програмної реалізації механізмів захисту тощо);
- організація робіт з встановлення та оновлення програмного забезпечення, а також контролю за цілісністю встановленого ПЗ;
- заходи, що вживаються щодо забезпечення обліку і схоронності носіїв інформації (дисків, дискет, магнітних стрічок і т.п.), а також з їх безпечного знищення після закінчення використання;
- ефективність організації взаємодії співробітників підприємства - користувачів інформаційних систем - із службою інформаційної безпеки (зокрема, з питань реагування на інциденти та усунення їх наслідків).

1.3. ВИСНОВКИ

Підсумовуючи, можна сказати, що для побудови якісної СЗІ, яка задовольняла б усім законодавчим актам, необхідно використання тільки сертифікованих засобів захисту інформації. Також необхідний детальний аналіз об'єкта інформаційної безпеки для виявлення всіх вразливих місць компанії або організації.

2. РОЗРОБКА СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ БЮРО КРЕДИТНИХ ІСТОРІЙ

2.1. Організаційна структура

Бюро кредитних історій - юридична особа, яка реєструється відповідно до законодавства

Одним із головних завдань є прийом, обробка та зберігання інформації, яку надають кредитні організації. При цьому необхідно забезпечити передачу інформації захищеними каналами..

Об'єктами захисту відповідно до політики безпеки є:

1. Конфіденційна інформація, у тому числі інформація, що містить відомості, що становлять комерційну таємницю та персональні дані.
2. Склад відомостей конфіденційного характеру, зміст яких визначено у документі «Перелік відомостей конфіденційного характеру, що обробляються в організації», який затверджує генеральний директор.
3. Інформаційні ресурси АС різного рівня доступу, що містять конфіденційну інформацію.
4. Параметри конфігурації засобів захисту інформації АС.

Технічні заходи забезпечення безпеки інформації, що обробляється з використанням АС, реалізовані в комплексній системі захисту, даної АС і є застосування таких підсистем безпеки:

1. Захист від несанкціонованого доступу.
2. Захист мережного периметра системи (периметр, на якому знаходиться АС).
3. Захист інформації при її прийомі та передачі.
4. Захисту від шкідливих програмно-математичних впливів (вплив на інформацію, що захищається за допомогою шкідливих програм).
5. Контролює захищеність мережевої структури системи (телефонні лінії, ЛОМ тощо).

У підсистемах захисту від НСД, захисту мережевого периметра, прийому, передачі та контролю захищеності використані сертифіковані за вимогами безпеки інформації засоби захисту інформації та засоби електронного підпису.

У підсистемі захисту від шкідливих програмно-математичних впливів використано засоби антивірусного захисту з регулярно оновлюваними базами вірусних сигнатур.

Механізм розмежування доступу користувачів до інформаційних ресурсів системи реалізує призначення та надання прав доступу відповідно до документа «Матриця доступу суб'єктів до ресурсів АС», затвердженого керівником Товариства. Користувач, який намагається отримати доступ до заданого ресурсу, виконує процедуру ідентифікації та аутентифікації.

Також можна виділити чотири основні критерії, що пред'являються до безпеки автоматизованих систем:

1. D – мінімальний захист (Системи, безпека яких була оцінена, але виявилася такою, що не задовольняє вимогам більш високих розділів).
2. C – дискреційний захист;

2.1. C1 – дискреційне забезпечення секретності (поділ користувачів та даних; дискреційне управління доступом, що припускає примусове обмеження доступу на індивідуальній основі).

2.2. C2 – управління доступом (більш чітко оформлене дискреційне управління доступом; індивідуальні облікові записи, вхід під якими можливий через процедуру авторизації; журнал контролю доступу до системи; ізоляція ресурсів).

3. B – мандатний захист;

3.1. B1 – захист із застосуванням мета-безпеки (мандатне управління доступом до вибраних суб'єктів та об'єктів; маркування даних).

3.2. B2 – структурований захист (чітко визначена та документована модель правил безпеки; застосування розширеного дискреційного та мандатного управління доступом до всіх об'єктів та суб'єктів; приховані канали зберігання).

3.3. B3 – домени безпеки (відповідність вимогам монітора звернень; структурування для виключення коду, що не відповідає вимогам обов'язкової політики безпеки; підтримка адміністратора системи безпеки; прикладом такої системи є XTS-300, попередниця XTS-400).

4. A – перевірений захист;

4.1. A1 – перевірений дизайн (за функціями ідентично B3; формалізований дизайн та перевірені техніки, що включають високорівневу специфікацію; формалізовані процедури управління та розповсюдження; прикладом такої системи є SCOMP, попередниця XTS-400).

Незважаючи на класифікацію, широкий спектр ЗЗК та методів реалізації, буквально всі структурно-функціональні елементи АС є вразливими.

В даний час найбільш значущими нормативними документами, що визначають критерії оцінки ІБ та вимоги до її реалізації, є «Загальні критерії оцінки безпеки інформаційних технологій» (Code of practice for Information security management/ISO 17799).

2.2. Аналіз посадових обов'язків співробітників

До складу персоналу, що експлуатує АС, керівником товариства призначаються співробітники, кваліфікація та ступінь благонадійності (довіри) яких дозволяє безпечно експлуатувати автоматизовану систему. Співробітники, що призначаються до складу персоналу, виконують дії з управління системою відповідно до рольової моделі та експлуатаційної документації.

Рольова модель включає необхідність виконання персоналом АС наступних ролей: «Адміністратора АС», «Оператора АС» та адміністратора безпеки.

Суб'єктами доступу до АС є:

1. Співробітники, які мають право самостійного доступу до технічних засобів АС та виконують функціональні обов'язки в обсязі дій, передбачених ролями:

1.1. «Адміністратор АС».

1.2. «Оператор АС».

2. Джерела та користувачі кредитних історій, що формуються з використанням АС.

Роль «Адміністратора АС» передбачає виконання дій щодо конфігурування та настроювання засобів операційної системи на серверний компонент і компонент управління АС, управління засобами захисту і покладає на виконавця ролі відповідальність за безпечну і безперебійну роботу АС.

Роль «Оператора АС» передбачає виконання дій щодо управління процедурами отримання, зберігання та надання даних кредитних історій використанням АС, щодо взаємодії джерел та користувачів кредитних історій з АС.

Дані, що містять інформацію, що захищається, оброблювану АС, розміщуються в наступних основних ресурсах АС:

1. Таблиці реляційної бази даних (СУБД PostgreSQL Server 9.0):

1.1. Кредитні історії (credit_history).

1.2. Чорнові кредитні історії (draft_credit_history).

1.3. Кредитні звіти (Report).

1.4. Платежі (payment).

1.5. Запити отримання кредитного звіту (request).

1.6. Чорнові запити на отримання кредитного звіту(Draft_request).

1.7. Користувачі (users).

2. Xml-вивантаження з реляційної бази даних АС для відправлення титульних частин кредитних історій та запитів.
3. Реквізити доступу до ресурсів АС.
4. Ключі електронного підпису, які використовуються в АС.
5. Дані системних журналів та підсистеми логування.
6. Резервні копії бази даних.

Перелік даних і ресурсів АС, а також відповідні їм права доступу суб'єктів АС (матриця доступу) представлений нижче (табл. 2.1 – Перелік даних і ресурсів АС УБКІ, що захищаються, права суб'єктів доступу до АС УБКІ).

Перелік даних та ресурсів АС, права суб'єктів доступу до АС

Інформаційні дані	**Найменування ресурсу**	**Адміністратор АС**	**Оператор АС**	**Джерело кредитних історій**	**Користувач кредитних історій**
1	**2**	**3**	**4**	**5**	**6**
Інформація таблиць реляційної бази даних					
Таблиця credit_history	Кредитні історії	Читання, зміна	Читання	Створіння, читання	Немає доступу
Таблиця draft_credit_his -tory	Чорнові кредитні історії	Читання, зміна	Читання	Створення, читання, зміна	Немає доступу

Таблиця report	Кредитні звіти	Створення, читання, зміна	Створіння, читання	Немає доступу	Читання
Таблиця payment	Платежі	Читання, зміна	Читання	Створіння, читання	Немає доступу
Таблиця request	Запити на отримання кредитного звіту	Читання, зміна	Читання	Немає доступу	Створення, читання

Таблиця draft_request	Чорнові запити	Читання, зміна	Читання	Немає доступу	Створення, читання, зміна
Таблиця users	Дані користувачеві АС	Створення, читання, зміна	Читання	Немає доступу	Немає доступу
Інші ресурси, що захищаються					
Реквізити доступу	Реквізити доступу до ресурсів АС	Створення, читання, зміна	Читання власних реквізитів	Читання власних реквізитів	Читання власних реквізитів
Ключі електронного підпису	Ключі електронного підпису, використовуємо в АС	Створення, читання, зміна	Читання	Немає доступу	Немає доступу
Дані системних журналів та підсистеми логуванняя	Дані системних журналів та підсистеми логуванняя	Читання	Немає доступу	Немає доступу	Немає доступу

xml-вивантаження	Титульні частини	Створеня, читання	Читання	Немає доступу	Немає доступу
Резервні копії бази даних	Резервні копії на жорсткому диску сервера АС, оптичних носіях інформації	Створеня, читання	Читання	Немає доступу	Немає доступу

Табл. 2.1. Перелік даних та ресурсів АС

Таким чином, в АС передбачено розмежування доступу суб'єктів та об'єктів доступу до конфіденційної інформації. Це дозволяє обмежити доступ до інформаційної бази АС та відстежити можливі факти НДД.

До складу експлуатаційної документації входять технологічні інструкції персоналу, який виконує зазначені ролі, технічна документація виробника технічних засобів, включаючи засоби захисту інформації, документи, що регламентують надання послуг споживачам.

В даний час в організації доступ до АС здійснюється лише за допомогою логіну та паролю, чого не достатньо. Це може призвести до того, що, використовуючи відповідні програми, можна підібрати логін та пароль. У деяких випадках, якщо пароль встановлюється безпосередньо співробітником, пароль можна підібрати, виходячи із загальних знань про людину. Більш надійним варіантом аутентифікації є електронний замок, який має бути у кожного працівника. Що має доступ до АС.

Також не проводиться шифрування інформації в основі бюро. Для повнішої організації захисту необхідно шифрувати дані ключем, відомим лише певної категорії співробітників.

2.3. Аналіз моделі загроз інформаційного характеру

Однією з основних завдань розробки системи захисту є побудова моделі загроз.

Основними групами загроз, на протистояння яким спрямовані цілі та вимоги безпеки, є:

1. Загрози, пов'язані із здійсненням несанкціонованого доступу (ознайомлення) з інформацією, що містить відомості про кредитні історії, при її обробці та зберіганні.
2. Загрози, пов'язані з несанкціонованим копіюванням (розкраданням) інформації, що містить відомості про кредитні історії (у тому числі БД кредитних історій загалом).
3. Загрози, пов'язані із здійсненням доступу до інформації, що містить відомості про кредитні історії, без дозволу на те її власника (суб'єкта кредитної історії).
4. Загрози, пов'язані з порушенням доступності інформації, що містить відомості про кредитні історії, що передається заінтересованим особам.
5. Загрози, пов'язані з перехопленням інформації, що містить відомості про кредитні історії, з каналів передачі з використанням спеціалізованих програмно-технічних засобів.
6. Загрози, пов'язані з втратою (втратою) інформації, що містить відомості про кредитні історії, внаслідок збоїв (відмов) програмного та апаратного забезпечення.
7. Загрози, пов'язані з порушенням узгодженості даних, що приймаються від джерел кредитних історій, що розміщуються в БД кредитних історій, а також розміщуються в додаткову частину кредитної історії (у разі оновлення кредитної історії).
8. Загрози, пов'язані з запереченням фактів надсилання запитів на отримання кредитних історій та фактів отримання кредитних звітів.
9. Загрози, пов'язані з використанням комп'ютерних вірусів та іншого шкідливого програмного забезпечення.

10. Загрози, пов'язані із здійсненням несанкціонованих інформаційних впливів (спрямованих на «відмову в обслуговуванні») для сервісів, модифікацію конфігураційних даних (програмно- апаратних засобів, підбір автентифікаційної інформації тощо).

Модель загроз є обов'язковим пунктом у побудові системи захисту інформації. Даний захід необхідний виявлення слабких місць АС, ефективної постановки завдання.

З перерахованого вище списку загроз можна зробити висновок, що основними напрямками розробки системи захисту інформації будуть захист від НСД при прийомі, передачі та зберіганні конфіденційної інформації.

У додатку 1 наведено приклад моделі загроз для офісних приміщень.

2.4. Аналіз організаційних заходів щодо забезпечення безпеки інформації

Співробітниками товариства підписується зобов'язання встановленої форми про нерозголошення отриманих під час виконання службових (посадових) обов'язків та включених до документа «Перелік відомостей конфіденційного характеру, оброблюваних у створенні» відомостей.

Для місць розміщення технічних засобів (приміщень) АС визначаються межі контрольованої зони, вільний доступ до якої для сторонніх осіб заборонено.

Доступ обслуговуючого персоналу до приміщення, де розташовані технічні засоби АС, допускається лише в присутності осіб, відповідальних за безпеку інформації при її обробці в АС.

Вхідні двері технічних приміщень розміщення обладнання АС забезпечуються засобами (замками та іншими пристроями), що перешкоджають неконтрольованому самостійному фізичному доступу сторонніх осіб.

Рис. 2.1 Фізичні засоби захисту Компанії Інфотек

Сторонніми особами вважаються працівники товариства, яким не надано право самостійного доступу до технічних засобів АС, а також особи, які не є працівниками Товариства.

У товаристві встановлюється режим проходу територію (приміщення) офісу, включаючи службові приміщення. При цьому унеможливлюється знаходження сторонніх осіб на території приміщень товариства без контролю з боку відповідальних співробітників. Режим пропуску до службових приміщень визначається керівником товариства.

Виключається можливість візуального (у тому числі з використанням оптичних засобів спостереження) перегляду інформації обмеженого доступу із пристроїв візуалізації інформації (відеодисплейних терміналів та пристроїв виведення на друк).

Рис. 2.2 Камери спостереження Компанії Інфотек

Вхідні двері приміщень, де розміщені засоби АС, на час відсутності в них відповідального персоналу, що обслуговує АС, зачиняються на замок, опечатуються та здаються під охорону.

Корпуси апаратних засобів, що входять до складу АС (сервер, АРМ, мережеве обладнання), забезпечуються засобами контролю розтину (опечатуються).

Зберігання документів, що містять конфіденційну інформацію, а також зберігання ключових носіїв із закритими ключами електронного підпису, проводиться в спеціальних сховищах (шафах) сейфового типу. Відповідальність за збереження носіїв та документів покладається керівником Товариства на працівників у персональному порядку.

Щодо співробітників, призначених на виконання обов'язків адміністратора та оператора АС, здійснюються суворі відбірково-кадрові заходи, що виключають можливість появи серед них зловмисників.

2.5. Аналіз використовуваних засобів захисту конфіденційної інформації

Апаратно-програмний комплекс захисту конфіденційною інформації включає наступні засоби:

1. Електронний замок

Ідентифікація та аутентифікація; контроль цілісності; апаратний ДСЧ; реєстрація спроб доступу; довірене завантаження.

2. СКЗІ Secret Disk Server NG.

Забезпечує захист від несанкціонованого доступу до баз даних, корпоративної пошти та іншої інформації на дисках сервера; двофакторну аутентифікацію адміністраторів за допомогою електронних ключів; надання доступу до конфіденційних даних лише довіреним працівникам; розраховану на багато користувачів роботу із захищеними даними; екстрене блокування доступу до даних; можливість використання сертифікованих криптопровайдерів; надійний захист баз даних 1С; Microsoft Windows Server 2012 R2.

3. Ключовий носій.

Технічний засіб, призначений для коректної автентифікації, безпечного зберігання конфіденційних даних, виконання криптографічних обчислень та роботи з асиметричними ключами та цифровими сертифікатами.

4. Засіб створення моделі системи розмежування доступу

Забезпечує автоматичне сканування локальних логічних дисків, доступних папок мережі; автоматичне зчитування встановлених прав доступу до файлової системи NTFS (для АРМ під управлінням ОС сімейства Windows NT); побудова за результатами сканування дерева ресурсів, що відповідає структурі ресурсів АРМ та ЛОМ; автоматичне отримання списку локальних та доменних користувачів (для АРМ під управлінням ОС сімейства Windows NT); ручну реєстрацію в ПРД користувачів та встановлення їх рівнів доступу; встановлення прав доступу користувачів до об'єктів доступу, а також грифів

секретності об'єктів доступу; відображення всієї інформації, що міститься в ПРД, у зручній формі; створення звітів на основі інформації про суб'єктів та об'єкти доступу.

5. Засіб контролю захищеності.

Забезпечує відображення всієї інформації, що міститься в ПРД (можливий перегляд); порівняння структури ресурсів АРМ, описаної в ПРД, із реальною структурою ресурсів; створення звіту за результатами порівняння; побудова плану тестування об'єктів АРМ; перевірка реальних прав доступу користувачів до об'єктів доступу; створення звіту за результатами тестування.

6. Мережевий сканер.

Призначений для виявлення вразливостей встановленого програмного та апаратного забезпечення, що використовує протоколи стека TCP/IP.

7. Засіб фіксації та контролю вихідного стану програмного комплекса

Забезпечує фіксацію вихідного стану програмного комплексу; контроль вихідного стану програмного комплексу; фіксацію та контроль каталогів; контроль відмінностей у заданих файлах (каталогах); можливість роботи з довгими іменами файлів та іменами, що містять символи кирилиці.

8. Програма пошуку та гарантованого знищення інформації на дисках.

Забезпечує вибір диска для пошуку ключових слів; перегляд вмісту поточного диска; перегляд параметрів поточного диска; збереження фрагмента поточного диска файл; копіювання фрагмента поточного диска буфер обміну; друк поточного диска на принтері; збереження образу поточного диска файл; підключення образу диска, збереженого файл; формування списків ключових слів; вибір параметрів пошуку ключових слів; пошук ключових слів на диску; вибіркове гарантоване знищення знайдених ключових слів; формування звіту за результатами пошуку; пошук файлу, який містить знайдене ключове слово; перегляд журналу подій програми; перегляд параметрів ліцензії програми.

9. Антивірус.

10. Криптомаршрутизатор (VPN-з'єднання).

Таким чином, частина загроз, описаних у пункті 1.3, може бути усунена наявними ЗЗК. Але слід зазначити, що залишаються слабкі місця в системі, які не захищені жодними засобами. Завдання виконання даної роботи полягає в тому, щоб забезпечити надійним захистом усі моменти, описані в моделі загроз. Для цього необхідно розширити коло засобів захисту, що використовуються.

2.6. ТЕХНІЧНЕ ЗАВДАННЯ

1. Загальні відомості.

У цьому технічному завданні наведено опис, призначення та цілі створення, технічні вимоги до системи захисту інформації, у тому числі визначено вимоги до організаційного, інформаційного, програмного та технічного забезпечення, а також до робіт з впровадження вищезгаданої системи на підприємстві.

2. Призначення та цілі створення.

Система захисту інформації – комплекс організаційних і технічних заходів, спрямованих на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається.

Необхідно розробити систему захисту інформації для АС, що відповідає класу захищеності 1Г та класу К3 інформаційної системи для обробки персональних даних.

Система захисту інформації повинна забезпечувати такі основні можливості АС та розв'язання задач:

1. Ідентифікація та аутентифікація суб'єктів та об'єктів доступу.
2. Управління доступом суб'єктів та об'єктів доступу.
3. Реєстрація подій безпеки.
4. Антивірусний захист.
5. Виявлення (запобігання) вторгнень.
6. Контроль захищеності інформації.
7. Цілісність інформації.
8. Доступність інформації.
9. Захист технічних засобів.
10. Захист АС, її засобів, систем зв'язку та передачі даних.

3. Вимоги до продукту.

3.1. Функціональні вимоги СЗІ має забезпечувати:

1. Встановлення захищених каналів зв'язку для передачі прийому конфіденційної інформації.

2. Безпечне зберігання конфіденційної інформації в АС.
3. Санкціонований доступ до АС.
4. Моніторинг рівня безпеки АС (періодичне тестування функцій програмних засобів, їх періодичне оновлення та контроль працездатності).
5. Для сервера – резервне копіювання конфіденційної інформації; елементи системи повинні мати можливість динамічного резервування подій у випадку відмови каналів зв'язку.

3.2. Технічні вимоги.

Система захисту інформації має безперешкодно забезпечувати штатну роботу АС. Для цього необхідно дотримання таких функцій:

1. Безперебійність живлення.
2. Корекція при падіннях напруги та підвищеній напрузі.
3. Фільтрування та захист від стрибків напруги.
4. Забезпечення санкціонованого доступу в приміщення, що охороняється.

3.3. Вимоги до якості.

Система має бути побудована повністю за допомогою сертифікованих ліцензованих. Повинні бути дотримані основні функціональні вимоги до системи.

3.4. Склад та зміст робіт із створення.

Моделювання загроз АС при передачі, прийомі та зберіганні конфіденційної інформації. Тестування вже існуючої системи захисту інформації. Аналіз результатів тестування. Побудова моделі нової системи захисту на основі зібраних даних.

Необхідно:

1. Впровадити систему електронного документообігу.
2. Цифровий підпис прийому, передачі.
3. Шифрування конфіденційної інформації на базі АС. Для АРМ:

1. Застосувати індивідуальний електронний ключ для кожного співробітника, який має доступ до АС.

2. Впровадити технічні засоби захисту інформації від витоку каналами зв'язку.

3.5. Порядок контролю та впровадження системи

При здійсненні робіт із запровадження необхідно погодити нововстановлені обладнання та програми з раніше встановленими. Роботи мають бути виконані у суворій відповідності до проекту. Матеріали та обладнання повинні відповідати вказаним у проекті моделям та найменуванням приладів та програм.

3.6. Вимоги до документаційного забезпечення.

2.7. ВИСНОВКИ

У ході роботи було проведено аналіз роботи АС, моделі загроз даної системи, наявних засобів захисту інформації. ТЗ було складено на підставі зіставлення аналізу моделі загроз та наявних в організації засобів захисту. Було зроблено висновок, що є істотні недоліки в системі захисту, які можуть призвести до суттєвих збитків у разі виявлення.

На підставі цих даних у ТЗ завдання поставлені ті організаційні заходи, які необхідно виконати в першу чергу для безпечного функціонування АС БКІ.

3. РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

3.1. Організація електронного документообігу, ЦП та шифрування баз даних

В даний час існує два варіанти організації ЕДО:

1. Реалізація за допомогою сторонніх компаній.
2. Реалізація за допомогою власної ЕЦП.

Звичайно, перший варіант є більш зручним та економічним, тому що всі головні функції виконує стороння організація. Але, слід зазначити, що ці послуги спрямовані на реалізацію бухгалтерського ЕДО. Для передачі будь-яких інших документів таких засобів захисту буде недостатньо.

Якщо розглядати ЕДО лише у бухгалтерському середовищі, то таке рішення було б логічним: простота використання, універсальна сумісність із різними бухгалтерськими програмами. Але в нашому випадку необхідно розглянути варіант надсилання різних документів. Таким чином, варіант із залученням сторонньої організації ми розглядати не можемо.

Другий варіант є більш трудомістким, тому що необхідно придбати сертифікований криптографічний засіб, сертифікат ЦП і інтегрувати в АС.

Оскільки необхідно, щоб підписання документів відбувалося автоматично, потрібне програмне забезпечення, яке можна було б інтегрувати в АС. Також необхідна функція генерації ключів, формування ЦП та шифрування даних. Такий засіб можна буде застосувати і до шифрування даних у базі.

3.2. Впровадження індивідуального електронного ключа працівників, які мають доступ до АС

Електронний ключ – апаратний засіб, який призначений для захисту програмного забезпечення та конфіденційної інформації від несанкціонованого копіювання, нелегального використання та несанкціонованого розповсюдження.

Використання таких ключів дозволяє вдосконалити процеси ідентифікації та аутентифікації на локальних робочих комп'ютерах співробітників організації та корпоративної мережі компанії. Виробники пропонують два варіанти ключів: смарт-карти та usb- ключі. Для нашої системи буде зручніше використання саме usb-ключів, оскільки планується використання на робочих комп'ютерах.

Для авторизації на сервері вже використається ключовий носій eToken Pro 32k.

Характеристики eToken Pro:

Двофакторна аутентифікація – удосконалений вид захисту, при якій використовується пароль, при цьому користувач авторизується, надаючи як мінімум два засоби аутентифікації. Одним із цих засобів є token, наприклад, USB-ключ або смарт-карта eToken PRO (Java), а друге – персональний PIN-код користувача.

Як другий критерій ідентифікації користувача при використанні електронних USB-ключів та смарт-карт eToken PRO (Java) використовуються:

1. Цифрові сертифікати, що використовують національний стандарт X.509 (Public Key Infrastructure – інфраструктура відкритих ключів).
2. Паролі користувачів, коди доступу або інша інформація для здійснення аутентифікації, що зберігаються в захищеній пам'яті.

Робота з електронними ключами не становить особливої складності користувачів ПК будь-якого рівня. Принцип роботи з ключами полягає в наступному: ключ приєднується до певного інтерфейсу комп'ютера. Далі захищена програма через спеціальний драйвер надсилає йому інформацію, яка обробляється відповідно до алгоритму, заданого раніше, і повертається назад.

Якщо ключ надсилає правильну відповідь, програма продовжує свою роботу. В іншому випадку, програма може виконувати різні дії, які задані розробником. Наприклад, переключатися в демонстраційний режим, блокувати доступ до деяких функцій.

Таким чином, впровадження в роботу подібних ключів є необхідним заходом при побудові системи захисту інформації. Аутентифікації лише паролем часто буває недостатньо. Навіть пароль більш ніж 10 символів досить просто зламати, маючи доступ до робочого комп'ютера. Наявність електронного ключа значно ускладнює завдання зломщиків.

3.3. Впровадження технічних засобів захисту інформації від витоку каналами зв'язку

Як правило, у багатьох організаціях каналів витоку інформації по каналах практично не приділяється уваги. Багато керівників не вважають за потрібне витрачати на цей час і гроші. Однак, для досвідчених зломщиків не складе ніяких труднощів отримати всі необхідні дані, використовуючи, наприклад, телефонну мережу. Саме тому захист каналів зв'язку є одним із пріоритетних завдань при побудові системи захисту інформації.

3.3.1. Захист телефонних мереж

Велику небезпеку компанії представляє НСД зловмисників до програмним портам АТС через зовнішні канали зв'язку. Гарантію те, що в комутаційних станціях відсутні не декларовані можливості, може дати експертиза їх принципових схем та вихідних текстів програмного забезпечення, що проводиться лише за сертифікації виробів. Таким чином, без будь-яких додаткових заходів щодо організації захисту телефонних мереж ризик злому сильно зростає.

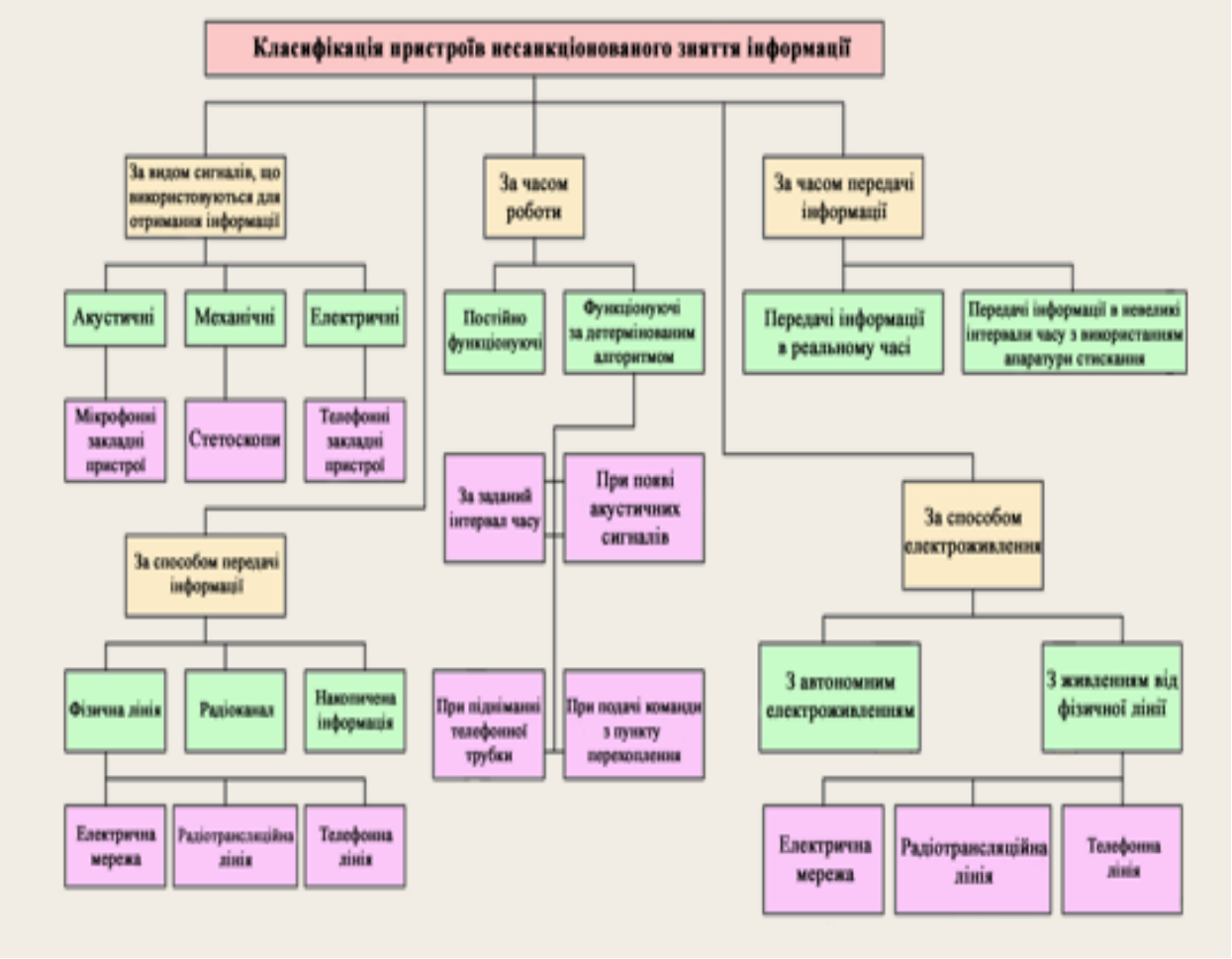

Рис. 3.1. Класифікация ЗП

Структурна схема типового закладного устрою представлена на рис. 2.4.

Рис 3.2. Структурна схема закладного устрою.

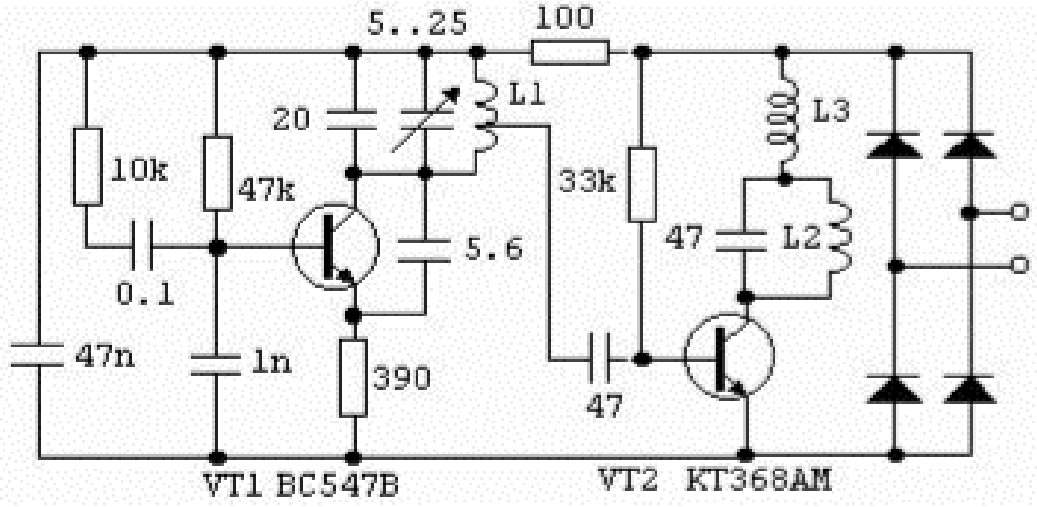

Рис 3.3. Схема електрична принципова телефонного ЗП

Основними технічними засобами забезпечення захисту від злому в телефонних мережах є міжстанційні екрани. Принцип роботи таких пристроїв: пристрій підключається до розриву цифрових ліній, які з'єднують АТС компанії та АТС загального користування, забезпечує постійний контроль усіх подій, що відбуваються в користувальницьких та службових каналах на фазах встановлення та розриву з'єднання, у стані розмови.

Також існують блокатори телефонів. Основною їх функцією є відстеження та запобігання спробам прослуховування через паралельну лінію.

Аналізатори телефонних ліній можна розділити на два види: індивідуальні та тестові комплекти. Індивідуальні сигналізатори слід

встановлювати заздалегідь перевірену лінію. Вони служать контролю параметрів телефонної пари. Як правило, подібні сигналізатори називають "телефонними сторожами". Такий страж зазвичай надається у вигляді розетки із двома світлодіодами: зелений означає лінія чиста, червоний означає Тривога! Параметри лінії змінилися. Безперечним плюсом таких індивідуальних сигналізаторів є простота експлуатації, мінусом – висока ймовірність помилкового спрацьовування. Тестові комплекти призначені саме для перевірки лінії фахівцями. Такий комплект посилає в лінію зондуючий сигнал і аналізує сигнал у відповідь, за яким визначає наявність в лінії будь-яких радіоелементів, властивих ланцюгам знімання та передачі інформації.

Рис 3.4. Цифровий аналізатор дротових і телефонних ліній TALAN версії 3.0

«Найкраща оборона – це напад» – таким принципом користуються пристрої активного захисту телефонних ліній. Зазвичай їх називають телефонними пригнічувачами. Такий пристрій здійснює зашумлення верхнього звукового діапазону, погіршуючи співвідношення сигнал/шум на вході пристроїв. Насправді виходить, що придушувач шуму створює дуже гучний звук, що практично неможливо.

Переваги аналізаторів, придушувачів та блокаторів гармонійно поєднують у собі універсальні пристрої захисту телефонних ліній. Вони працюють у двох режимах: виявлення та придушення. При будь-якому контактному підключенні до лінії прилад подасть сигнал тривоги, після чого можна включити режим придушення. Перешкода, що подається в лінію, діє на ділянці від приладу до АТС, тим самим наводячи всі засоби знімання в неробочий стан.

Клас пристроїв захисту інформації від витоку по телефонних лініях є найбільш прийнятним для забезпечення захисту телефонних переговорів.

Від системи оперативно-розшукових заходів частково може захистити клас таких пристроїв захисту телефонних переговорів, як скремблер. Телефонні скрімблери - це пристрої шифрації/дешифрації мовних переговорів. Оскільки будь-який код і шифр можна розкрити, то скремблер тільки знижує цінність розкритої розмови. Наприклад, ви розмовляли по телефону про будь-яку важливу зустріч, використовуючи пристрій, що скремблює. Розмова була перехоплена, але результати дешифрації були отримані лише через якийсь час після зустрічі. Таким чином, оперативну цінність інформації втрачено. Сам скремблер є чорною (сіру, білу) коробку, яку розміщують поруч із телефонним апаратом. Така сама коробка має бути у всіх абонентів, із якими необхідно засекретити переговори.

Рис 3.5. Телефоні скремблери

Останній клас приладів захисту телефонної лінії – це випалювачі засобів знімання. Працює такий засіб досить просто: на лінію подається малий струм високої напруги. Таким чином всі пристрої, що прослуховують, згорають. Придбання такого пристрою, як правило, не виправдовує себе. Це досить дорогий захід, який мають проводити кваліфіковані спеціалісти у цій галузі. Таким чином, з усіх засобів захисту та контролю телефонних мереж загального користування найбільш ефективними за критеріями захисту та експлуатації є універсальні пристрої захисту та скремблери.

3.4. Порядок робіт із впровадження

1. Цифровий підпис.

Для інтеграції Sun IdM та КриптоПро JCP:

Спочатку необхідно встановити IdM.

Потім на сервер слід поставити JCP відповідно до рекомендацій щодо встановлення ПО СКЗІ.

Налаштувати конфігурацію сервера документації. (Для встановлення: security.nonrepudiation.signedApprovals=true) .

Далі необхідно відкрити налагоджувальну сторінку Identity Manager (http://PathToIDM/debug). Завантажиться сторінка із системними налаштуваннями. У пункті «List Objects» необхідно вибрати з меню, що випадає "Configuration" і натиснути "List Objects", з'явиться сторінка "List Objects of type: Configuration". У пункті "System Configuration" необхідно вибрати "Edit", з'явиться файл, який містить системну конфігурацію. Його необхідно редагувати, встановивши "signedApprovals=true".

```
<Attribute name='nonrepudiation'>
<Object>
<Attribute name='signedApprovals'>
<Boolean>true</Boolean>
</Attribute>
</Object>
</Attribute>
```

Далі необхідно встановити сертифікати з інтерфейсу адміністратора. Для цього необхідно в пункті Адміністратор вибрати Конфігурація і вибрати Сертифікати.

Потім необхідно додати алгоритми JCP IdM.

У файлі samples_src.jar у каталозі SunIdM знаходяться дві модифіковані форми IdM: Approval Form.xml і Work Item Configuration.xml. Вони додані

параметри «supportedKeyStoreTypes» та «keytypeSignatureMapping» для полів типу «TransactionSigner».

<Property name='keytypeSignatureMapping' value='DSA=SHA1withDSA,RSA=SHA1withRSA,RSA=MD5withRSA,RSA=MD2withRSA,GOST3410=GOST3411withGOST3410EL'/>

<Propertyname='supportedKeyStoreTypes' value='JKS,PKCS12,HDImageStore'/>

Далі необхідно встановити в полі "supportedKeyStoreTypes" типи сховищ ключів, які будуть використані на клієнтській машині для підпису. Ці форми необхідно по черзі імпортувати у конфігурацію через web-інтерфейс (Configure -> Import Exchange File). Потім необхідно перезавантажити IdM.

Далі встановлення JCP на клієнті. Необхідно підготувати сховища та ключі, які будуть використовуватись для підпису. Вказівки «Obtain a certificate and private key, and then export them to a PKCS#12 keystore.» необхідно ігнорувати.

У СКЗІ JCP ключ зашифрування повідомлення збігається з ключом розшифрування (загальний закритий ключ зв'язку). При зашифруванні повідомлення користувача А для користувача Б загальний закритий ключ зв'язку виробляється на основі закритого ключа шифрування користувача А та відкритого ключа шифрування користувача Б. Відповідно, для розшифрування цього повідомлення користувачем Б формується загальний закритий ключ зв'язку на основі свого власного закритого ключа шифрування та відкритого ключа шифрування користувача А.

Таким чином, для забезпечення зв'язку з іншими абонентами кожному абоненту необхідно мати:

1. власний закритий ключ шифрування;
2. відкриті ключі шифрування (сертифікати відкритих ключів) інших користувачів.
2. Установка "eToken PRO (Java)".

Необхідно встановити набір драйверів eToken RTE (версії 3.66) або eToken PKI Client (версії 5.1). Підключати eToken до встановлення драйвера не потрібно.

3. Встановлення фільтра

Рекомендується розташовувати фільтр керуючись такими принципами: фільтр не повинен встановлюватися у приміщенні із слабкою циркуляцією повітря; прилад не повинен розташовуватися поблизу нагрівальних та опалювальних конструкцій.

Установка: фільтр закріплюється у горизонтальному або вертикальному положенні за допомогою кріплення для стін або підлоги. Важливо, щоб поверхня, на яку встановлюється фільтр, була міцною та могла витримувати вагу фільтра довгий час.

Рис. 3.6. Фільтр: проти перешкод; мережевий; 250ВАС; Cx: 0,47мкФ; Cy: 10нФ

Підключення фільтрів здійснюється у знеструмленому стані. Підключення до проводів, що проводять струм, має здійснюватись кваліфікованим персоналом, що має допуск до роботи на електроустановках до 1000 В, за допомогою кабельних з'єднувачів, що входять до складу мережевих фільтрів. Потрібно здійснювати підключення екранованим кабелем. Екрани вхідного та вихідного кабелів повинні бути з'єднані з муфтами, що екранують, кабельних з'єднувачів. Необхідно розпаювати, використовуючи тільки спиртові флюси. Вхід фільтра необхідно підключати до мережі змінного струму з напругою 220В та частотою 50Гц. Вихід фільтра необхідно підключити до навантаження. Перед початком використання фільтра необхідно зробити заземлення приладу. До клеми заземлення треба приєднати мідний дріт, протилежний кінець дроту підключити до болта для заземлення. Болт

заземлення необхідно розміщувати на шині заземлення. Потрібно організувати контактний майданчик для з'єднання із заземлюючим провідником навколо болта. Болт для заземлення і контактний майданчик повинні бути захищені від корозії або виготовлені з антикорозійного металу, так само не повинні мати поверхневого фарбування. Фільтр краще розташовувати поблизу або всередині щита. Вхід виробу необхідно приєднувати безпосередньо зі щита до мережі. З виходу приладу необхідно протягнути кабель із розетками, які будуть послідовно врізані. Протягнути його необхідно до СВТ або до інших електронних пристроїв.

3.5. Порядок внесення змін до керівних документів

1. Внесення змін до договірних відносин із суб'єктами/користувачами кредитних історій, що передбачають взаємодію між суб'єктами/користувачами за допомогою електронного документообігу.
2. Внесення змін до договірних відносин із суб'єктами/користувачами КІ щодо використання ЦП (НЕП) для забезпечення електронного документообігу.
3. Внести зміни до керівних документів організації, що зумовлюють дії в галузі захисту інформації АС у зв'язку з використанням ЦП та шифруванням баз даних АС.
4. Внести зміни до керівних документів організації, що зумовлюють зовнішні технічні засоби захисту інформації АС у зв'язку з використанням засобів захисту телефонних мереж та ЛОМ.
5. Надати план встановлення засобів захисту телефонних мереж.

3.6. **ВИСНОВОК**

Ця дипломна робота виконана з метою розробки системи захисту інформації для.

При виконанні цієї дипломної роботи було проведено аудит та аналіз наявних засобів захисту інформації. На підставі висновків даного аналізу було розроблено технічне завдання щодо організації системи захисту інформації. В результаті була представлена система захисту інформації, яка має такі властивості:

1. Шифрування баз даних для більш надійного зберігання конфіденційної інформації.
2. Використання цифрового підпису, для забезпечення цілісності та незмінності переданої/одержуваної інформації.
3. Використання цифрового підпису реалізації електронного документообігу, що значно спрощує взаємодію Космосу з партнерами.
4. Використання індивідуального електронного ключа для кожного співробітника для більш надійної процедури ідентифікації та аутентифікації об'єктів на робочих місцях.
5. Використання засобів, спрямованих проти знімання інформації за телефонними лініями.
6. Використання коштів, спрямованих проти несанкціонованого доступу до корпоративної мережі компанії.
7. Система захисту відповідає вимогам законодавчих актів та керівних документів, прийнятими в Україні.

Таким чином було виконано поставлене технічне завдання на розробку системи захисту інформації на підприємстві. Внесені зміни суттєво впливають на забезпечення безпеки. Були розроблені інструкції щодо впровадження ЕДО та ЦП. Так само був представлений план розміщення технічних засобів захисту

конфіденційної інформації у телефонних мережах. Звіт про виконану роботу подано у вигляді дипломної роботи.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Майкл Дж. Д. Саттон Корпоративний документообіг. Принципи, технології, методологія застосування. 2002. - 446 с.
2. Ахрамович В. М. (Akhramovych V. M.), Вдовиченко О. В. (Vdovychenko O. V.), Загиней А. Ю. (Zahyney A. Yu.). Метод розрахунку захисту персональних даних від довіри між користувачами та інтенсивності передавання даних у соціальних мережах. Зв'язок. К. ДУТ. - 2021.- №3.- с.27-34
3. Блінов А.М. Інформаційна безпека: Навчальний посібник. Частина 1.
8. Аверченко, В.І. Криптографічні методи захисту/В.І. Аверченко, М.Ю. Ритов, С.А. Шпичак, 2010. - 216 с.
9. Аверченко В.І. Організаційний захист інформації: навч. Посібник для вузів/В.І. Аверченко, М.Ю. Ритов. - 184 с.
10. Болдирєв, А.І. Методичні рекомендації щодо пошуку та нейтралізації засобів негласного знімання інформації: практ. Посібник / А. І. Болдирєв – М. 2001. - 137 с.
12. Велика енциклопедія промислового шпигунства / Ю.Ф. Каторін., Є.В.Куренков, А.В. Лисів. 2000. - 886 с.
13. Малюк, А.А. Введення на захист інформації в автоматизованих системах/А.А. Малюк, С.В. Пазізін, Н.С. Погожин. 2001. - 178 с.
14. Бєлкін, П.Ю. Програмно-апаратні засоби забезпечення інформаційної безпеки. Захист програм та даних: навч. посібник для вузів/П.Ю. Бєлкін, О.О. Михальський, А.С. Перваків. 2000. - 215 с.
15. Іванов, М.А. Криптографічні методи захисту в комп'ютерних системах і мережах: учеб.-справ/М.А., 2001. -365 с.
16. Галатенко В.О. Стандарти інформаційної безпеки: курс лекцій: навчальний посібник/В.А. Глатенко. 2006.-264 с.
17. Джонс К.Д., Шема М., Джонсон Б.С., Інструментальні засоби забезпечення безпеки / К.Д. Джонс, М. Шема, Б.С. Джонсон.-1028 с.
18. P. Mahalanobis, Proceedings of the National Institute of Science 12: 49–55.

ДОДАТОК

Експлікація приміщень			
Номер	Найменування	Площа	Категорія пожежо вибухобезпеки
1	Коридор	160 м2	Ні
2	Кабінет №1	17 м2	Ні
3	Кабінет №2	17 м2	Ні
4	Кабінет №3	34 м2	Ні
5	Кабінет №4	32 м2	Ні
6	Кабінет директора	38 м2	Ні
7	Кабінет секретаря	19 м2	Ні
8	Бухгалтерія	25 м2	Ні
9	Кабінет №5	25 м2	Ні
10	Кабтнет №6	25 м2	Ні
11	Переговорна	51 м2	В 4
12	Серверна	14 м2	В 4
13	Кабінет №7	29 м2	Ні
14	Кабінет №8	29 м2	Ні
15	Кабінет №9	29 м2	Ні

Таблиця 1.

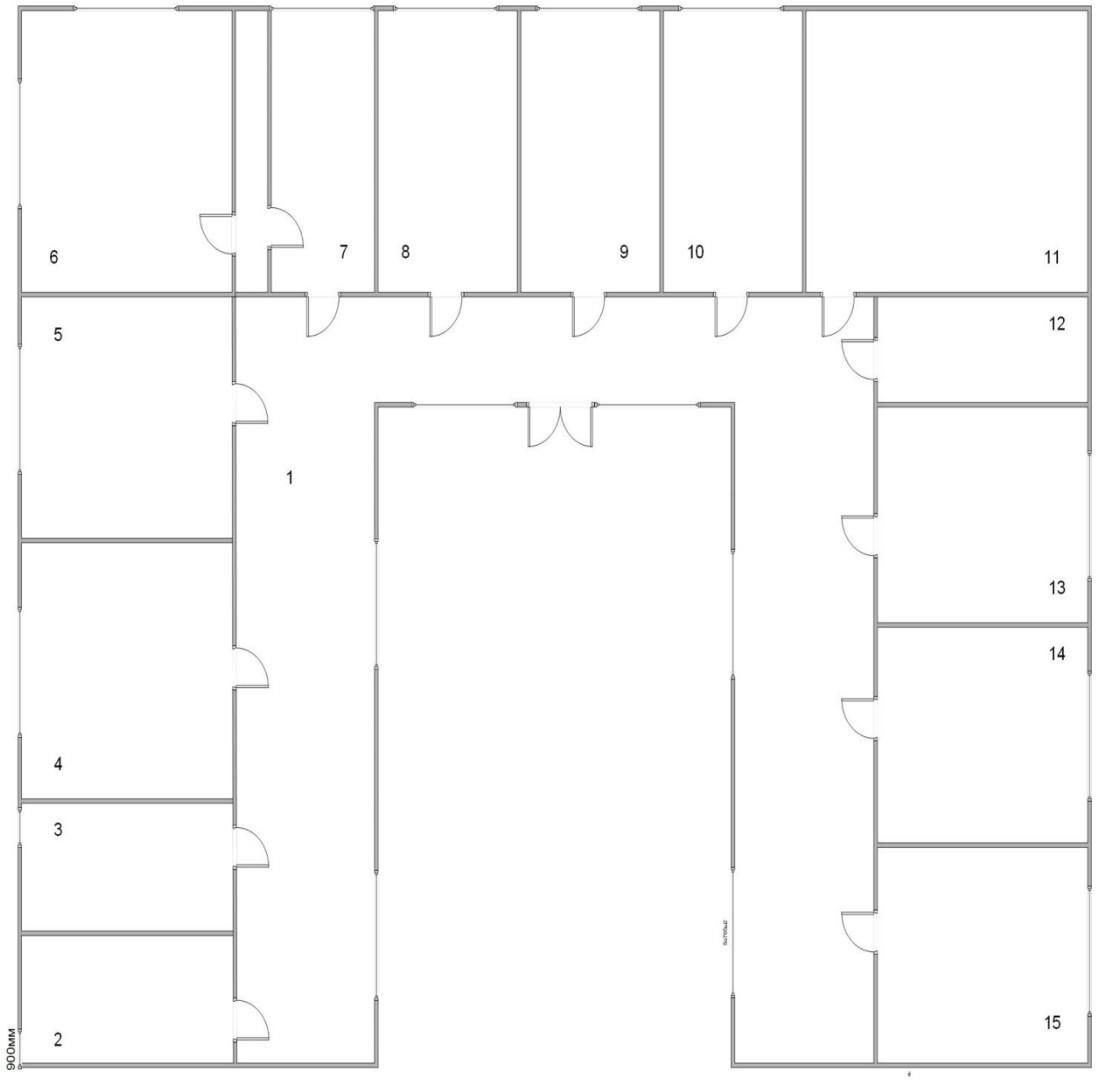

Рисунок 1. Загальна схема поверху

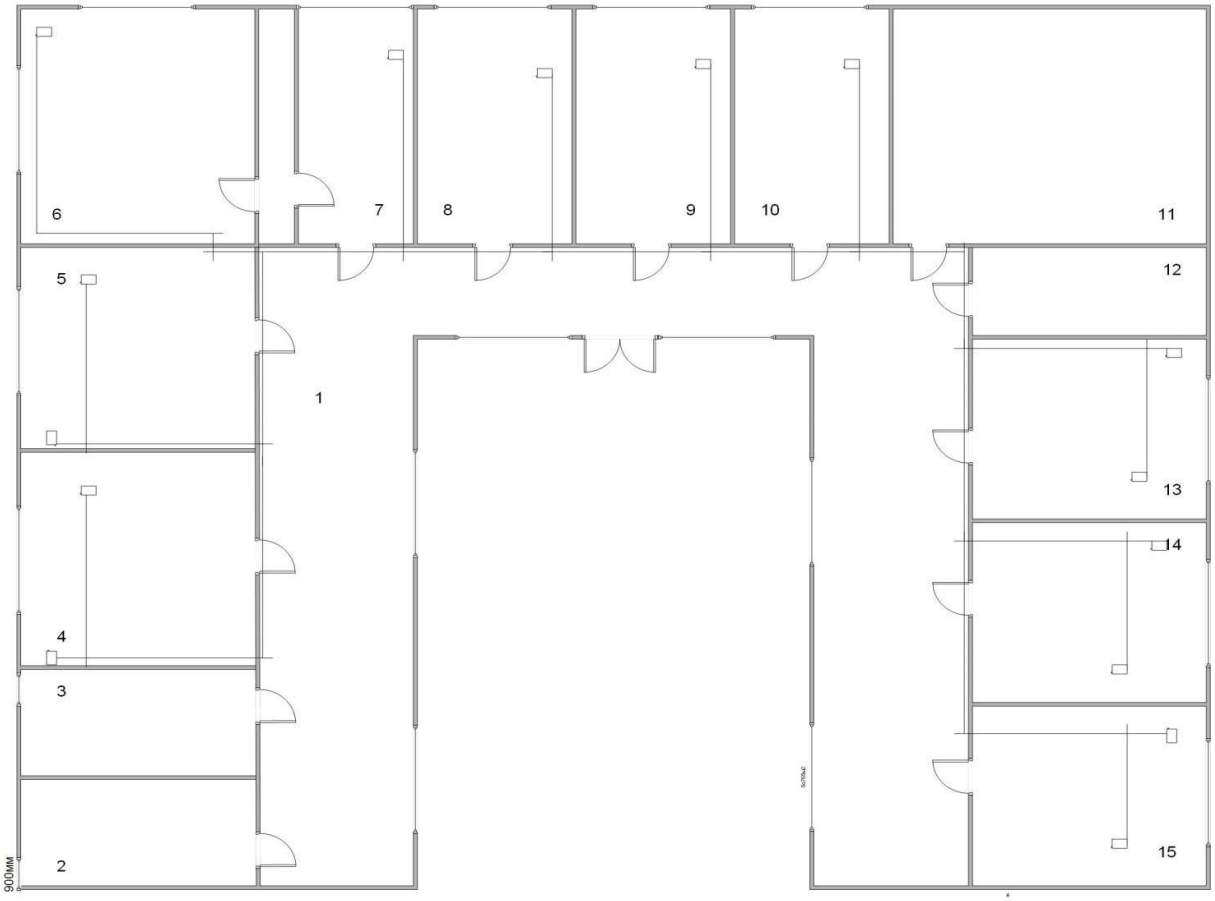

Рисунок 2. Комп’ютерна мережа

Приміщення	Кількість комп'ютерів, прим.
1	0
2	0
3	0
4	2
5	2
6	1
7	1
8	1
9	1
10	1
11	0
12	0
13	2
14	2
15	2

Таблиця 2.

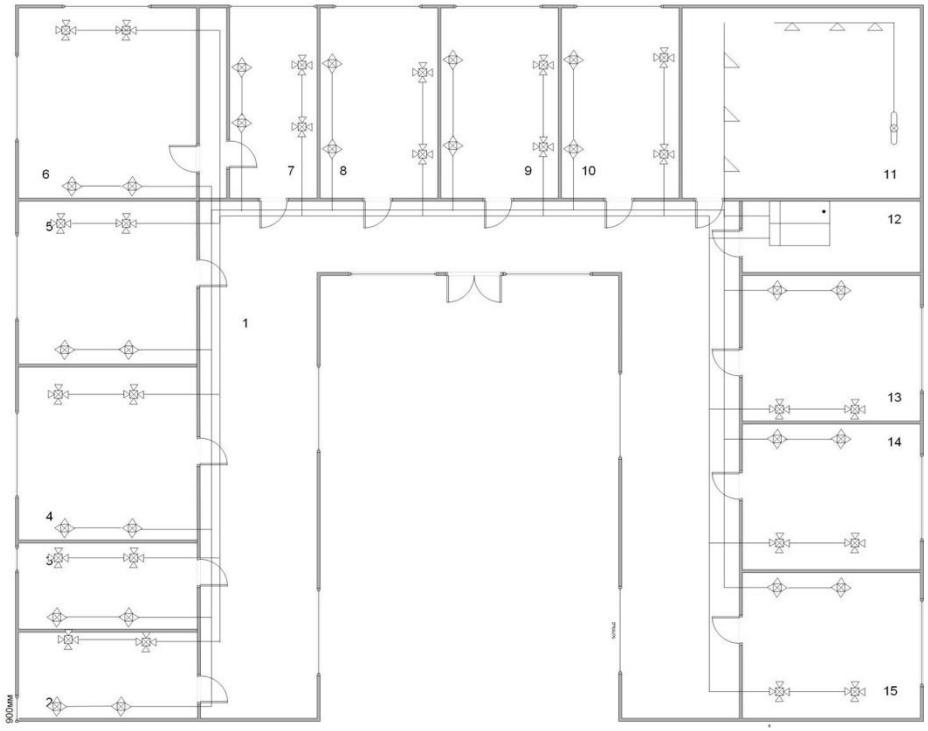

Рисунок 3. Вентиляція

Приміщення	Кількість об'єктів (вентиляція), прим.
1	0
2	4
3	4
4	4
5	4
6	4
7	4
8	4
9	4
10	4
11	6
12	1
13	4
14	4
15	4

Таблиця 3.

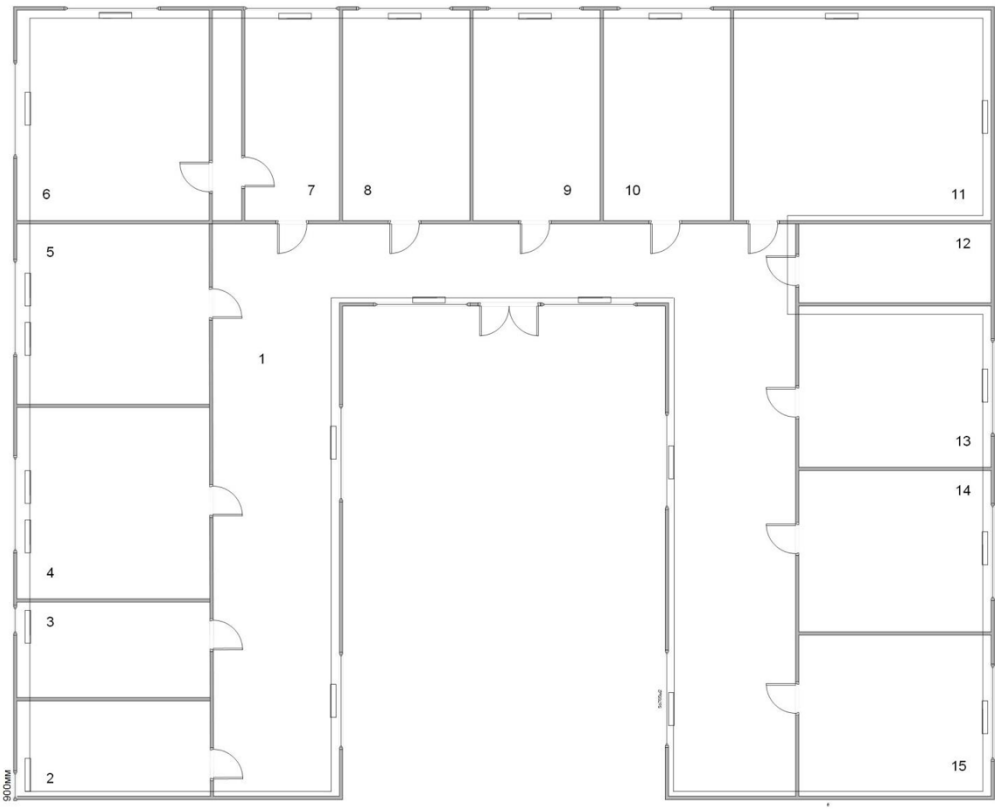

Рисунок 4. Опалення

Приміщення	Кількість батарей, шт.
1	6
2	1
3	1
4	2
5	2
6	2
7	1
8	1
9	1
10	1
11	2
12	0
13	1
14	1
15	1

Таблиця 4.

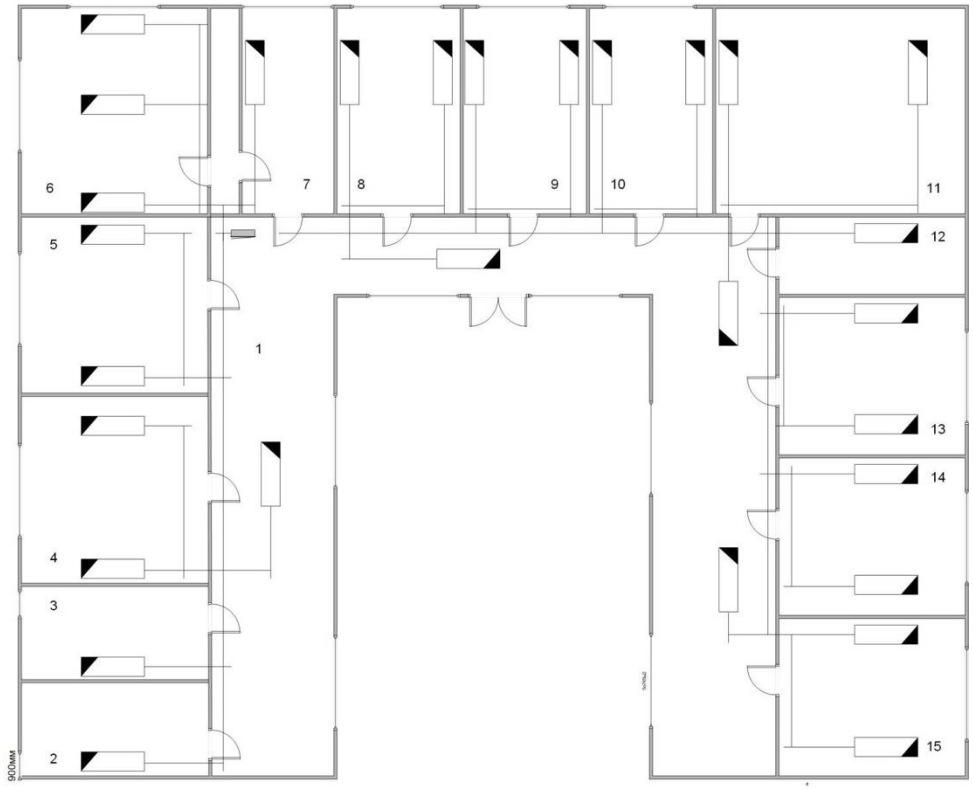

Рисунок 5. Освітлення

Приміщення	Кількість ламп, прим.
1	4
2	1
3	1
4	2
5	2
6	3
7	2
8	2
9	2
10	2
11	2
12	1
13	2
14	2
15	2

Таблиця 5.

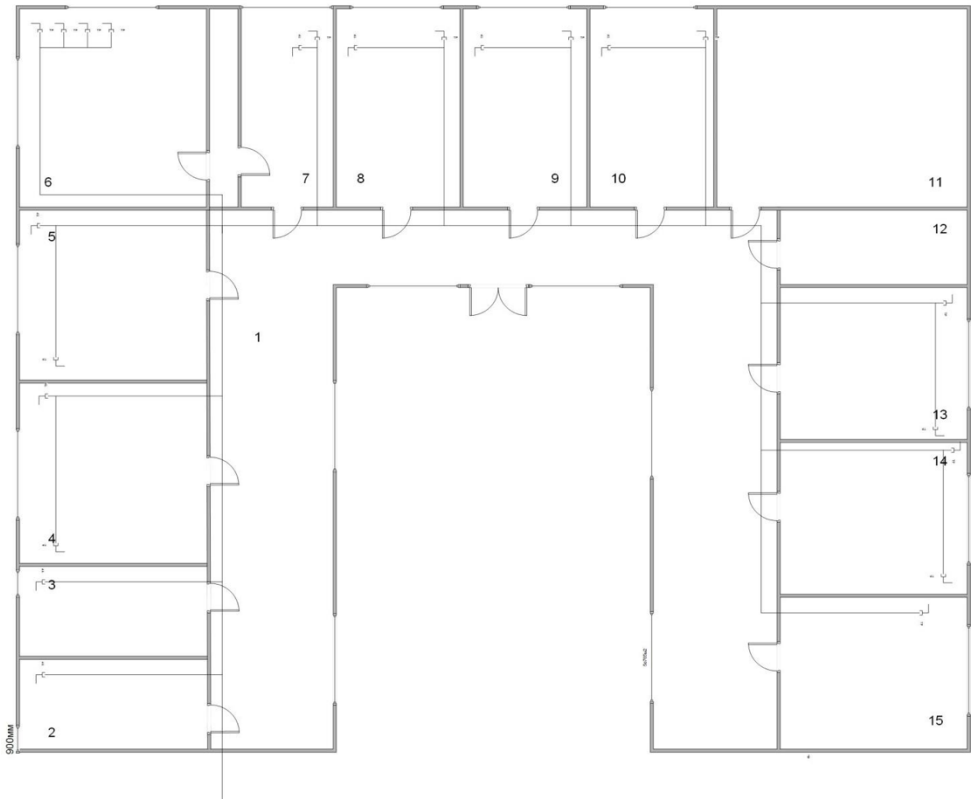

Рисунок 6. Телефонна мережа

Кількість ламп	Кількість телефонних розеток, прим.
4	0
1	1
1	1
2	2
5	2
6	4
7	2
8	2
9	2
10	2
11	0
12	0
13	2
14	2
15	1

Таблиця 6.

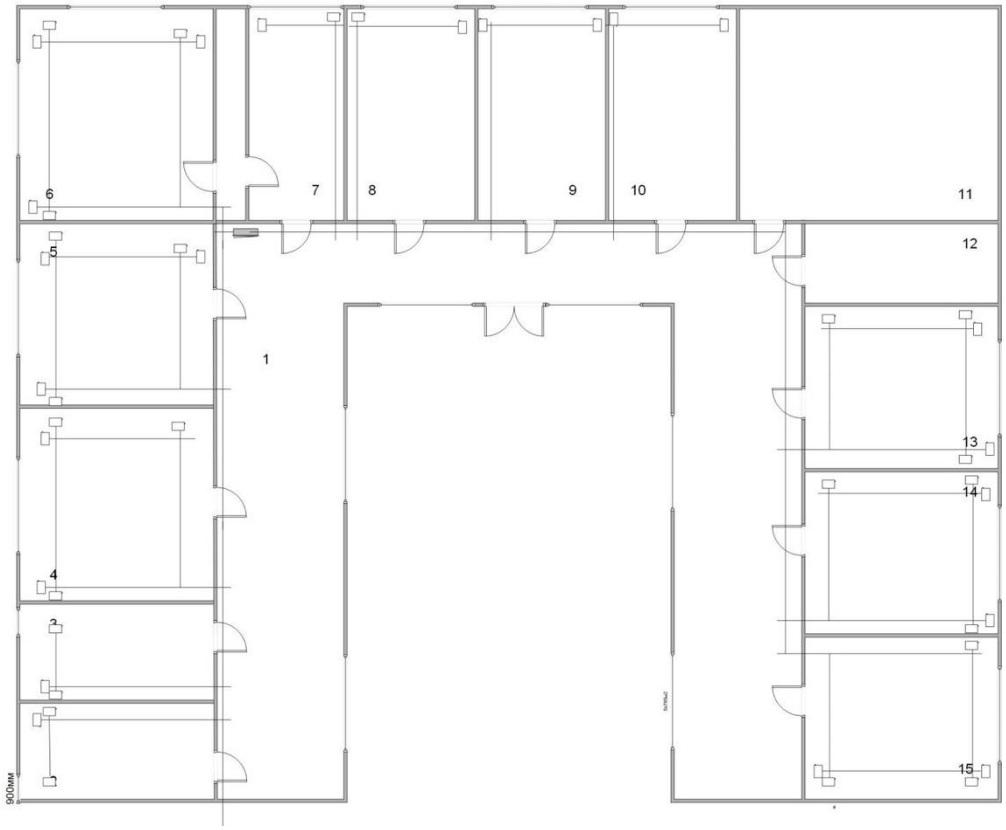

Рисунок 7. Електрика

Кількість ламп	Кількість розеток, прим.
4	Щиток
1	3
1	3
2	5
5	6
6	6
7	2
8	2
9	2
10	2
11	0
12	0
13	5
14	5

Таблиця 7.

Рисуні

Рисунок 8. Загрози

Тип загрози	Прилади
Високочастотне нав'язування	Телефонні апарати
Паразитна генерація	Комп'ютери, принтери, факси, сканери
Акустичний	Вентиляція, відчинені двері, вікно
Акустоелектричний	Телефонні апарати, електроживлення, заземлення
Канал витоку інформації ПЕМІН	Комп'ютери
Акустооптичний	Зачинене вікно
Віброакустичний	Захисні конструкції, трубопроводи
Інші канали витоку інформації	Мобільні телефони, диктофони, спец. технічні засоби

Таблиця 8.

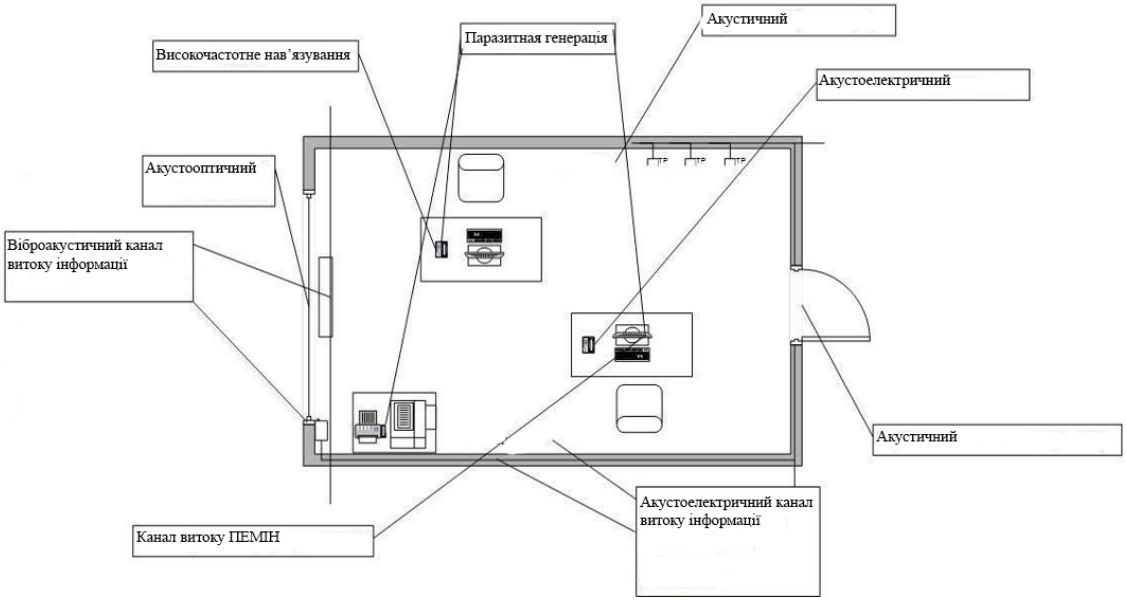

Рисунок 9. Бухгалтерія канали витоку інформації.

Тип загрози	Прилади
Високочастотне нав'язування	Телефонні апарати
Паразитна генерація	Комп'ютери, принтери, факси, сканери
Акустичний	Вентиляція, відчинені двері, вікно
Акустоелектричний	Телефонні апарати, електроживлення, заземлення
Канал витоку інформації ПЕМІН	Комп'ютери
Акустооптичний	Зачинене вікно
Віброакустичний	Захисні конструкції, трубопроводи
Інші канали витоку інформації	Мобільні телефони, диктофони, спец. технічні засоби

Таблиця 9.

Переговорна

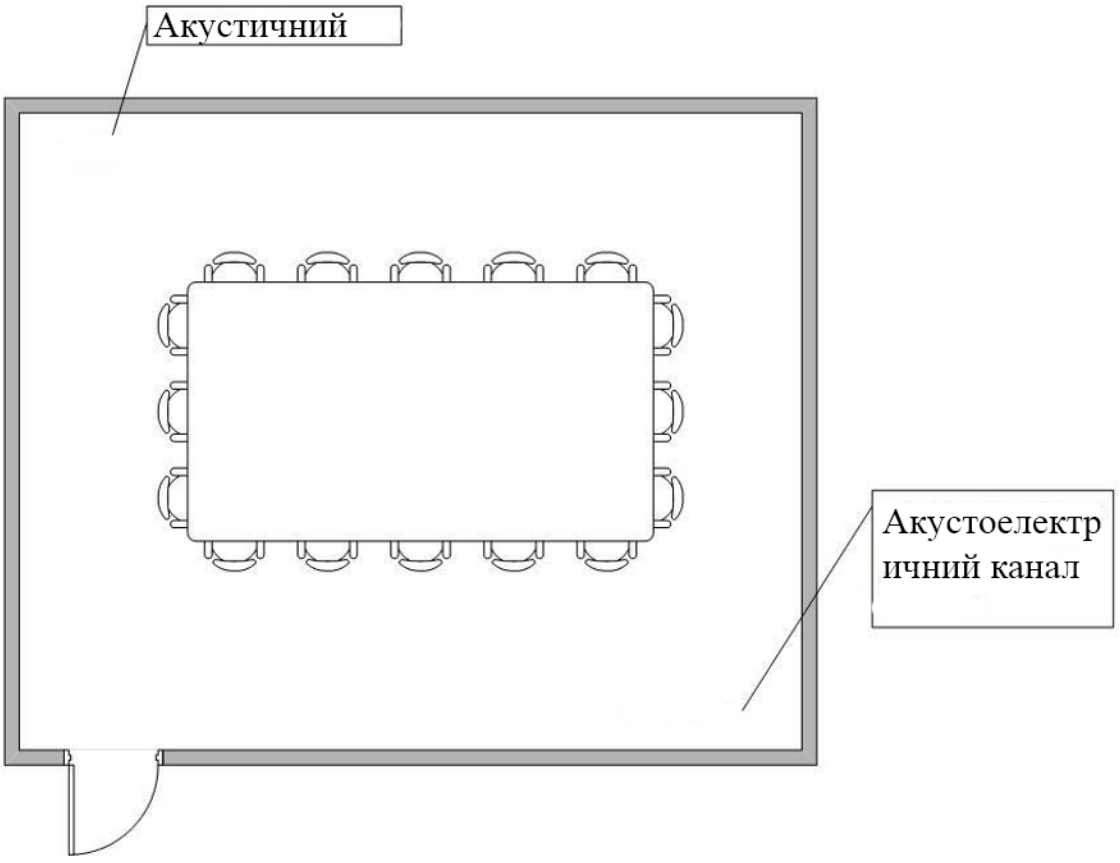

Рисунок 10. Переговорна канали витоку інформації.

Тип загрози	Прилади
Акустичний	Вентиляція, відчинені двері
Акустоелектричний	Електроживлення, заземлення, освітлення

Таблиця 10.

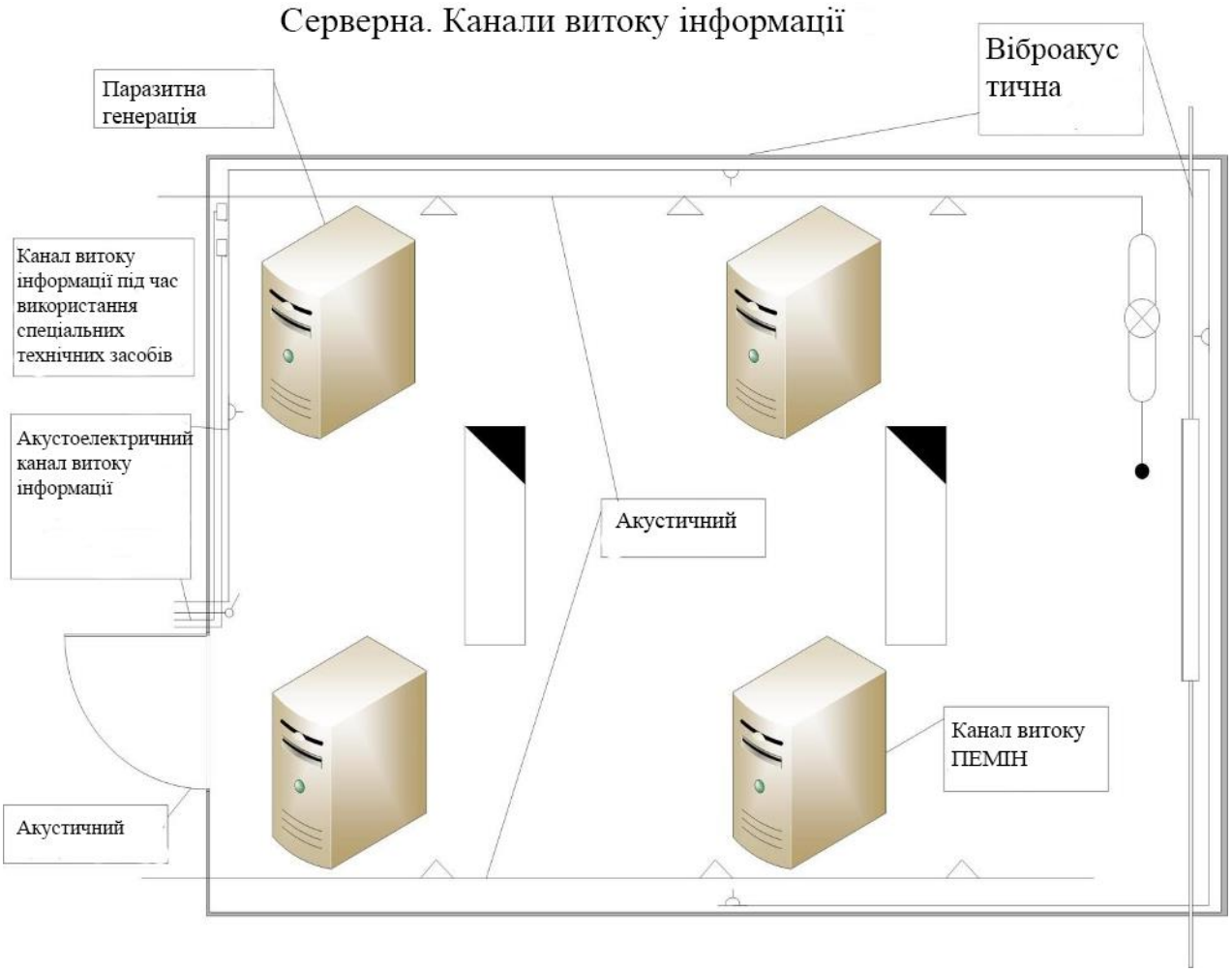

Рисунок 11. Серверна канали витоку інформації.

Тип загрози	Прилади
Паразитна генерація	Комп'ютери, принтери, факси, сканери
Акустичний	Вентиляція, відчинені двері
Акустоелектричний	Електроживлення, заземлення
Канал витоку інформації ПЕМІН	Сервери
Віброакустичний	Захисні конструкції, трубопроводи
Інші канали витоку інформації	Спец. технічні засоби

Таблиця 11.

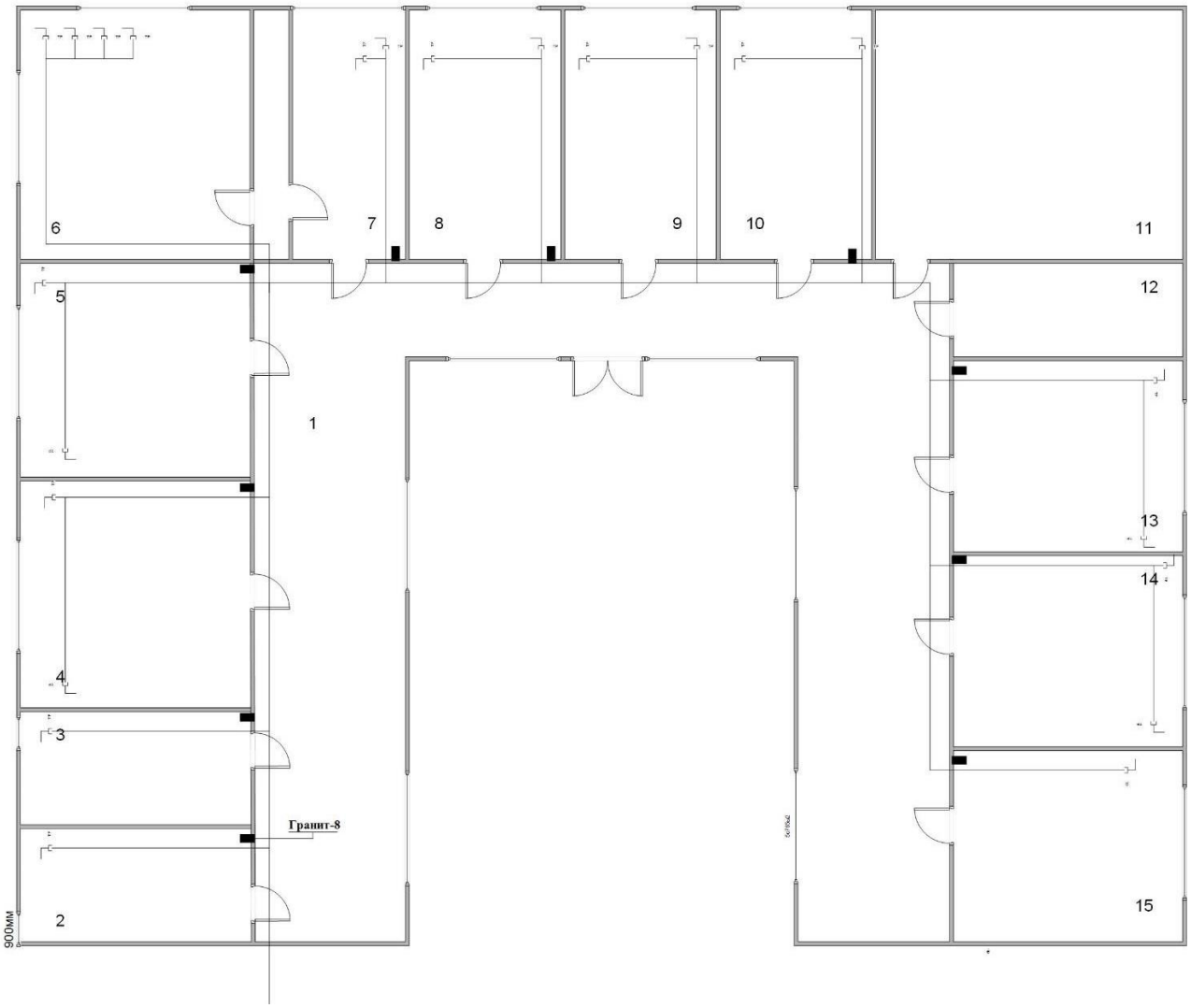

Рисунок 12. Телефонна мережа

Рисунок 13. Комп’ютерна мережа