МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5

ДИПЛОМНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система комплексного захисту інформації на підприємстві

Виконавець: С.В. Попков
Керівник: к.т.н., доцент М.Б. Гумен
Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«___» _____ 20___ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Попкова Сергія Віталійовича

1. Тема: Система комплексного захисту інформації на підприємстві затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати умови функціонування інформаційно-телекомунікаційної системи; скласти та проаналізувати моделі загроз та порушника; розробити систему комплексного захисту інформації підприємства, що гарантує забезпечення захисту інформації та контролю за її обміном.
4. Зміст пояснювальної записки: аналіз існуючих систем комплексного захисту інформації; розробка системи аналізу та основні принципи організації комплексної системи захисту; розробка політики безпеки на підприємстві.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	10.05.2021	*Виконано*
2.	Аналіз літературних джерел	11.05.2021-14.05.2021	*Виконано*
3.	Обґрунтування вибору рішення	15.05.2021 - 17.05.2021	*Виконано*
4.	Збір інформації	18.05.2021 - 22.05.2021	*Виконано*
5.	Дослідження сучасних комплексних систем захисту інформації	23.05.2021-24.05.2021	*Виконано*
6.	Розробка методики та структури КСЗІ	25.05.2021-28.05.2021	*Виконано*
7.	Дослідження комп'ютерних систем	29.05.2021-02.06.2021	*Виконано*
8.	розробити систему комплексного захисту інформації підприємства	03.06.2021	*Виконано*
9.	Перевірка на антиплагіат	04.06.2021-06.06.2021	*Виконано*
10.	Оформлення і друк пояснювальної записки	07.06.2021-08.06.2021	*Виконано*
11.	Оформлення презентації	09.06.2021 – 11.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	14.06.2021	*Виконано*

Здобувач вищої освіти С.В. Попков

(підпис, дата)

Керівник дипломної роботи М.Б. Гумен

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, двох розділів, загальних висновків, списку використаних джерел загальним обсягом робота складає 73 сторінок, має 1 рисунок, 13 таблиць. Список використаних джерел містить 22 найменування і займає 3 сторінки.

Метою роботи є створення комплексної системи захисту інформації на підприємстві

Можливі напрямки розвитку цієї роботи пов’язані із розробою системи комплексного захисту інформації підприємства, що гарантує забезпечення захисту інформації та контролю за її обміном. роботи можуть бути використані для розробки повноцінної системи комплексного захисту цілісності інформації в залежності від типу і характеру діяльності підприємства.

Ключові слова: об’єкт інформаційної діяльності, комплена система захисту інформації, модель загроз, об’єкт загроз

ЗМІСТ

ПЕРЕЛІК ПРИЙНЯТИХ СКОРОЧЕНЬ

БД – база даних

ДТЗ – допоміжні технічні засоби

ЕОМ – електронно-обчислювальна машина

ІД – інформаційна діяльність

ІзОД – інформація з обмеженим доступом

ІТС – інформаційно-телекомунікаційна система

КЗЗ – комплекс засобів захисту

КРТ – копіювально-розмножувальна техніка

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації;

НД – нормативний документ

НД ТЗІ – нормативний документ системи технічного захисту інформації

НСД – несанкціонований доступ

ОС – обчислювальна система

ОТЗ – основні технічні засоби

ПЗІ – підрозділ захисту інформації

ПЕМВН – побічні електромагнітні випромінювання і наведення

ПЗ – програмне забезпечення

ПЗП – постійний запам’ятовувальний пристрій

ПРД – правила розмежування доступу

ПМА – програми та методики атестації

ТЗІ – технічний захист інформації.

ВСТУП

В наш час інформаційних технологій, комрьютерні технології розвиваються досить швидко, та вносять достатньо помітні зміни в нашому житті. Інформація - стає товаром, з яким можно проводити операції обміну, продажу та покупки. Водночас вартість самої інформації найчастіше перевищує вартість комп'ютерної системи, в котрій вона міститься.

Все більше і більше паперові документи зміняють електронні. Для обслуговування цієї інформації необхідні системи, які б забеспечували потрібний захист даних, адже найменшу вразливість можливо використати проти власників інформації.

Безпековий захист комп'ютерної системи досягається шляхом забезпечення конфіденційності, цілісності та доступності даних, що обробляються, а також доступності та цілісності інформаційних компонентів і ресурсів системи.

Подавляюча більшість організацій не знають, як започаткувати захист конфіденційної інформації. Класифіковані типи інформації щодо цін та конфіденційності, компанії можуть визначати пріоритети, дані яких потрібно захищати в першу чергу. про все ще почати з системної інформації про клієнтів або навчальних записів співробітників.

Номери соціального страхування, номера рахунків, ідентифікаційні номери, номери кредитних карток та інші типи структурованої інформації - це обмежені області, які необхідно захищати. Захист неструктурованої інформації, таких як контракти, фінансові звіти та переписка з клієнтами, є важливим наступним шагом, який слід виконувати на рівні відділів.

Мета роботи: спроектувати комплексну систему захисту інформації на підприємстві

Основні завдання:

- проаналізувати умови функціонування інформаційно-телекомунікаційної системи;
- скласти та проаналізувати моделі загроз та порушника;
- розробити політики безпеки інформації на підприємстві

Об’єкт дослідження: Процес комплексного захисту інформації .

Предмет дослідження: Система комплексного захисту інформації підприємства

Практична цінність полягає у розробці системи комплексного захисту інформації підприємства, що гарантує забезпечення захисту інформації та контролю за її обміном.

РОЗДІЛ 1. СИСТЕМА КОМПЛЕКСНОГО ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Поняття системи комплексного захисту інформації на підприємстві

Україна дедалі більше просувається у світовий інформаційний простір, і в контексті пандемії коронавірусу COVID-19 багато компаній використовують найновіші досягнення в галузі Інтернет-технологій. Вони розробляють інформаційні та комп'ютерні технології, розширюють межі обробки, зберігання та передачі інформації (віртуальні офіси тощо), а також онлайн-торгівлю. Інформаційна цінність при впровадженні інноваційних методів значно зростає. Як результат, зростає активність інформаційно-аналітичних структур різних типів винних.

Створення служби захисту інформації гарантує повний захист інформації та контроль за її функціонуванням. Дивно, але навіть сьогодні не всі менеджери усвідомлюють нагальну необхідність організації служби захисту інформації у своїй компанії. Велика кількість книг ШІ присвячена організації захисту інформації в компаніях. Марущака, псевдонім Гриня, В.Б. евича, В.О. Ну.

Аналіз наукових публікацій дозволяє зробити висновок, що в контексті збільшення потоку інформації на підприємстві необхідно створити службу захисту інформації. Служба захисту інформації компанії повинна регулюватися нормативно-правовими актами, розробленими керівництвом, на основі яких доцільно використовувати ці рекомендації міжнародних стандартів та чинного законодавства компанії.

Такими міжнародними стандартами є: ISO / IEC 27002 "Інформаційні технології. Методи захисту. Кодекс поведінки для управління інформаційною безпекою"; ISO / IEC 27003 "Інформаційні технології.

Методи захисту. Посібник із застосування системи управління інформаційною безпекою"; ISO / IEC 27004 "Інформаційні технології. Методи захисту. Вимірювання"; ISO / IEC 27005 «Інформаційні технології. Методи безпеки. Управління ризиками інформаційної безпеки "; ISO / IEC 27006 "Інформаційні технології. Методи забезпечення безпеки. Вимоги до аудиту та сертифікації систем управління інформаційною безпекою "; ISO / IEC 27011" Інформаційні технології. Посібник з управління інформаційною безпекою в телекомунікаціях. Національні нормативні акти включають: типові положення щодо захисту інформації в автоматизованих системах (ND TZI 1.4-001-2000) [4]; Порядок створення повної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003-05) [5]; Методичні вказівки з розробки технічної проблеми при створенні складної системи захисту інформації в автоматизованій системі (НД ТЗІ 3.7-001-99) [6] та інші.

Дотримання принципів міжнародних стандартів серії ISO 27000 забезпечує управління та контроль доступу, розробку та обслуговування апаратних та програмних систем [7]. Дотримання міжнародних стандартів та відповідність національним правовим стандартам інформаційної безпеки необхідні для сталого розвитку бізнесу.

Відповідно до чинного законодавства України та вимог деяких нормативно-правових актів Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та Закону України "Про захист персональних даних" підлягають обов'язковому захисту інформації: Держава право власності на інформацію або інформацію з обмеженим доступом, вимоги до захисту яких визначені законодавством, включаючи персональні дані громадян.

Комплексна система захисту інформації – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу.

Організаційні заходи є обов'язковою складовою побудови будь-якої КСЗІ. Інженерно-технічні заходи здійснюються в міру необхідності.

Організаційні заходи. Організаційна діяльність включає створення концепції інформаційної безпеки та:

- створення посадових інструкцій для користувачів та обслуговуючого персоналу;

- створення адміністративних правил щодо компонентів інформаційної системи, обліку, зберігання, відтворення, знищення носіїв даних, ідентифікації користувачів;

- розробка планів дій на випадок виявлення несанкціонованих спроб доступу до інформаційних ресурсів системи, виходу з ладу захисних засобів, виникнення надзвичайної ситуації;

- навчання правилам захисту інформації користувачів.

За необхідності в рамках організаційних заходів може бути створена служба захисту інформації, а система управління файлами та система зберігання документів може бути реорганізована.

Інженерно-технічні заходи - сукупність спеціальних технічних засобів та їх використання для захисту інформації. Вибір інженерних заходів залежить від рівня гарантованості інформаційної безпеки.

Технічні заходи щодо захисту інформаційної інфраструктури компанії можуть включати використання захищених з'єднань, брандмауерів, розділення потоку інформації між сегментами мережі, використання шифрування та захист від несанкціонованого доступу.

При необхідності встановлення систем охорони та пожежної сигналізації, систем контролю та управління доступом у приміщеннях може бути здійснено в рамках інженерно-технічних заходів.

Деякі кімнати можуть бути обладнані засобами захисту від витоку акустичної (голосової) інформації.

Суб'єкти КСЗІ. У процес створення КСЗІ залучаються такі сторони:

- організація, для якої здійснюється побудова КСЗІ (Замовник);

- організація, що здійснює заходи з побудови КСЗІ (Виконавець);

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

- організація, що здійснює державну експертизу КСЗІ (Організатор експертизи);

- організація, що в разі необхідності залучається Замовником або Виконавцем для виконання деяких робіт зі створення КСЗІ (Підрядник).

Об'єктом захисту КСЗІ є інформація у будь-якій формі та формі. Матеріальні носії - це сигнали. За своєю фізичною природою інформаційні сигнали можна поділити на такі типи: електричні, електромагнітні, акустичні та їх поєднання. Сигнали можуть бути представлені у вигляді електромагнітних, механічних та інших вібрацій, а інформація, що захищається, міститься в її змінних параметрах. Залежно від типу, інформаційні сигнали поширюються в певних фізичних середовищах. Носії можуть бути газоподібними, рідкими або твердими. Наприклад, повітряний простір, будівельні конструкції, сполучні лінії та провідні елементи, заземлення та інші.

Залежно від типу та форми інформаційних сигналів, що циркулюють в інформаційно-телекомунікаційній системі (ITS), включаючи автоматизовані системи (AS), при налаштуванні KSZI можуть застосовуватися різні захисні заходи.

Служба захисту інформації є структурним підрозділом компанії. Структура служби захисту інформації, її склад та її кількість визначаються реальними потребами інформаційно-телекомунікаційних систем з метою задоволення вимог політики інформаційної безпеки та затверджуються керівництвом компанії. Кількість та склад служби захисту інформації повинні бути достатніми для виконання всіх завдань захисту інформації в інформаційних та телекомунікаційних системах.

Метою створення служби інформаційної безпеки є організаційна підтримка управління повною системою захисту інформації в інформаційно-телекомунікаційних системах та контролю її функціонування.

Служба захисту інформації відповідає за виконання робіт з визначення вимог щодо захисту інформації в інформаційних та телекомунікаційних системах, концепцію, розробку та модернізацію системи захисту даних, комплексну інформаційну безпеку, а також експлуатацію, обслуговування, обслуговування комплексна система інформаційної безпеки, контроль інформаційної безпеки в інформаційних системах - телекомунікаціях.

Нормативно-правовою основою вирішення проблем захисту інформації в інформаційно-телекомунікаційних системах українських компаній різних форм власності є: Конституція України [1], відповідні закони України, укази Президента України та Кабінету Міністрів Міністрів України, інші нормативні акти щодо захисту інформації, державні та галузеві стандарти, адміністративні та інші документи організації [2; 3].

Служба захисту інформації повинна здійснювати свою діяльність згідно з "планом захисту інформації в інформаційно-телекомунікаційних системах", графіком, перспективними планами роботи та іншими, затвердженими керівником (заступником директора) компанії [9].

У компаніях, у яких графіком не передбачено створення служби захисту інформації, заходи щодо захисту інформації в інформаційно-телекомунікаційних системах можуть проводити працівники, призначені розпорядженням керівника заводу.

Тому завдання служби захисту інформації включають:

- захист юридичних вимог, пов’язаних з інформаційною безпекою компанії, її відокремлених структурних підрозділів, персоналу в процесі інформаційної діяльності та взаємодії один з одним, а також у відносинах із зовнішніми організаціями в країні та за кордоном;

– дослідження технологій обробки інформації в інформаційно-телекомунікаційних системах з метою виявлення можливих джерел витоків та інших загроз інформаційній безпеці, створення моделі загроз, розробка політики інформаційної безпеки, визначення заходів щодо їх реалізації;

- організація та координація роботи, пов’язаної із захистом інформації в інформаційно-телекомунікаційних системах, вразливість яких визначається їх власником або чинним законодавством, підтримуючи необхідний рівень захисту інформації, ресурсів та технологій;

- розробка проектів нормативних актів та розпорядчих документів, що застосовуються в компанії, згідно з якими повинен бути гарантований захист інформації в інформаційно-телекомунікаційних системах;

- організація роботи зі створення та використання комплексної системи захисту інформації на всіх фазах життєвого циклу інформаційно-телекомунікаційних систем;

- участь в організації професійно-технічної освіти та навчання персоналу та користувачів інформаційно-телекомунікаційних систем захисту інформації;

- навчання персоналу та розуміння користувачами необхідності дотримання вимог нормативних актів, розпоряджень та розпорядчих документів у сфері захисту інформації;

- організація дотримання персоналом та користувачами вимог нормативно-правових актів, нормативних та розпорядчих документів щодо захисту інформації в інформаційно-телекомунікаційних системах шляхом здійснення контрольних перевірок їх відповідності;

- своєчасне виявлення загроз інформації, що захищається, причин та умов їх виникнення та реалізації;

- виявлення та максимальне накладання потенційно можливих каналів та методів несанкціонованого доступу до інформації;

- розробка оперативних механізмів реагування на загрози, використання правових, економічних, організаційних, соціальних та психологічних засобів і методів, технологій та прийомів для виявлення та знешкодження джерел небезпеки для безпеки компанії;

- організація спеціальної діловодства, яка унеможливлює отримання несанкціонованої конфіденційної інформації [8].

1.2 Основні етапи щодо захисту інформації

Визначення складу захищеної інформації - це перший крок у створенні системи захисту. Результат розвитку системи розвитку залежить від точності, з якою вона здійснюється. Загальний підхід полягає в тому, що вся інформація з обмеженим доступом (ISD) захищена: інформація, що є державною таємницею (секретна інформація), інформація, яка є комерційною таємницею і визначається власником, частина публічної інформації. У цьому випадку IZOD повинен бути захищений від витоків і втрат і відкритий - лише від втрат.

Ми часто чуємо, що не всю відкриту інформацію можна захистити. Не всі погоджуються на включення інформації про державну таємницю до ІЗОД.

Тому ми розглянемо ці питання більш детально.

Захист відкритої (публічної) інформації існував завжди і досягався за допомогою запису її засобів масової інформації з урахуванням її руху та розташування. Створено безпечні умови зберігання. Відкритість інформації не зменшує її цінності, і цінна інформація повинна бути захищена від втрат. Цей захист не повинен мати на меті обмеження загальної доступності інформації. Доступ до інформації не може бути відмовлено, але доступ повинен відповідати вимогам щодо її збереження відповідно до вимог обробки та використання (наприклад, бібліотеки).

Інформація є характеристикою взаємодії повідомлення з користувачем.

Публічна інформація - це інформація, яка відтворюється та документується будь-яким способом та на будь-якому носії, отримується або створюється в контексті виконання обов’язків, передбачених правителями відповідно до чинних правових положень або в розпорядженні влад суб’єктів, інше адміністратори публічної інформації, визначені Законом України "Про доступ до публічної інформації".

Конфіденційна інформація - це інформація, доступ до якої обмежена фізична або юридична особа, яка не перебуває при владі, і яка може бути розповсюджена відповідно до методів, передбачених ними на їх прохання та на визначених ними умовах.

Конфіденційна інформація - це інформація, доступ до якої обмежений і розголошення якої може завдати шкоди окремій людині, суспільству чи державі. Інформація, що містить державну, професійну, банківську, слідчу та інші таємниці, передбачені законодавством, вважається таємницею.

Наступна інформація може бути пов'язана з послугою:

1. Інформація, що міститься в документах правителів, що становить внутрішню офіційну кореспонденцію, звіти, рекомендації, якщо вони стосуються розвитку інституту або здійснення контрольних функцій контролю з боку влади, процесу прийняття рішень і перейти до публічних дебатів та / або прийняття рішень наперед.

2. Інформація, зібрана в ході оперативних контррозвідувальних розслідувань в оборонному секторі України, яка не вважається державною таємницею.

Інформаційна безпека - це інформаційний стан, при якому збереження властивостей інформації гарантується конкретною політикою безпеки. Складовими інформаційної безпеки є конфіденційність, цілісність, доступність.

Конфіденційність - це властивість інформації, яка не підлягає розголошенню, секретності, чистої конфіденційності.

Цілісність - це властивість інформації, яку не може змінити неавторизований користувач або процес. Інформація зберігає свою цілісність, якщо зафіксовані правила, встановлені для її модифікації та видалення.

Доступність - це властивість інформаційного ресурсу, що означає, що користувач або процес з відповідними повноваженнями може використовувати цей ресурс відповідно до правил, встановлених політикою безпеки.

1.3 Завдання КСЗІ та вимоги до неї

• Система захисту інформації повинна забезпечувати, щоб АС виконував свої основні функції без значного погіршення його властивостей.

• Це має бути економічно виправданим, оскільки витрати на систему захисту інформації включаються до витрат на АС.

• Захист інформації в межах АС повинен бути гарантований на всіх фазах життєвого циклу з усіма технологічними формами обробки інформації, включаючи роботи з ремонту та обслуговування.

• Система захисту інформації повинна включати можливості для вдосконалення та розвитку відповідно до умов експлуатації та конфігурації АС.

• ICCA повинна гарантувати обмеження доступу до ISOD, щоб відвернути винного від неправдивої інформації, тобто мати характеристики активного та пасивного захисту.

• При взаємодії із захищеною АС із незахищеною АС система безпеки повинна забезпечувати відповідність визначеним правилам обмеження доступу.

• Система безпеки повинна забезпечувати облік та розслідування випадків порушень інформаційної безпеки в межах АС.

• Застосування захисної системи не повинно погіршувати екологічну ситуацію, ускладнювати користувача або викликати психологічний опір і волю до відмови.

Перелік основних завдань, які повинна вирішити складна система захисту інформації:

• керувати доступом користувачів до ресурсів UA, щоб захистити їх від випадкового або навмисного несанкціонованого доступу до системи та несанкціонованого доступу (поза межами повноважень) до її інформації, ресурсного програмного та апаратного забезпечення третіми сторонами та організаційним персоналом та користувачами;

• захист даних, що передаються за каналами зв'язку;

• отримання, збір, зберігання, обробка та передача інформації про всі події, що відбулися в системі та стосуються її безпеки;

• моніторинг роботи користувачів системи адміністрацією та негайне повідомлення адміністратора безпеки про спроби несанкціонованого доступу до системних ресурсів;

• контроль та підтримка цілісності критичних ресурсів системи захисту та середовища програми;

• забезпечення закритого середовища перевіреного програмного забезпечення для захисту від безконтрольного впровадження в систему потенційно небезпечних програм (які можуть містити шкідливі закладки або небезпечні помилки) та засобів подолання системи захисту та від впровадження та поширення комп’ютерних вірусів;

• система управління засобами захисту.

1.4. Основні принципи організації КСЗІ

Захист інформації в межах АС повинен базуватися на таких основних принципах:

• систематизація;

• складність;

• безперервність захисту;

• розумна адекватність;

• гнучкість в адмініструванні та застосуванні;

• відкриття алгоритмів та механізмів захисту;

• простота застосування заходів та захисних засобів.

Принцип систематизації. Системний підхід до захисту комп'ютерних систем вимагає врахування всіх взаємопов'язаних, інтерактивних та змінних у часі елементів, умов та факторів, що є важливими для розуміння та вирішення проблеми безпеки атомної електростанції. При створенні системи безпеки слід враховувати всі слабкі місця, більшість слабких місць комп'ютерної системи, а також тип, можливі об'єкти та напрямки атак на систему з боку винних (особливо висококваліфікованих зловмисників), що означає проникнення розподілені системи та інформація про НСЗ. Система захисту повинна не тільки враховувати всі відомі канали проникнення та інформацію про НСЗ, але також повинна враховувати можливість кардинально нових способів реалізації загроз безпеці, що виникають.

Принцип складності. Фахівці з IT-безпеки мають широкий спектр заходів, методів та засобів захисту IT-систем. Їх глобальне використання включає скоординоване використання різних засобів для побудови цілісної системи захисту, яка охоплює всі важливі канали загроз і не містить слабких місць у місцях з'єднання окремих компонентів. Захист слід будувати шарами. Зовнішній захист повинен забезпечуватися фізичними, організаційними та правовими засобами. Однією з найсильніших ліній захисту є засіб захисту,

реалізований на рівні операційної системи (ОС), оскільки операційна система є лише тією частиною комп'ютерної системи, яка контролює використання всіх ресурсів комп'ютера. Рівень захисту, що застосовується з урахуванням особливостей району, утворює внутрішню лінію оборони.

Принцип безперервності захисту. Захист інформації - це не одноразовий захід або навіть комплекс заходів та встановлених захисних заходів, а рішучий і безперервний процес, що включає в себе прийняття відповідних заходів на всіх фазах життєвого циклу УА, починаючи з ранньої фази розвитку і не лише під час експлуатації . Розробка системи захисту повинна відбуватися паралельно з розвитком самої системи захисту. Як результат, при розробці архітектури беруться до уваги вимоги до безпеки і, зрештою, створюються більш ефективні системи захисту (як з точки зору ресурсів, так і стійкості).

Більшість заходів фізичної та технічної безпеки вимагають постійної організаційної (адміністративної) підтримки, щоб мати можливість ефективно виконувати свої функції (своєчасна зміна та забезпечення правильного зберігання та використання імен, паролів, ключів шифрування, зловживання повноваженнями тощо). Переривання в роботі захисних пристроїв можуть використовуватися зловмисниками для аналізу застосовуваних захисних методів та засобів, реалізації спеціальних програмних та апаратних "закладок" та інших засобів для подолання захисної системи після її відновлення.

Адекватна адекватність. Принципово неможливо створити повністю непереборну систему захисту. Маючи достатньо часу та грошей, ви зможете подолати будь-який захист. Тому має сенс говорити лише про певний прийнятний рівень безпеки. Високоефективна система захисту є дорогою, споживає значну частину енергії та ресурсів комп'ютерної системи та може створити значні додаткові незручності для користувачів. Важливо вибрати

правильний рівень захисту, при якому вартість, ризик та розмір потенційної шкоди є прийнятними (завдання аналізу ризику).

Гнучкість системи захисту. Часто доводиться створювати захисну систему в умовах великої невизначеності. Тому вжиті заходи та встановлене захисне обладнання, особливо на початковій фазі їх експлуатації, можуть забезпечити як надмірний, так і недостатній захист. Для того, щоб мати можливість змінювати рівень захисту, захисні засоби, звичайно, повинні мати певну гнучкість. Ця властивість особливо важлива, коли захисне обладнання повинно бути встановлене на системі, яка працює без порушення нормальної роботи. Крім того, зовнішні умови та вимоги змінюються з часом. У таких ситуаціях властивість гнучкості економить власникам ОД різкі заходи щодо повної заміни захисного обладнання на нове.

Відкриття алгоритмів та механізмів захисту. Суть принципу відкритості алгоритмів та механізмів захисту полягає в тому, що захист повинен бути гарантований не лише обмеженням доступу до організаційної структури та функціонуючих алгоритмів її підсистем. Знання алгоритмів системи захисту не слід перевищувати (також автор). Однак це не означає, що інформація про певну систему захисту повинна бути загальнодоступною.

Принцип простого застосування захисту. Механізми захисту повинні бути інтуїтивно зрозумілими та простими у використанні. Використання гарантій не повинно передбачати знання конкретних мов або дій, що вимагають значних додаткових трудових витрат при нормальній роботі законних користувачів, і не повинно вимагати від користувача виконання погано зрозумілих рутинних операцій (введення декількох паролів та імен тощо).

РОЗДІЛ 2. РОЗРОБКА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Загальні відомості про приватне підприємство «Сіріус»

“Сіріус” – приватне охоронне підприємство, що надає спеціалізовані галузеві і комплексні послуги з фізичної, технічної, інформаційної, банківської, пожежної та техногенної безпеки.

Адреса: 03058, м. Київ, вул. Ніжинська, 29 Г.Специфікація діяльності ОІД:

Технічний відділ працює за програмним забезпеченням інформаційно-комунікаційних системи приватного підприємства "Сіріус".

Час роботи понеділок-п’ятниця з 8:00 – 17:00, перерва 12:00 – 13:00,субота – неділя вихідні дні.

2.2 Обґрунтування необхідності створення КСЗІ

Підставою для визначення необхідності створення ІССА є норми та вимоги чинного законодавства, які передбачають обмеження доступу до певних видів інформації або забезпечення її цілісності чи доступності, або рішення власника інформації, якщо нормативні акти передбачають йому / їй надано право діяти на власний розсуд.

"Відповідно до Закону" Про захист інформації в інформаційно-телекомунікаційних системах "умови обробки інформації в системі встановлюються власником системи відповідно до угоди з власником інформації, якщо не передбачена процедура Доступ до інформації, перелік користувачів та їх повноваження щодо цієї інформації визначаються власником інформації ".

Відповідальність за захист інформації в системі покладається на власника системи.

Інспекція з питань інформаційної діяльності

Об'єктом інформаційної діяльності (далі OID) є інформаційно-телекомунікаційна система приватної компанії "Сіріус"

Розслідування, яке є предметом інформаційної діяльності, проводилось відповідно до керівних принципів щодо структури та змісту концепції захисту інформації в автоматизованій системі - НД ТЗІ 1.4-001-2000 із змінами, внесеними положенням про спеціальні державні комунікації адміністрація від 28 грудня 2012 р. № 806 - типові положення щодо інформації служб охорони в UA, дослідження робочого середовища. Закон видано згідно з Додатком А. «Форма та зміст акта перевірки суб’єкта інформаційної діяльності у зв’язку зі створенням запису ТКІ, НД ТКІ 3.1-001-07 Захист інформації щодо суб’єкта інформаційної діяльності. Будівництво комплексу технічного захисту інформації. Попередня проектна робота “Порядок проведення вимірювань відповідає ДСТУ 3396.1.

У ході розслідування було враховано робоче середовище ІТС: комп’ютерна система, фізичне середовище, середовище користувача та оброблена інформація. Надано опис кожного робочого середовища ІТС.

Згідно з НД ТЗІ 1.6-005-2013 «Захист інформації про об’єкти інформаційної діяльності. Розпорядження про категоризацію об’єктів, щодо яких циркулює інформація з обмеженим доступом, що не є державною таємницею », розглядається ОІД визначено у категорії IV (четверта). оскільки об’єкт використовує технічні засоби для обробки інформації з обмеженим доступом, яка не є державною таємницею.

Вивчення фізичного середовища: характеристики OID, де розміщена та функціонує інформаційно-телекомунікаційна система.

ІТС знаходиться в залі за адресою: 03058, м. Київ, вул. Ніжинська, 29 Г. Одноповерхова будівля OID розташована в орендованому офісі загальною площею 40,3 м2. На території діє паспортний режим, працює цілодобова служба охорони.

Діаграма розташування OID та оточуючих об'єктів показана на карті розташування (Додаток В. Рисунок 1). Оглядовий план показує схеми

відеоспостереження та протиугінної сигналізації (Додаток G. Рисунок 2).

Особливості OID-компонентів:

- висота стелі - 420 м;

- перекриття - 500 мм;

- перегородки - 150 мм;

- Зовнішні стіни з цегли - 500 мм.

Вікна: склопакет із металопластикових вікон у всіх приміщеннях розміром 1400,1320 мм. Віконні отвори оснащені регульованими пристроями, такими як: ролети.

Двері спальні виготовлені з металу 2700x900. Дверні петлі захищені захистом від порізів. Розсувний внутрішній металевий кожух на дверях біля входу в OID.

Система живлення (освітлення): мережа 220 В; немає незалежного джерела живлення; Лампи зі світлодіодними лампами. Кабельне підключення до Інтернету - екранована вита пара UTP 4x2x0,5 5. у коробці.

Система опалення автономна. Система вентиляції - випускний потік. Заземлення - доступне. Системи сигналізації:

- пожежа - димовий сповіщувач SPD 3, ручний пожежний сповіщувач, стельові петлі, пристрій Mon 7P, прилади сигналізації;

- Безпека - магнітні контактні сповіщувачі для відкривання дверей і вікон, оптичні сповіщувачі руху Swan - 2, клавіатура, панель управління.

Підключення - екранований кабель 4x2.

Будівля обладнана електромережею, опаленням, водопостачанням та каналізацією, автоматичною пожежною сигналізацією. Електроживлення систем освітлення, електропостачання та опалення забезпечується через підключення до комунальних служб. Пожежна сигналізація підключена до центру управління.

Біля входу в будівлю є відомча охорона, яка забезпечує доступ і пропонує цілодобову охорону. У передній частині кімнати встановлена система відеоспостереження з візуальним контролем безпеки приміщення біля входу в будівлю.

У табл. 2.1 зазначені основні складові системи комунікації підприємства

Таблиця 2.1

Системи комунікації

Електропостачання	Підключено до трансформаторної підстанції №3, яка має сторонніх споживачів і знаходиться за межами КЗ
Система опалення	Підключена до міської мережі опалення, знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Система каналізації	Підключена до міської мережі, яка знаходиться за межами КЗ
Система водопостачання	Підключена до міського водоканалу, яка знаходиться за межами КЗ (пластикові труби, однотрубна вертикальна система опалення)
Заземлення	Всі прилади, комп'ютери заземлені на спільний контур заземлення, який є замкнутий і виходить за межі КЗ
Система вентиляції	Приточно-витяжна
Internet	Кабельне підключення, що виходить за межі ОІД

Штат співробітників підприємства складається з 19 осіб: директор, бухгалтер, системний адміністратор, чотири диспетчери, 12 охоронників. На рис. 2.1. зображена організаційна структура робітників підприємства.

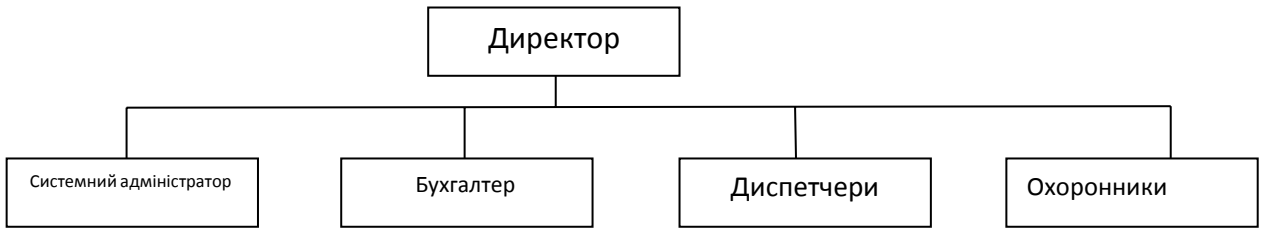

Рис. 2.1. Організаційна структура

Залежно від рівня авторизації доступу до інформації та типу роботи, що виконується в процесі експлуатації ІТС, користувачі системи мають різні рівні доступу до ІТС.

Обов'язки працівників зазначені в їх посадових інструкціях відповідно до їх діяльності.

Обов'язки директора:

- приймати рішення в межах своїх функціональних обов'язків, визначених статутом компанії та відповідно до чинного в Україні законодавства;

- підбір та розстановка персоналу;

- визначати, формулювати та координувати всю діяльність компанії;

- визначити напрямок корпоративного розвитку у всіх сферах діяльності;

- здійснення кадрової роботи;

- розробити посадові інструкції, внутрішні документи та інші документи.

Завдання системного адміністратора:

- встановлення, налагодження системного програмного забезпечення;

- впровадження засобів захисту від комп’ютерних вірусів;

- управління локальною комп'ютерною мережею компанії;

- організація прийняття відповідальності за угоди із сторонніми організаціями, що надають комунікаційні, програмні та апаратні послуги компанії;

- усунення надзвичайних ситуацій, пов’язаних з пошкодженням програмного забезпечення;

- адміністрування ІТС, обмежує доступ користувачів до системи.

Обов'язки бухгалтера:

- бухгалтерський облік з урахуванням специфіки діяльності фірми;

- Реєстрація та подання первинних документів;

- Підготовка звітів про фінансовий стан компанії, результати діяльності та рух коштів;

- забезпечити передбачену законодавством передачу податків та зборів;

- провести інвентаризаційні роботи на підприємстві;

- створення документів, реєстрів та журналів, які обробляються для їх зберігання;

- запустити інвентаризацію.

Обов'язки диспетчерів:

- контроль над об'єктами, що перебувають під охороною компанії, в Інтернеті;

- виклик групи реакції в режимі тривоги. Дослідження операцій ІТС:

Дослідження щодо інформаційного середовища включає інформацію, яка

підлягає обробці ІТС.

Власником інформації є менеджер. В автоматизованій системі немає секретної та офіційної інформації, інформації, що є державною власністю, або інформації, що є державною таємницею.

Залежно від режиму доступу інформація, що обробляється ІТС, поділяється на:

- інформацію про обмежений доступ (IZOD);
- відкриту для захисту інформацію;
- відкриту інформацію що не потребує захисту.

IZOD представлений в ITS як електронні документи, створені за допомогою пакета програм Microsoft Office 2010, Adobe Reader або у паперовій формі. Папірець зберігається у сейфі.

Правила доступу до інформації встановлює директор. Доступ до ISOD мають лише зареєстровані користувачі. Інформація з обмеженим доступом має цінність, тому втрата або передача може призвести до майнової шкоди компанії.

ВОТ, що циркулює в ІТС, зберігається:

- на магнітному жорсткому диску;
- на папері.

Документи, що містять МКБ, друкуються за допомогою принтерів, що входять до складу ІТС. Копіювання на гнучкі носії та флешки заборонено. Перелік інформації, що становить ІТС, а також вся інформація про тип доступу, правову систему та тип презентації в ІТС перелічені та розміщені в таблиці 3.4. Вимога щодо захисту визначається власником відповідно до офіційних вимог.

Адміністративний контроль доступу налаштований для всіх типів інформації, показаних у таблиці. Атрибути доступу присвоюються, коли документ створюється в системі. Інформацію можна зберігати в системі у форматах doc, docx, xls, pdf.

Інформація імпортується та експортується в ІТС за допомогою електронної пошти, сканування паперу та друку документів.

У табл. 2.2 наведено основні класіфікаційні ознаки інформації.

Таблиця 2.2

Класифікація інформації

Опис	Правовий режим	Режим доступу	Тип представлення	Вимоги до захисту	Доступ мають
Організаційно-розпорядча документація	Конфіденційна	ІзОД	Зберігається в кабінетіу директора на паперовому носії та на сервері	Ц,Д	Директор, системний адміністратор
Облік внутрішніх документів	Конфіденційна	ІзОД	Зберігаються в кабінетіу директора на паперовому носії	К,Ц,Д	Директор, бухгалтер
Інформація про надання послуг, тарифи, контактна інформація підприємства	-	Відкрита, не потребує захисту	Текстова та числовоінформація в цифровому та паперовому вигляді.	Ц,Д	Директор, системний адміністратор, бухгалтер
Інформація проробітників	Конфіденційна	ІзОД	Зберігаються в кабінеті у директора на паперовому носії	К,Ц,Д	Директор, Бухгалтер
Статутні документи підприємства	-	Відкрита, не потребує захисту	Зберігається в кабінетіу директора на паперовому носії	Ц.Д	Усі працівники
Облік та реєстрація вхідних та вихідних документів організації	Конфіденційна	ІзОД	Зберігається в кабінетіу директора на паперовому носії та на сервері	К,Ц,Д	Директор, системний адміністратор

Дослідження комп'ютерних систем. Комп’ютерна система локальна - пристрої, розташовані в OID, підключені. Локальна мережа створена для покриття внутрішніх потреб компанії. Існує підключення до глобальної мережі Інтернет для взаємодії із зовнішніми органами (державна податкова служба, інші фонди тощо). Канал зв'язку в мережі компанії та підключення до Інтернету забезпечуються постачальником "Київстар", який надає послуги будівництво, забезпечення та підтримка телекомунікаційної мережі департаменту за домовленістю між Сіріусом та. він приносить

Київська зірка. Обладнання AU, що використовується для обробки інформації про OID: керівні посади; Робоче місце диспетчера; Робоча станція системного адміністратора; АРМ бухгалтерського обліку; МФП, підключений до робочого місця директора; Принтер формату А4, підключений до робочого місця директора та бухгалтера. Всі робочі місця підключені до Інтернету за допомогою кабелю; Бездротовий маршрутизатор забезпечує підключення до Інтернету. Спосіб підключення мережевих пристроїв за топологією пов’язаний із типом зірки. Всі комп'ютери в мережі підключені до центрального вузла, тобто маршрутизатора.

У табл. 2.3. наведено характеристику складових ІТС інформаційних комунікаційних систем

Таблиця 2.3

Характеристика складових ІТС наявних у системі

Назва	**Умовне позначенняна схемі**	**IP адреса пристрою**	**Серійний номер**	**Характеристика**
Робоча станція 1 (директора) HP Z440 (T4K25EA)	ПК3	192.168.0.104	UTY13UT76R	Intel Core i5-8400 (2.8 - 4.0 ГГц) / RAM16 ГБ / HDD 2 ТБ + SSD 240 ГБ / Intel UHD Graphics 630 /без ОД / LAN

Продовження табл. 2.3

Назва	**Умовне позначенняна схемі**	**IP адреса пристрою**	**Серійний номер**	**Характеристика**
Робоча станція 2 (бухгалтера) HP Z440 (T4K25EA)	ПК2	192.168.0 .103	KTY13U T80D	Intel Core i5-8400 (2.8 - 4.0 ГГц) / RAM 16 ГБ / HDD 2 ТБ + SSD 240 ГБ / Intel UHD Graphics 630 / LAN
Робоча станція 3 (системного адміністратора) HP Z440 (T4K25EA)	ПК1	192.168.0 .101	RRY13U T87R	
Робоча станція 4 (диспетчера) HP Z440 (T4K25EA)	ПК4	192.168.0 .102	RTY13R R80D	
Сервер	S1	192.168.1 11	DDY12U T87F	Dell PowerEdge R510 2 x XEON 4 Core E5620 2.4 GHz 24GB DDR3 12 слотов под диски 3.5" SATA/SAS PERC H700

Продовження табл. 2.3

Назва	**Умовне позначенняна схемі**	**IP адреса пристрою**	**Серійний номер**	**Характеристика**
БФП, підключений до ПК 3 Brother HL-L2365DWR	P1	-	JNZNR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;
БФП, підключений до ПК 2 Brother HL-L2365DWR	P2	-	TY JNR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;
БФП, підключений до ПК 1 Brother HL-L2365DWR	P3	-	UTY NR0013	Максимальна роздільна здатність друку 600x2400 dpi Технологія друку Лазерний (ч/б) Стандартний лоток: A4, Letter, A5, A6, Executive Швидкість друку: до 30 стр/хв;

Продовження табл. 2.3

Назва	**Умовне позначенняна схемі**	**IP адреса пристрою**	**Серійний номер**	**Характеристика**
Принтер, підключений до ПК 1 HP LaserJetPro M102	РК1	-	SN03PRC05	Максимальна роздільна здатність друку 600x600 dpi Технологія друку Лазерний (ч/б) Інтерфейс USB 2.0
Принтер, підключени й до ПК 3 Epson L1800A3	РК2	-	CN684JZ20M	Максимальна роздільна здатність друку 5760x1440 dpi Технологія друку Струменевий Інтерфейс USB 2.0
Комп'ютерна миша, підключена до: ПК 1; ПК2; ПК 3; ПК 4 Logitech Wireless Mouse M185 (910-002238) Grey	-	-	910-002238 910-003501 910-002256 910-002257	Джерело живлення1 x AA Тип датчика Оптичний Кількість кнопок 2Інтерфейс Wireless
Монітор, підключений до: ПК 1; ПК 2; ПК 3; ПК 4 Philips V-line 203V5LSB26 /10/62	-	-	PE19HS4P60 PE19TR5K30 PE19HS4S45 PE19NY4R69	Діагональ дисплея 19.5" Тип матриці TN+film Максимальна роздільна здатність дисплея 1600 x 900 Покриття Матове
Клавіатура, підключена до: ПК 1; ПК2; ПК 3; ПК4 Logitech K120 USB Black	-	-	C-8940C-8745 C-8170C-8952	Інтерфейс USB Кількість кнопок:104 Тип: мембранна

2.3 Аналіз загроз інформації, що циркулює на ОІД

Визначення інформаційних ресурсів на підприємстві, що потребують захисту.

Sirius Enterprise ITS вимагає захисту таких інформаційних ресурсів:

- файли, записи, які обробляються, зберігаються та передаються;

- системне та функціональне програмне забезпечення;

- база даних із конфіденційними даними компанії.

Інформаційні ресурси ІТС протікають через засоби ІТ та

а саме оперативна пам'ять, екран, принтер, сканер, клавіатура, мережеві пристрої, які підлягають захисту.

У табл. 2.4. зазначені види інформації та рівні конфіденційності, цілосності, та доступності

Таблиця 2.4

Визначення рівня конфіденційності, цілісності тадоступності інформації

Інформація	**Рівень конфіденційності**	**Рівень цілісності**	**Рівень доступності**
Організаційно-розпорядча документація (зберігається в кабінеті у директора на паперовому та електронному носії)	К2	Ц4	Д4
Облік внутрішніх документів (накази, службові записки, інструкції) (зберігаються в кабінеті у директора на паперовому та електронному носії)	К1	Ц4	Д3
Інформація про надання послуг,тарифи, контактна інформація підприємства	К4	Ц3	Д3
Інформація про робітників (зберігається в кабінеті у директора напаперовому та електронному носії)	К1	Ц4	Д3

Продовження табл 2.4

Статутні документи підприємства (документи, що дозволяють займатися підприємницькою діяльністю) (зберігається в кабінеті у директора на паперовому та електронному носії)	К4	Ц3	Д4
Облік та реєстрація вхідних та вихідних документів організації	К4	Ц4	Д3
Трудові договори робітників (зберігається в кабінеті у директора на паперовому та електронному носії)	К4	Ц4	Д2
Записи файлів відеоспостереження	К5	Ц5	Д5

У табл. 2.4 стосовно коніденційності прийняті такі позначення

Конфіденційність:

– К0 - розголошення інформації призводить до краху роботи суб'єкта абодуже великих матеріальних втрат;

– К1-розголошення призводить до значних матеріальних втрат, якщо небуде вжито заходів;

– К2 - розголошення призведуть до деяких матеріальних втрат;

– К3 - Приносить матеріальний збиток в певних випадках;

– К4 - може принести малозначний збиток в рідкісних випадках.

Стосовно цілосності:

– Ц0 – призводить до неправильної роботи суб'єкта в цілому або значної його частини і наслідки зміни незворотні;

– Ц1 –несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки незворотні;

– Ц2 – несанкціоновані зміни призведуть до неправильної роботи суб'єктів через деякий час, якщо не буде вжито заходів. Наслідки оборотні;

– Ц3 – несанкціоновані зміни не приведуть до збою в роботі суб'єкта,наслідки оборотні;

– Ц4 - несанкціоновані зміни не відражатимуться на роботі системи.

Стосовно доступності:

– Д0 – у разі порушення доступності інформації даного типу підприємство не понесе матеріального збитку, робота підприємства не буде порушена, бажано впровадження, зміни в існуючих технологічнихпроцесах;

– Д1 – у разі порушення доступності інформації даного типу підприємство понесе мінімальний збиток матеріального прибутку, робота підприємства не буде порушена, загальний дохід залишиться без зміни;

– Д2 – у разі порушення доступності інформації даного типу підприємство понесе середній збиток матеріального прибутку за поточний квартал, робота підприємства не буде порушена, можливі відставання від конкурентних підприємств;

– Д3 – у разі порушення доступності інформації даного типу підприємство понесе збиток матеріального прибутку, робота підприємства буде ускладнена, загальний дохід може знизиться до половини існуючого;

– Д4 – у разі такого порушення доступності інформації компанія зазнає найбільшої можливої шкоди матеріальній вигоді протягом декількох кварталів, повинні бути прийняті радикальні рішення щодо наявності інформації в компанії.

Визначення переліку загроз. Загроза — будь-які обставини або події, що можуть бути причиноюпорушення політики безпеки інформації і/або нанесення збитків АС.

Загрози в залежності від виду впливів на інформацію й НСД до неї можна розділити на випадкові й навмисні.

До випадкових загроз варто віднести:

– відмови й збої апаратури;
– перешкоди на лінії зв'язку від впливів зовнішнього середовища;
– помилки людини як ланки системи;
– системні й системотехнічні помилки розробників;
– структурні, алгоритмічні й програмні помилки;
– аварійні ситуації й інші впливи.
– відмова від функціонування ІТС в цілому, наприклад вихід з ладу

електроживлення;

– стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки тощо.

Навмисні загрози пов'язані з діями людини, причинами яких можуть бути

певне невдоволення своєю життєвою ситуацією, сугубо матеріальний інтерес абопроста розвага із самоствердженням своїх здатностей, як у хакерів, й т.д.

Усі джерела загрози мають різний ступінь небезпеки (Сор) і, що може бути визначено кількісно за допомогою рейтингу. У цьому випадку ступінь ризику оцінюється за допомогою непрямих показників.

В якості критеріїв порівняння (показників) ви можемо вибрати:

Можливість джерела (К1) - визначає ступінь доступності об’єкта, що охороняється (для антропогенних джерел), відстань до об’єкта, що охороняється (для штучних джерел), або особливості ситуації (для випадкових джерел).

Наявність джерела (К2) - визначає ступінь кваліфікації та привабливості дій джерела загрози (для антропогенних джерел) або наявність необхідних умов (для штучних та природних джерел).

Fatality (К3) - визначає ступінь нездоланності наслідків загрози.

Кожен показник оцінюється за п’ятибальною шкалою за допомогою експертно-аналітичного методу. Крім того, 1 відповідає мінімальному впливу оціночного показника на ризик використання джерела, а 5 - максимальному.

У табл 2.5 рівні загроз та вразливостей на підприємстві «Сіріус»

Таблиця 2.5

Рівень загроз та вразливостей на підприємстві «Сіріус»

	Вид загрози	**Вразливості, що призведуть дореалізації загроз**	**Ймовірність**	**Що порушує**	**Рівень загрози**	**Джерело**	**Загальна оцінка загрози**
	1. Навмисні загрози (антропогенні та техногенні)						
.1	НСД до даних з порушенням встановлених правил розмежування доступу внаслідок використання порушником відомих вразливостей системного та прикладного ПЗ	-недосконале або нове ПЗ; -помилки при розмежуваннідоступу до системи.	2	К,Ц,Д,С	3	внутрішнє, зовнішнє	2,5
.2	Порушення конфіденційності або цілісності інформації, що зберігається в ІТС, внаслідок навмисних дій авторизованого користувача	-відсутність резервних копій; -неправильний підбор персоналу; -неефективне розмежування прав доступу в системі.	1	К,Ц,Д,С	3	внутрішнє	2
.3	Впровадження і використання комп'ютерних вірусів, закладних програм для порушення безпеки даних	-відсутність або неефективністьантивірусного ПЗ; -наявність незахищеного з`єднання.	2	К,Ц,Д,С	3	внутрішнє, зовнішнє	2,5

Продовження табл. 2.5

	Вид загрози	**Вразливості, що призведуть дореалізації загроз**	**Ймовірність**	**Що порушує**	**Рівень загрози**	**Джерело**	**Загальна оцінка загрози**
.4	Одержання технологічної інформації (атрибутів доступу адміністраторів або інших користувачів системи) іншим користувачем ІТС атрибутами доступу для розширювання своїх повноважень або маскування під іншого зареєстрованого	-необізнаність персоналу; -відсутність/неефективність ідентифікації та автентифікації користувача.	3	К,Ц,Д,С	2	внутрішнє	2,5
.5	Одержання та використання атрибутівдоступу системи сторонніми особамивнаслідок необережного поводження користувачів	-передавання паролів у відкритому вигляді; -необізнаність персоналу в питання інформаційної безпеки.	2	К,Ц,Д,С	5	зовнішнє	3,5
.6	Читання залишкової інформації з оперативної та зовнішньої пам’яті ЕОМ	-не реалізованість забороніповторного використання інформації.	2	К	3	внутрішнє	2,
	2. Випадкові загрози						

Продовження табл. 2.5

.1	Ненавмисні дії користувачів, що призводять до відмови функціонування мережі чи окремих її елементів, пошкодження обладнання (телекомунікаційного, програмних та інформаційних ресурсів)	-необізнаність персоналу в питаннях інформаційної безпеки; -доступність до елементів систем, в якій немає необхідності.	2	К,Ц,Д,С	4	внутрішнє	3
.2	Порушення цілісності інформації, що зберігається, внаслідок ненавмисних дійкористувачів	-відсутність резервного обладнання	3	Ц,Д,С	4	внутрішнє	3,5
.3	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цих носіях	-недосвідченість персоналу	2	Ц,Д	3	внутрішнє	2,5
.4	Неправомірна зміна режимів роботи обладнання, програмних засобів тощо, ініціювання процесів, які здатні призвести до незворотних змін у системі	-недосвідченість персоналу	1	К,Ц,Д,С	4	внутрішнє	2,5
.5	Випадкове зараження програмних засобівкомп'ютерними вірусами	-необізнаність персоналу; -неякісне антивірусне ПЗ.	4	К,Ц,Д,С	4	внутрішнє	4

Продовження табл. 2.5

.6	Невиконання організаційних заходів, посадових і технологічних інструкцій щодо порядку та правил експлуатації чи використання мережевих ресурсів	-недбалість персоналу; -недосвідченість персоналу в питаннях інформаційної безпеки.	2	К,Ц,Д,С	2	внутрішнє	2
.7	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ (системне та прикладне ПЗ, навчальні та ігрові програми та ін.)	-недбалість персоналу	2	К,Ц,Д,С	1	внутрішнє	1,5
.8	Порушенні цілісності інформації, що зберігається внаслідок апаратного або програмного збою	-відсутність резервного обладнання; -відсутність плану безперервної роботи.	3	Ц,Д,С	4	внутрішнє	3,5
3. Стихійні (впливи природних факторів)							
.1	Зміна умов фізичного середовища (стихійні лиха, такі як землетрус, повінь, пожежа і аварії або інші випадкові події)	-наявність легкозаймистих матеріалів; -несправність каналізаційноїсистеми; -старе приміщення.	2	Ц,Д,С	3	зовнішнє	2,5

Продовження табл. 2.5

.2	Впливи природних завад (грозові розряди,іскріння в електромережах, під час електрозварювання тощо)	-відсутність захисту від блискавки; -неякісна електропроводка; -відсутність резервних каналівелектроживлення.	2	Ц,Д,С	3	зовнішнє	2,5

Визначення переліку порушників. Порушник- це особа, яка випадково, по необізнаності, навмисно, зі злочиною або без неї намагалася, використовуючи різні можливості, методи та засоби, здійснити операції, що призвели або можуть призвести до порушення інформації, визначеної в політиці. безпеки.

Що стосується ІТС, винні особи можуть бути: внутрішніми (із працівниками або користувачами системи) або зовнішніми (третіми сторонами).

Користувач системної інформації - фізична або юридична особа, якій надано право доступу до системної інформації в порядку, передбаченому законодавством;

Залежно від повноважень доступу до інформації, типу та складу роботи, що виконується в процесі ІТС, люди, які мають до неї доступ, поділяються на такі категорії:

- користувачі, уповноважені розробляти та підтримувати систему захисту інформації, а також повноваження забезпечувати управління ІТС - адміністратором мережі;

- Користувачі, яким надано право доступу до конфіденційної інформації на одному або декількох рівнях класифікації - директор, керівник відділу кадрів, працівник відділу кадрів, головний економіст, економіст, секретар;

- Розробники програмного забезпечення, які розробляють та впроваджують нові бізнес-процеси та підтримують існуючі;

- Постачальники обладнання та технічних ресурсів ІТС та спеціалісти, які виконують монтаж та обслуговування в гарантійному та післягарантійному періодах;

- технічний персонал, що забезпечує щоденне підтримання фізичного середовища ІТС - інженер, електрик, технічний персонал з обслуговування будинків, ліній зв'язку.

Модель злочинця - це абстрактний, офіційний або неформальний опис винного. Модель злочинця відображає його практику та потенціал, можливості, попередні знання, час і місце дії тощо.

У табл 2.6 -2.10 наведено характеристики моделі порушника

Таблиця 2.6

Специфікація моделі порушника за рівнем кваліфікації таобізнаності

Позначення	Основні ознаки порушника
К0	Не знає функціональні особливостісистеми, основні закономірності формування масивів даних та потоків запитів до них, має навички щодокористування штатними засобами системи.
К1	Знає функціональні особливостісистеми, основні закономірностіформування масивів даних та потоків запитів до них, має навички щодо користування штатними засобами системи.
К2	Володіє високим рівнем знань та практичними навичками роботи з технічними засобами системи та їх обслуговування
К3	Володіє високим рівнем знань у галузі програмування та обчислювальноїтехніки, проектування та експлуатації автоматизованих інформаційних систем.
К4	Знає структуру, функції й механізми дії засобів захисту, їх недоліки.
К5	Знає недоліки та вади механізмів захисту, які вбудовані у системне програмне забезпечення та його не документовані можливості.
К6	Є розробником програмних та програмно-апаратних засобів захисту або системного програмного забезпечення.

Таблиця 3.7

Специфікація моделі порушника за часом дії

Позначення	Характеристика можливостей порушника
Ч1	До впровадження АС або її окремих компонентів.
Ч2	Під час бездіяльності компонентів системи (в неробочий час, під час планових перерв у роботі, перерв для обслуговування і ремонту і т.д.).
Ч3	Під час функціонування АС (або компонентів системи).

Продовження табл 3.7

Ч4	Як у процесі функціонування АС, так і під час зупинки компонентів системи.

Таблиця 3.8

Специфікація моделі порушника за місцем дії

Позначення	Характеристика місця дії порушника
Д1	Без доступу на контрольовану територію організації.
Д2	З контрольованої території без доступу у будинки та споруди.
Д3	Усередині приміщень, але без доступу до технічних засобів АС.
Д4	З робочих місць користувачів АС.
Д5	З доступом у зони даних (баз даних, архівів й т.ін.).
Д6	З доступом у зону керування засобами забезпечення безпеки АС.

Таблиця 3.9

Специфікація моделі порушника за мотивами здійснення порушень

Позначення	Мотив порушення
М1	Безвідповідальність
М2	Самозатвердження
М3	Корисливий інтерес

Таблиця 3.10

Модель порушника

Посада	Можливий мотив	Категорія обізнаності порушника	Можливе місце дії	Можливий час дії
Внутрішні				
Директор	М2,М3	К1	Д6	Ч4
Диспетчер	М2,М3	К2	Д5	Ч4
Бухгалтер	М1,М2, М3	К1	Д4	Ч3
Системний адміністратор	М2, М3	К5	Д6	Ч4
Прибиральниця	М2, М3	К0	Д3	Ч2
Зовнішні				

Продовження табл 3.10

Представники організацій, щовзаємодіють з питань технічного забезпечення	М3	К5	Д2	Ч1
Представники організацій, що взаємодіють з питань ПЗ	М3	К4	Д3	Ч1
Злочинці (хакери)	М2, М3	К3	Д1	Ч3

Визначення каналів несанкціонованого доступу до ІТС Несанкціонований доступ до інформації – доступ до інформації, за якого порушуються встановлений порядок його здійснення та (чи) правові норми.

Доступ порушенням посадових повноважень співробітника, доступ до закритої для публічного доступу інформації з боку осіб, котрі не мають дозволу на доступ до цієї інформації. Також іноді несанкціонованим доступом називають одержання доступу до інформації особою, що має право на доступ до цієї інформації в обсязі, що перевищує необхідний для виконання службових обов'язків.

Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання (ДСТУ 3396.2-97 [4]).

Основними каналами витоку інформації в ІТС на ОІД є :

– змінні носії, та носії на які здійснюється архівування;

– робочі станції працівників відділів;

– робоча станція адміністратора системи;

– засоби вводу\виводу інформації;

– канали передачі інформації в ІТС;

– комутатор.

Вибір заходів захисту інформації в ІТС підприємства. Забезпечення інформаційної безпеки в ІТС включає використання ряду заходів захисту інформації: організаційні, організаційні та технічні, використання програмного, апаратно-програмного та апаратного захисту, використання засобів технічного

захисту.

Згідно НД ТЗІ 1.1-003-99 матриця доступу – n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об’єктів КС одного типу (об’єктів-користувачів, об’єктів-процесів чи пасивних об’єктів), і містить визначені права доступу суб’єктів до кожного із типів об’єктів.

Доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

Основними видами інформаційної діяльності є створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації.

У табл. 2.11 наведено інформацію показників керування доступом

Таблиця 2.11

Матриця керування доступом

О1	О2	О3	О4	О5	О6	О7	О8	О9
Ч,З,Д,ЗМ,ЗН,К	Ч,З, Д	Ч,З,Д,ЗМ,ЗН,К	Ч,З,Д,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗМ,ЗН	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ	Ч,З,Д,К,ЗН,ЗМ
-	Ч,З,Д	Ч,З,Д,	-	Ч,К	-	Ч,З,Д,К,ЗН	Ч,З,Д,К,ЗН,ЗМ	Ч,З,К,Д,ЗМ,ЗМ
-	-	Ч,З,Д,	Ч,З,Д,ЗН,ЗМ	Ч,З,Д,К	-	Ч,З,Д,К,ЗН,ЗМ	-	-
-	-	-	-	Ч,З	-	Ч,З,К,Д	Ч,З,Д,К	Ч,З,Д,К
О10	О11	О12	О13	О14	О15	О16	О17	О18
Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,З,ЗМ,ЗН	Ч,З,К,Д	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН
Ч,З,К,Д,З	Ч,З,К,Д	-	-	-	-	-	Ч,З,К,Д,ЗМ,ЗН	-
-	-	Ч,З,К,Д	-	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ
-	Ч,З,К,Д	-	Ч,З,К,Д,ЗМ,ЗН	-	-	-	-	-

Продовження табл 2.11

О19	О20	О21	О22	О23	О24	О25	О26	О27
Ч,З,К,Д,ЗМ,ЗН	Ч,З,Д,К,	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ
Ч,З,К,Д	Ч,З,Д,К	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ	Ч,З,К,Д,ЗМ
Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д	-	-	-	-	-	-
Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д	-	-	-	Ч,З,К,Д,ЗМ	Ч,З,К,Д	Ч,З,К,Д
О28	О29	О30						
Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН	Ч,З,К,Д,ЗМ,ЗН						
Ч,З,К,Д,ЗМ	Ч,З,К,Д	Ч,З,К,Д						
-	-	-						
О28	О29	О30						
Ч,З,К,Д	Ч,З,К,Д	Ч,З,К,Д						

Позначення:

Суб’єкти доступу:

S1 – директор;

S2 – системний адміністратор;S3 – бухгалтер;

S4 – диспетчер;

Об’єкти доступу:

O1 – організаційно-розпорядча документація;

O2 – облік внутрішніх документів (накази, службові записки, інструкції);

O3 – інформація про надання послуг, тарифи, контактна інформація підприємства;

O4 – Інформація про робітників;

O5 – Статутні документи підприємства (документи, що дозволяють займатися підприємницькою діяльністю);

O6 – Облік та реєстрація вхідних та вихідних документів організації;O7 – Трудові договори робітників;

O8 – Договори про надання послуг клієнтам;O9 – База даних клієнтів;

O10 – Заявки на підключення обладнання;

O11 – Акти прийому виконаних спеціалістом з монтажу робіт;O12 – Дані про лицьові рахунки замовників;

O13 – Заявки на розірвання договору про надання послуг;O14 – Відомості про фінанси підприємства;

O15 – Плани закупівель;

O16 – Відомості постачальників;

O17 – Зміст та характер договорів, контрактів однією із сторін яких виступає підприємство;

O18 – База вхідних цін;

O19 – Коди програмного обладнання;O20 – Інформація по ліцензійне ПО;

O21 – Повна характеристика комп’ютерної техніки (серійний номер, заводський номер і т.д.);

O22 – Звіт про виконання ремонтних послуг офісної техніки;

О23 – База даних клієнтів;

О24 – Відомості про дату заключення договору між клієнтом та підприємством;

О25 – Відомості про створення сертифіката клієнта;

О26 – Відомості про генерацію ключів ЕЦП, формування сертифікатів відкритих ключів ключей ЕЦП;

О27 – Відомості про надання послуг приватним підприємствам;

О28 – Відомості про надання послуг державним підприємствам;

О29 – Формування та ведення реєстра форм звітних документів;

О30 – Формування та відправка пакетів звітності в електронному вигляді по електронній пошті з використання криптографічного захисту.

Операції з файлами:

Ч – читання;

З – зберігання;

Д – друкування;

К – копіювання;

Зн – знищення;

Зм – змінення.

Критерії впровадження системи. В результаті проведеного аналізу загроз та вразливостей підприємства, був обраний профіль захищеності (опис послуг безпеки наведено у табл. 2.12, критерії захищеності в табл. 2.13): 3.КЦД.1 = { КД-2, КО-1, КВ-1,ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Таблиця 3.12

Профіль захищеності ІТС

Критерії	**Послуги безпеки**	**Вимоги до рівнів послуг безпеки**
	1	**2**
Конфіденційності	Довірча конфіденційність	КД-2 (базова довірча конфіденційність)
	Повторне використанняоб'єктів	КО-1 (повторне використанняоб'єктів)
	Конфіденційність приобміні	КВ-1(мінімальна конфіденційністьпри обміні)
Цілісності	Довірча цілісність	ЦД-1 (мінімальна довірча цілісність)
	Відкат	ЦО-1 (обмежений відкат)
	Цілісність при обміні	ЦВ-1 (мінімальна цілісність приобміні)
Доступності	Використання ресурсів	ДР-1 (квоти)
	Відновлення після збоїв	ДВ-1 (ручне відновлення)
Спостережності	Реєстрація	НР-2 (захищений журнал)
	Ідентифікація і автентифікація	НИ-2 (одиночна ідентифікація і автентифікація)
	Цілісність комплексузасобів захисту	НЦ-2 (КЗЗ з гарантованою цілісністю)
	Самотестування	НТ-2 (самотестування при старті)
	Ідентифікація і автентифікація при обміні	НВ-1(автентифікація вузла)

Таблиця 3.13

Критерії захищеності

Критерії захищеності	**Чим реалізуються до впровадження політики безпеки**	**Чим реалізуються після впровадження політики безпеки**
КД-2	Розмежування прав доступу за допомогою Active Directory	Розмежування прав доступу за допомогою Active Directory
КО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
КВ-1	Використання протоколу SSL	Використання протоколу SSL
ЦД-1	Розмежування прав доступу за допомогою Active Directory	Розмежування прав доступу за допомогою Active Directory
ЦО-1	Вбудовані засоби Windows	Вбудовані засоби Windows
ЦВ-1	-	Використання засобів криптозахисту
ДР-1	Вбудовані засоби Windows	Вбудовані засоби Windows
НР-2	Вбудований журнал реєстрації Windows	Вбудований журнал реєстрації Windows
НИ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НК-1	-	Мережевий протокол автентифікації
НО-2	-	Призначення адміністратора безпеки
НЦ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НТ-2	Вбудовані засоби Windows	Вбудовані засоби Windows
НВ-1	-	Мережевий протокол автентифікації

Наведемо коротку характеристику змісту різних видів послуг.

Базова довірча конфіденційність (КД-2)

Послуга використовується для обмеження доступу користувачів до захищених об'єктів і дозволяє користувачеві контролювати потік інформації в

операційній системі від захищених об'єктів, що належать до їхнього домену, іншим користувачам.

Декларація про захист даних поширюється на об'єкти та гарантує взаємодію таких об'єктів:

- користувачі всіх категорій;

- об'єкти, що містять конфіденційну інформацію, за умови, що групи користувачів, що мають однакові повноваження щодо цієї інформації, ідентифіковані в UA та лише в межах цих груп;

- всі інші об'єкти, що потребують захисту, які не належать до зазначених вище типів.

Декларація про захист даних CRP застосовується до об’єктів, які користувач створює в процесі своєї роботи.

Послуга використовується для обмеження доступу користувачів до захищених об'єктів і дозволяє користувачеві контролювати потік інформації в операційній системі від захищених об'єктів, що належать до їхнього домену, іншим користувачам.

Декларація про захист даних поширюється на об'єкти та гарантує взаємодію таких об'єктів:

- користувачі всіх категорій;

- об'єкти, що містять конфіденційну інформацію, за умови, що групи користувачів, що мають однакові повноваження щодо цієї інформації, ідентифіковані в UA та лише в межах цих груп;

- всі інші об'єкти, що потребують захисту, які не належать до зазначених вище типів.

Декларація про захист даних CRP застосовується до об’єктів, які користувач створює в процесі своєї роботи.

КЗЗ реалізує обмеження доступу на основі атрибутів доступу користувача та захищеного об'єкта.

Запити на зміну прав доступу до об’єкта обробляються КЗЗ на основі атрибутів доступу запитуючого користувача та об’єкта.

КЗЗ повинен надати користувачеві, як власнику процесу, можливість ідентифікувати певних користувачів та / або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні бути встановлені під час створення або ініціалізації. реалізує обмеження доступу на основі атрибутів доступу користувача та захищеного об'єкта.

Запити на зміну прав доступу до об’єкта обробляються CPD на основі атрибутів доступу запитуючого користувача та об’єкта.

КЗЗ повинен надати користувачеві, як власнику процесу, можливість ідентифікувати певних користувачів та / або групи користувачів, які мають право ініціювати цей процес.

Права доступу до кожного захищеного об'єкта повинні бути встановлені під час створення або ініціалізації.

Повторне використання об’єктів (КО-1). Послуга дозволяє забезпечити правильне повторне використання спільних об'єктів, забезпечуючи, що спільний об'єкт, коли він присвоєний новому користувачеві або процесу, не містить залишкової інформації від його використання користувачем або процесом.

Політика повторного використання об'єктів, що реалізується КЗЗ, стосується тільки тих об'єктів ЛОМ, які містять конфіденційну інформацію і ресурси яких поділяються між користувачами ЛОМ та прикладними процесами, що виконуються в ЛОМ.

Вимоги цієї послуги поширюються на сегменти оперативної пам'яті робочих станцій та серверів (усіх без виключення типів) та носії інформації на жорстких магнітних дисках (ЖМД), якими укомплектовані робочі станції й сервери, і використовуються системними та функціональними процесами під час оброблення конфіденційної інформації, а також на окремі види периферійних пристроїв, які мають власну пам’ять і задіяні під час експорту (імпорту) конфіденційної інформації з (в) ЛОМ та створенні «твердих» копій тощо.

Перш ніж користувач або процес може отримати об'єкт, яким користується інший користувач або процес, права, надані попередньому користувачеві або процесу на цей об'єкт, повинні бути скасовані.

Перш ніж користувач або процес може отримати об’єкт, опублікований іншим користувачем або процесом, інформація в цьому об’єкті більше не повинна бути доступною.

Вимога до цієї послуги повністю стосується процесів, які одночасно використовуються декількома користувачами.

Мінімальна конфіденційність при обміні (КВ-1):

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься;

– політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності;

– КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається.

Мінімальна довірча цілісність (ЦД-1)

Послуга використовується для захисту обробленої інформації від несанкціонованих модифікацій і дозволяє користувачеві будь-якої категорії контролювати потік інформації від інших користувачів з метою захисту об'єктів, що належать до його домену.

Політика довірливої доброчесності, реалізована КЗЗ, поширюється на слабо та міцно пов’язані об’єкти, які створюються користувачем під час виконання його функціональних функцій. Користувач, який створив об'єкт, має право визначати конкретних користувачів та / або групи користувачів, які мають право змінювати цей об'єкт.

КЗЗ повинен розрізняти доступ на основі атрибутів доступу користувача та захищеного об'єкта.

Запити на зміну прав доступу до об’єкта обробляються КЗЗ на основі

атрибутів доступу запитуючого користувача та об’єкта.

Права доступу до кожного захищеного об'єкта повинні бути встановлені під час створення або ініціалізації.

Обмежений відкат (ЦО-1)

Послуга пропонує можливість скасування однієї операції або послідовності операцій і переведення захищеного об'єкта, яким користувач маніпулює, у попередньо визначений стан.

Обмежена політика відновлення гарантує взаємодію наступних об'єктів і застосовується до:

- користувачі всіх категорій;

- сильно і слабо пов’язані об’єкти, що містять в обробці конфіденційну інформацію, можливість якої може бути змінена користувачем, а також технологічну інформацію від КЗСІ.

Компоненти КЗЗ повинні мати автоматизовані засоби, які дозволяють уповноваженому користувачеві або процесу скасувати або скасувати ряд операцій, які вже були виконані над захищеним об'єктом протягом певного періоду часу.

Той факт, що користувач користується послугою, повинен бути записаний в системний журнал. Скасування процесу не призводить до видалення згодом скасованого запису даних транзакції, якщо це було записано відповідно до вимог служби безпеки.

Мінімальна цілісність при обміні (ЦВ-1)

Ця послуга допомагає захистити об'єкти від несанкціонованих змін інформації, яку вони містять, коли вони експортуються / імпортуються через незахищене середовище. У більшості випадків ця послуга реалізується з використанням механізмів криптографічного захисту, таких як цифрові підписи та коди автентифікації повідомлень. Рівні цієї послуги класифікуються відповідно до повноти захисту та вибірковості управління. Повний захист, як послуга конфіденційності біржі, слід розуміти як сукупність типів загроз, проти яких забезпечується захист. Під ступенем безпеки експортованих об'єктів

загалом розуміють криптографічну стабільність використовуваних алгоритмів шифрування.

Використання ресурсів (ДР-1)

Послуга дозволяє управляти використанням сервісів та ресурсів користувачами.

Політика використання ресурсів, реалізована КЗЗ, поширюється на наступні об'єкти та передбачає взаємодію цих об'єктів, пропонуючи можливість обмеження їх використання користувачами всіх категорій.

Обмеження на використання одного користувача та / або процесу щодо обсягу обчислювальних ресурсів АС або кількості об'єктів встановлюються адміністратором безпеки або користувачами, уповноваженими іншими адміністраторами. Запити на зміну обмежень повинні оброблятися КЗЗ, лише якщо вони надходять від адміністраторів.

Спроби користувачів перевищити обмеження ресурсів слід реєструвати.

Ручне відновлення після збоїв (ДВ-1)

Політика відновлення після збоїв, що реалізується КЗЗ, поширюється на нижчезазначені об’єкти та забезпечує їх взаємодію:

– системне та функціональне ПЗ;

– засоби захисту інформації та засоби управління КСЗІ;

– засоби адміністрування та управління обчислювальною системою;

– окремі периферійні пристрої (принтери, накопичувачі інформації, змінні носії інформації і т.і.), які задіяні для обробки конфіденційної інформації.

Послуга гарантує повернення гучномовця до відомого захищеного стану після збоїв або перебоїв у службі, спричинених неправильними діями користувача, які не спричинені несправністю програмного та апаратного забезпечення (наприклад, виявленими під час будівництва), іншими непередбаченими ситуаціями.

Політика відновлення після катастрофи повинна визначати та документувати безліч видів збоїв та перебоїв в обслуговуванні локальної

мережі або окремих її компонентів, після чого можна повернутися до відомого захищеного стану, не порушуючи політики безпеки. Рівні помилок, які слід перевищити, повинні бути чітко визначені для кожної помилки.

Переінсталюйте автоматизовану систему.

Повернення АС (окремих компонентів) з режиму, визначеного погіршеними експлуатаційними характеристиками, у нормальний режим роботи повинно здійснюватися за допомогою ручних (не автоматизованих) процедур.

Захищений журнал (НР-2)

Послуга реєстрації рівня НР-2 дозволяє контролювати небезпечні для АС дії зі сторони користувачів будь-яких категорій відносно процесів і об'єктів.

Політика реєстрації поширюється та забезпечує взаємодію користувачів усіх категорій.

КЗЗ повинен забезпечувати реєстрацію всіх подій, які мають безпосереднє відношення до його безпеки. До таких відносяться наступні класи подій:

– вхід/вихід або намагання входу/виходу в/із системи користувачів будь-яких категорій;

– реєстрація та видалення або намагання реєстрації та видалення користувачів будь-якої категорії із системи;

– зміна паролю користувачем будь-якої категорії;

– отримання або намагання отримання доступу користувачем будь-якої категорії до будь-яких процесів і об'єктів АС, що мають ступінь обмеження доступу на рівні конфіденційної інформації;

– виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на призначений для цього пристрій друку, або намагання виведення користувачем будь-якої категорії документа або інформації конфіденційного характеру на пристрій друку;

– копіювання записів із конфіденційною інформацією на пристрої зберігання даних, що використовують знімні носії, які можуть записувати

інформацію та спеціально призначені для операцій копіювання, або спроби копіювати конфіденційну інформацію на пристрої зберігання даних, що відповідають безпеці, для цього не призначені;

– виявлення і реєстрація фактів порушення цілісності КЗЗ;

– інші події, обов’язковість реєстрації яких передбачена політикою реалізації окремих послуг безпеки інформації.

Реєстрація всіх подій, що мають безпосереднє відношення до безпеки, здійснюється в журналі реєстрації, який містить інформацію щодо дати, часу, місця (адреси робочої станції в АС), імені користувача, типу й успішності чи неуспішності кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію достатню для однозначної ідентифікації робочої станції, користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події.

Адміністратор безпеки і користувачі, яким надано повноваження інших адміністраторів, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації, а КЗЗ повинен забезпечувати захист журналу реєстрації від НСД, модифікації або руйнування.

Одиночна ідентифікація та автентифікація (НИ-2**)**

Ідентифікація та автентифікація дозволяють визначити й перевірити особу користувача будь-якої категорії, що намагається одержати доступ до АС або до захищених об’єктів, та повинні гарантувати, що доступ може бути надано тільки авторизованому користувачу.

Політика ідентифікації та автентифікації поширюється на нижчезазначені об’єкти і забезпечує їх взаємодію .

Кожний користувач, що отримує доступ до АС, повинен ідентифікуватися КЗЗ на підставі присвоєного йому імені. Дозвіл на виконання будь-яких дій, що контролюються КЗЗ, користувач отримує тільки після автентифікації його КЗЗ на підставі введеного ним пароля.

Механізм реалізації послуги повинен відповідати умовам надійного та однозначного виконання ідентифікації та автентифікації.

КЗЗ повинен забезпечувати захист даних автентифікації від НСД, модифікації або руйнування.

Однонаправлений достовірний канал (НК-1)

Послуга повинна гарантувати користувачу будь-якої категорії можливість безпосередньої взаємодії з КЗЗ, а також те, що ніяка взаємодія користувача з ЛОМ не може бути модифікованою іншим користувачем або процесом. Послуга повинна визначати вимоги до механізму встановлення достовірного зв'язку між користувачем і КЗЗ.

Політика достовірного каналу поширюється на користувачів усіх категорій, окремі компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ, і забезпечує взаємодію зазначених об’єктів.

Для початкової ідентифікації та автентифікації слід використовувати дійсний канал. Зв'язок із використанням цього каналу може ініціювати лише користувач.

Розподіл обов’язків адміністраторів (НО-2)

Послуга дає змогу диференціювати повноваження користувачів, визначаючи категорії користувачів із конкретними та конкретними функціями для кожної з категорій. Послуга призначена для зменшення потенційних втрат від навмисних чи некоректних дій користувачів та обмеження авторитарного керування АС.

Політика розподілу відповідальності, запроваджена КЗЗ, застосовується до користувачів усіх категорій і повинна визначати принаймні такі ролі:

- адміністратор безпеки;

- принаймні ще один адміністратор (адміністратор бази даних, адміністратор мережевих пристроїв, адміністратор служби тощо);

- Користувачі, яким надано доступ до конфіденційної інформації.

Ролі адміністратора можуть дублювати уповноважені користувачі. Кількість таких користувачів повинна бути мінімальною.

Адміністратор безпеки повинен мати доступ до технологічної інформації КСЗІ, а також до системи та функціонального програмного забезпечення, що

реалізує механізми захисту. Інший адміністратор повинен мати доступ до технологічної інформації про управління автоматизованою системою та системою та функціональним програмним забезпеченням, що реалізує ці функції. Всім іншим користувачам не слід дозволяти доступ до цих об’єктів.

Адміністраторам слід забороняти доступ до об'єктів, що містять конфіденційну інформацію, що мають суттєву та вільну зв'язок, якщо їх функціональна відповідальність не включає поєднання адміністративної та конфіденційної інформації.

КЗЗ з гарантованою цілісністю (НЦ-2)

Дана послуга визначає міру спроможності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

Для рівня НЦ-2 необхідно, щоб КЗЗ підтримував власний домен виконання, відмінний від доменів виконання всіх інших процесів, захищаючи себе від зовнішніх впливів. Дана вимога є однією з вимог до реалізації диспетчера доступу. Як правило, реалізація даної вимоги повинна забезпечуватися можливостями апаратного забезпечення ОС.

Самотестування при старті (НТ-2**)**

Самотестування дозволяє КЗЗ перевірити й на підставі цього гарантувати правильність функціонування і цілісність множини функцій ЛОМ, що забезпечуються захистом.

Політика самотестування поширюється на нижчезазначені об’єкти і забезпечує їх взаємодію:

– адміністратора безпеки;

– компоненти системного та функціонального ПЗ, які задіяні для реалізації механізмів КЗЗ;

– засоби захисту інформації, а також технологічну інформацію КСЗІ.

До складу КЗЗ повинен входити набір тестових процедур, достатній для оцінки правильності виконання в ЛОМ всіх критичних для безпеки конфіденційної інформації та технологічної інформації КСЗІ функцій, а сам КЗЗ повинен бути здатним контролювати їх виконання.

Тести повинні виконуватися при ініціалізації КЗЗ за запитом адміністратора безпеки.

У разі неправильного виконання одного з тестів, КЗЗ повинен передати АС до стану, в якому обробка конфіденційної інформації загалом заборонена, або до стану, в якому обробка конфіденційної інформації заборонена, тест не проводити заборонено. Тільки адміністратор безпеки може повернути гучномовець до нормальної роботи після відновлення КЗЗ і повторення всіх тестів.

Автентифікація вузла (НВ-1)

Ця послуга допомагає захистити об'єкти від несанкціонованих змін інформації, яку вони містять, коли вони експортуються / імпортуються через незахищене середовище. У більшості випадків ця послуга реалізується з використанням криптографічних механізмів захисту, таких як цифрові підписи та коди автентифікації повідомлень. Включення цього рівня у вашу оцінку може кваліфікуватися як система, що дозволяє перевірити цілісність комп'ютерного програмного забезпечення за допомогою цифрових підписів, або як система електронних повідомлень, що забезпечує цифровий підпис повідомлень.

2.4 Розробка політики безпеки для підприємства

При розробці політики безпеки для підприємства, спираючись на наявність конфіденційної інформації, яка обробляється в ІТС, фінансових та матеріальних ресурсів, які є у розпорядженні власника ІТС, обрано принцип, при якому впровадження інформаційного захисту буде доцільним - досягнення необхідного рівня захищеності інформації за мінімальних затрат і допустимого рівня обмежень на технологію її обробки в ІТС.

Заходи, що представлені в політиці інформаційної безпеки, направлені на зниження ризиків реалізації загрози через вразливості ІТС, спираючись на існуючий аналіз ризиків.

Політика безпеки для системного адміністратора включає в себе інструкції для системного адміністратора, йогообов’язки та права включає:

1 Опис:

Політика включає в себе інструкції для системного адміністратора, його обов’язки та права.

2 Метою цієї політики захист підприємства від витоку та несанкціонованого доступу до інформації.

3 Галузь застосування:

Ця політика відноситься до системного адміністратора, хто єко

4 Інструкція політики

I. Загальні положення:

1. Системний адміністратор відноситься до категорії фахівців.

2. На посаду системного адміністратора призначається особа, яка має профільне професійну освіту, досвід технічного обслуговування і ремонту персональних комп'ютерів і оргтехніки, знає основи локальних мереж (стек протоколів TCP / IP, мережеве обладнання, принципи побудови локальних обчислювальних мереж).

3. Системний адміністратор повинен знати:

1 Технічні характеристики, призначення, режими роботи, конструктивні особливості, технічні правила експлуатації обладнання ЛВС, офісного обладнання, серверів та персональних комп’ютерів.

2 Апаратне та програмне забезпечення локальної мережі.

3 Принципи ремонту персональних комп’ютерів та оргтехніки.

4 Мови програмування та методи.

5 Основи інформаційної безпеки, засоби захисту інформації від несанкціонованого доступу, пошкодження або навмисного спотворення.

6 Порядок оформлення технічної документації.

7 Норми внутрішнього трудового законодавства.

8 Основи трудового права.

9 Норми та норми охорони праці, охорони та пожежної охорони.

10 1 Призначення системним адміністратором та звільнення здійснюються за розпорядженням директора.

11 2 Системний адміністратор підпорядковується безпосередньо директору Sirius.

II. Завдання системного адміністратора:

Системний адміністратор:

1 Встановлює необхідні операційні системи та програмне забезпечення на сервери та робочі станції.

2 Розробляє конфігурацію програмного забезпечення на серверах та робочих станціях.

3 Утримує програмне забезпечення сервера та робочої станції у належному стані.

4 Реєструє користувачів локальної мережі та поштового сервера, призначає імена користувачів та паролі.

5 Розробляє технічну та програмну підтримку для користувачів, консультує користувачів щодо роботи локальних мереж та програм, створює інструкції щодо використання програмного забезпечення та робить їх відомими користувачам.

6 Визначає права доступу та контролює використання мережевих ресурсів.

7 Забезпечує копіювання, архівування та резервне копіювання даних у режимі реального часу.

8 Вживає заходів для відновлення функціональних можливостей локальної мережі у разі несправності або несправності мережевих пристроїв.

9 Виявляє помилки користувача та програмне забезпечення та вживає заходів для їх виправлення.

10 Моніторить мережу, вносить пропозиції щодо розвитку мережевої інфраструктури.

11 Гарантує безпеку мережі (захист від несанкціонованого доступу до інформації, перегляд або зміну системних файлів і даних) та безпеку з'єднання.

12 Розробляє захист від вірусів для локальних мереж, серверів та робочих станцій.

13 Готує пропозиції щодо модернізації та придбання мережевого обладнання.

14 Контролює встановлення пристроїв локальної мережі сторонніми постачальниками.

15 Інформує свого керівника про випадки порушення правил користування локальною мережею та вжиті заходи.

16 Повинен відвідувати курси підвищення кваліфікації принаймні двічі протягом 6 місяців.

II. Права системного адміністратора:

Системний адміністратор має право:

1 Встановлювати і змінювати правила користування локальною обчислювальною мережею.

2 Знайомитися з документами, що визначають його права та обов'язкиза займаною посадою, критерії оцінки якості виконання посадових обов'язків.

3 Вносити на розгляд керівництва пропозиції щодо вдосконалення роботи, пов'язаної з передбаченими цією посадовою інструкцією обов'язками.

4 Вимагати від керівництва забезпечення організаційно - технічних умов, необхідних для виконання посадових обов'язків.

III. Відповідальність системного адміністратора:

1 Системний адміністратор несе відповідальність за:

Порушення функціонування локальної обчислювальної мережі, серверів і персональних комп'ютерів внаслідок неналежного виконання своїх посадових обов'язків.

Несвоєчасну реєстрацію користувачів локальної обчислювальної мережі і поштового сервера.

Несвоєчасне повідомлення керівництва про випадки порушення правил користування локальної обчислювальної мережею.

2 Системний адміністратор несе відповідальність:

За неналежне виконання або невиконання своїх посадових обов'язків.

За правопорушення, скоєні в процесі своєї діяльності.

За завдання матеріальної шкоди компанії.

Політика антивірусного захисту.

1 Опис

Політика включає в себе інструкції для користувачів із застосування антивірусного ПЗ.

2 Метою цієї політики захист системи від комп’ютерних вірусів.

3 Галузь застосування

Ця політика відноситься до всіх робітників підприємства, хто є користувачами системи.

4 Інструкція політики

Для директора: роботи

а) забезпечення вчасного отримання ПЗ для антивірусного захисту;

б) контроль за виконанням перевірки робочих станцій перед початком роботи

Для системного адміністратора:

а) вчасне встановлення антивірусного ПЗ та оновленняб)контроль за терміном дії ліцензії

в) контроль за виконанням перевірки робочих станцій перед початком роботи (за відсутності директора)

Для диспетчера та бухгалтера:

а) перевірка робочих станцій перед початком роботи

б) вчасно сповіщувати про некоректність роботи антивірусного ПЗ

в) завжди скануйте носії інформації та підозрілі файли або файли з невідомого джерела на наявність вірусів;

г) зберігайте резервні копії важливих даних в безпечному місці;

е) ніколи не завантажувати файли з невідомих чи підозрілих джерел; не

відкривайте невідомі вам файли, що прикріплені до електронної пошти від невідомого, підозрілого або ненадійного джерела. Видаляйте ці вкладення відразу, «подвійним видаленням», шляхом спорожнення кошика.

Політика чистого столу.

1 Опис

Дана політика визначає, в якому вигляді співробітники приватного підприємства повинні залишати свої робочі місця, коли вони залишають їх без нагляду або не використовують їх.

2 Метою даної політики є запобігання витоку або втрати інформації з обмеженим доступом

3 Галузь застосування

Вимоги даної політики поширюються на всіх співробітників підприємства.

4 Інструкція політики

– Співробітники зобов’язані забезпечувати збереження всієї інформації з обмеженим доступом у друкованому або електронному вигляді на своєму робочому місці, коли вони збираються покинути приміщення на короткий або тривалий проміжок часу.

– Персональні комп’ютери повинні бути заблоковані, якщо передбачається, що вони не будуть використовуватись деякий час.

– Персональні комп’ютери повинні бути повністю вимкнені в кінці робочого дня.

– Будь-яка інформація з обмеженим доступом повинна бути видалена з робочого місця і замкнена в ящику чи сейфі, коли стіл не зайнятий і в кінці робочого дня.

– Ключі, що використовуються для доступу до інформації з обмеженим доступом, не можна залишати без нагляду на столі.

– Паролі не можуть бути розміщені на комп’ютері, під ним або записанів нотатках.

– Інформація з обмеженим доступом, що була роздрукована, повинна

бути негайно видалена з принтера.

– Інформація, що підлягає знищенню, повинна бути утилізована за допомогою шредера якнайшвидше.

5. Відповідальність

– Кожен співробітник повинен дотримуватись вимог даної політики.

– Відповідальність за виконання співробітниками вимог даної політикинесе директор.

– Співробітники, що порушили дану політику, несуть відповідальність відповідно до внутрішніх нормативних документів підприємства.

2.5 Висновки до розділу 2

Наведені загальні відомості про приватне підприємство, обґрунтуване необхідность створення КСЗІ, Проаналізовано загрози інформації, що циркулює на ОІД, Розроблено політику безпеки для підприємства,В даному розділі розроблене технічне завдання для Системи комплексного захисту інформації на підприємстві на прикладі охоронної фірми «Сіріус».

ВИСНОВКИ

В рамках кваліфікаційної роботи було проаналізовано поточні загрози інформаційній безпеці в Україні, сформульовано мету та принципи формування політики безпеки та досліджено поточну ситуацію в Україні щодо інформаційної безпеки, законодавчу базу в галузі захисту інформації.

На основі аналізу умов функціювання, інформаційно-телекомунікаційної системи приватної компанії "Сіріус" розроблено моделі загроз та злочинців, та керівні принципи інформаційної безпеки інформаційно-телекомунікаційної системи цього відділу, зокрема

- політика чистого столу;
- політика безпеки для системного адміністратора;
- вказівки щодо захисту від вірусів.

Всі ці рішення спрямовані на зменшення ймовірності зараження шкідливим програмним забезпеченням на ПК, крадіжки та самостійного використання документів, які можуть бути залишені без нагляду та знищення, а також заборони доступу в уповноваженому користувачеві АС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. ДСТУ 3396.1-96 - Технічний захист інформації. Порядок проведення робіт; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=38911&cat_id=38836;

2. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80;

3. Закон України «Про захист персональних даних»; [Електронний ресурс] –Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17;

4. Закон України "Про інформацію" [Електронний ресурс]. – 101. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12;

5. НД ТЗІ 1.1-002-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106340;

6. НД ТЗІ 1.1-003-99 - Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу; [Електронний ресурс]– Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835;

7. НД ТЗІ 1.1-005-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102310&cat_id=46556&ctime=1344511142755;

8. НД ТЗІ 1.4-001-00 - Типове положення про службу захисту

інформації в АС; [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106341;

9. НД ТЗІ 1.6-005-13 - Положення про категорювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=107993&cat_id=89734&ctime=1366373635138;

10. НД ТЗІ 2.5-004- Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу; [Електронний ресурс] – Режим доступу до ресурсу: dsszzi.gov.ua/dsszzi/doccatalog/document?id=106342;

11. НД ТЗІ 2.5-005-99 - Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу; [Електронний ресурс] – Режим доступу до ресурсу: lib.univd.edu.ua/?controller=service&action;

12. НД ТЗІ 3.1-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Передпроектні роботи; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102310&cat_id=46556&ctime=1344511142755;

13. НД ТЗІ 3.3-001-07 - Захист інформації на об’єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Порядок розроблення та впровадження заходів із захисту інформації; [Електронний ресурс] – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=102265&cat_id=46556&ctime=1344504841243;

14. НД ТЗІ 3.7-001-99 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 – Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі; [Електронний ресурс] – Режим доступу до ресурсу:

www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106350;

15. НД ТЗІ 3.7-003 -05 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 - Порядок проведення робіт із створення КСЗІ в ІТС; [Електронний ресурс] – Режим доступу до ресурсу: https://pda.litres.ru/vadim-grebennikov-15/kompleksni-sistemi-zahistu-informaciyi-proektuvannya/chitat-onlayn/page-2;

16. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.99 р. №1229; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1229/99;

17. Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373; [Електронний ресурс] – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF;

18. ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» [Електронний ресурс] – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106343;

19. Вимоги до системи захисту інформації [Електронний ресурс] – Режим доступу до ресурсу: https://studfiles.net/preview/6012701/page:6/;

20. Проблеми та шляхи розвитку інформатизації в Україні [Електронний ресурс] – Режим доступу до ресурсу: https://studopedia.info/1-112574.html.

21. Бондарчук Ю.В., Марущак А.І. Безпека бізнесу: організаційно-правові основи : науково-практичний посібник. Київ : Видавничий дім «Скіф», 2008. 369 с.

22. Гринь А.К. Управління та організація служби захисту інформації : навчальний посібник. Київ : НА СБ України, 2010. 75 с.