МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ Скарга-Бандурова І.С.
«____»_____ 20__ р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Розробка політики безпеки розподіленої ІКС із відкритою архітектурою

Освітньо-кваліфікаційний рівень "бакалавр"

Керівник проекту: _____ (підпис) Скарга-Бандурова І.С. (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Критська Я.О. (ініціали, прізвище)

Студент: _____ (підпис) Гончар А.О. (ініціали, прізвище)

Група: БІКС-13д

Сєвєродонецьк 2017

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерної інженерії
Освітньо-кваліфікаційний рівень Бакалавр
Напрям підготовки 6.170101 "Безпека інформаційних і комунікаційних систем"
(шифр і назва)
Спеціальність
(шифр і назва)

ЗАТВЕРДЖУЮ:

Завідувач кафедри
І.С. Скарга-Бандурова
«_____» _____20____р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) БАКАЛАВРА

Гончара Андрія Олександровича
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка політики безпеки розподіленої ІКС із відкритою Архітектурою

керівник проекту (роботи) Скарга-Бандурова Інна Сергіївна д.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "15" 05 2017 р. № 124/48
2. Термін подання студентом роботи 16.06.2017
3. Вихідні дані до роботи матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) основні терміни інформаційної безпеки, загрози інформаційної безпеки, планування та розробка політики інформаційної безпеки.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) комп'ютерна презентація

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада Консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	асистент кафедри КІ Критська Я.О.		

7. Дата видачі завдання _____

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Ознайомлення з темою диплому	До 1.05.2017	
2	Аналіз методик побудови СІБ	До 26.05.2017	
3	Розробка політики інформаційної безпеки	До 5.06.2017	
4	Розробка розділу «Охорона праці»	До 11.06.2017	
5	Оформлення пояснювальної записки та презентації	До 15.06.2017	

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник _____ _____
(підпис) (прізвище та ініціали)

Р Е Ф Е Р А Т

Пояснювальна записка до дипломного проекту (роботи) бакалавра: 96 с., 4 рис., 7 табл., 13 бібліографічних джерел посилань , _2_ додатків.

Об'єкт розробки: об’єктом розробки моєї дипломної роботи є політика інформаційної безпеки в розподілених ІКС з відкритою архітектурою.

Мета роботи: поглибити знання нормативно-правових документів які регулюють дії у сфері інформаційної безпеки, ознайомитися з методикою визначення ризиків ІКС та методикою розробки системи інформаційної безпеки.

В проекті виконано:

1 Визначені основні терміни з інформаційної безпеки та ознайомлення з нормативно-правовими документами які регулюють дії в цій сфері.

2 Було визначено об’єкт захисту, визначено типи і види загроз, джерела загроз, а також ознайомлення з методикою оцінки ризиків.

3 Ознайомлення з методикою розробки СІБ, визначення можливих збитків, заходів з захисту СІБ та їх документування.

4 Визначення вимог з охорони праці яких потрібно дотримуватия на підприємстві.

Отримано наступні результати: За результатами роботи отримано знання з правової організації СІБ та створено політику інформаційної безпеки.

Практичне значення, галузь застосування роботи: сфера інформаційної безпеки підприємств.

Ключові слова: політика, СІБ, загрози інформаційної безпеки

Умови одержання дипломного проекту: СНУ ім. В. Даля, пр. Центральний 59-А,. м. Сєвєродонецьк, 93400.

ЗМІСТ

ВСТУП

Розвитку сучасних інформаційних технологій значно опереджае темпи розвитку рекомендаційних і нормативно-правових документів.

Тому питання про створення ефективної політики інформаційної безпеки в сучасних організаціях обов'язково пов'язане з проблемою вибору показників захищеності, а також надійності системи захисту інформації.Внаслідок цього, разом з вимогамита рекомендаціями, стандартами, Конституцією, законамита іншими керівними документами доводиться використовувати міжнародні рекомендації. У тому числі застосовувати на практиці та адаптувати методики міжнародних стандартів, таких, як ISO 17799, ISO 9001, ISO 15408, BSI, COBIT, ITIL та інші, а також використовувати управління інформаційними системами в сукупності з оцінками економічної ефективності інвестицій в забезпечення захисту інформації організації. Сучасні методології управління інформаційною безпекою дозволяють розв’язати ряд завдань розвитку сучасних організацій.

По-перше, якісно та кількісно оцінити рівень інформаційної безпеки підприємства, що потребує виявлення ризиків натехнологічному, технічному, правовому,а такожорганізаційно-управлінському рівнях забезпечення захисту інформації.

По-друге розробити політику безпеки і плани покращення корпоративної системи захисту інформації для досягнення прийнятного рівня захищеності інформаційних ресурсів компанії. Для цього необхідно:

- обґрунтувати і провести розрахунок фінансових вкладень в забезпечення безпеки на основі технологій аналізу ризиків, співвіднести витрати на забезпечення безпеки з потенційним збитком і ймовірністю його виникнення;

- виявити і провести першочергове блокування найбільш небезпечних вразливостей до здійснення атак на вразливі ресурси;

- визначити функціональні відносини і зони відповідальності при взаємодії підрозділів і осіб щодо забезпечення інформаційної безпеки компанії, створити необхідний пакет організаційно-розпорядчої документації;

- розробити і узгодити з службами організації, наглядовими органами проект впровадження необхідних комплексів захисту, що враховує сучасний рівень і тенденції розвитку інформаційних технологій;

- забезпечити підтримку впровадження комплексу захисту відповідно до умов, що змінюються роботи організації, регулярними доробками організаційно-розпорядчої документації, модифікацією технологічних процесів і модернізацією технічних засобів захисту.

Рішення названих завдань відкриває нові широкі можливості перед посадовими особами різного рівня.

Керівникам верхньої ланки це допоможе об'єктивно і незалежно оцінити поточну рівень інформаційної безпеки компанії, забезпечити формування єдиної стратегії безпеки, розрахувати, узгодити і обгрунтувати необхідні витрати на захист компанії. На основі отриманої оцінки начальники відділів і служб зможуть виробити і обгрунтувати необхідні організаційні заходи (склад і структуру служби інформаційної безпеки, положення про комерційну таємницю, пакет посадових інструкцій та інструкції дії в нештатних ситуаціях). Менеджери середньої ланки зможуть обгрунтовано вибрати засоби захисту інформації, а також адаптувати і використовувати в своїй роботі кількісні показники оцінки інформаційної безпеки, методики оцінки та управління безпекою з прив'язкою до економічної ефективності компанії.

Практичні рекомендації по нейтралізації та локалізації виявлених вразливостей системи, отримані в результаті аналітичних досліджень, допоможуть в роботі над проблемами інформаційної безпеки на різних рівнях і, що особливо важливо, визначити основні зони відповідальності, в тому числі матеріальної, за неналежне використання інформаційних активів компанії. При визначенні масштабів матеріальної відповідальності за шкоду, заподіяну

роботодавцю, в тому числі розголошенням комерційної таємниці, слід керуватися відповідними положеннями Трудового кодексу

1 ОСНОВНІ ТЕРМІНИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Інформаційна безпека це стан збереження інформаційних ресурсів і захищеності законних прав особистості і суспільства в інформаційній сфері. Досягається це шляхом забезпечення конфіденційності, цілісності та доступності інформації.

- Конфіденційність: Забезпечення доступу до інформації тільки авторизованим користувачам.
- Цілісність: Забезпечення достовірності та повноти інформації та методів її обробки.
- Доступність: Забезпечення доступу до інформації та пов'язаним з нею активів авторизованих користувачів в міру необхідності. Виходячи з даної інформації, можна виділити інше визначення інформаційної безпеки. Інформаційна безпека - всі аспекти, пов'язані з визначенням, досягненням і підтримкою конфіденційності, цілісності, доступності, неспростовності, підзвітності, автентичності і достовірності інформації або засобів її обробки.

Безпека інформації визначається відсутністю недопустимого ризику, пов'язаного з витоком інформації технічними каналами, несанкціонованими і ненавмисними діями на дані і (або) на інші ресурси автоматизованої інформаційної системи, що використовуються в автоматизованій системі.

Загрози інформаційної безпеки - сукупність умов і факторів, що створюють потенційну або реально існуючу небезпеку порушення безпеки інформації. Атакою називається спроба реалізації загрози, а той, хто робить таку спробу, - зловмисником. Потенційні зловмисники називаються джерелами загрози.

Загроза є наслідком наявності вразливих місць або вразливостей в інформаційній системі. Уразливості можуть виникати з різних причин, наприклад, в результаті ненавмисних помилок програмістів при написанні програм.

Загрози можна класифікувати за кількома критеріями:

a) за властивостями інформації (доступність, цілісність, конфіденційність), проти яких загрози спрямовані в першу чергу;

b) за компонентами інформаційних систем, на які загрози націлені (дані, програми, апаратура, що підтримує інфраструктура);

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

d) по розташуванню джерела загроз (всередині / поза даної ІС).

Забезпечення інформаційної безпеки є складним завданням, для вирішення якої потрібне комплексний підхід. Виділяють такі рівні захисту інформації:

- законодавчий - закони, нормативні акти та інші документи РФ і міжнародного співтовариства;
- адміністративний - комплекс заходів, що вживаються локально керівництвом організації;
- процедурний рівень - заходи безпеки, що реалізуються людьми;
- програмно-технічний рівень - безпосередньо засоби захисту інформації.

Законодавчий рівень є основою для побудови системи захисту інформації, так як дає базові поняття предметної області і визначає міру покарання для потенційних зловмисників. Цей рівень відіграє координуючу і спрямовуючу роль і допомагає підтримувати в суспільстві негативний (і каральне) ставлення до людей, які порушують інформаційну безпеку.

Політика ІБ є адміністративним рівнем захисту інформації, і в кожної організації вона буде відрізнятися в залежності від рівня загроз, конкурентності та секретності інформації.

1.1 Нормативно-правові акти про інформаційну безпеку в Україні

В Україні ІБ регламентуется такими нормативно-правовими актами:

а) Закони України:

1) Закон України «Про інформацію» від 02.10.1992 № 2657-XII
2) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР
3) Закон України «Про державну таємницю» від 21.01.1994 № 3855-XII
4) Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI

б) Постанови КМУ:

1) Постанова Кабінету міністрів України «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 №373
2) Постанова Кабінету міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять службову інформацію» від 27 листопада 1998 р. №1893

в) Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ:

1) НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі
2) Державний стандарт України. Захист інформації. Технічний захист інформації. Порядок проведення робіт. ДСТУ 3396.1-96

3) НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі
4) НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу
5) НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу
6) НД ТЗІ 2.5-008-02 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2
7) НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу
8) НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі
9) НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп’ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу
10) Автоматизированные системы. Требования к содержанию документов РД 50-34.698
11) Техническое задание на создание автоматизированной системы. ГОСТ 34.602-89
12) НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу

г) Галузеві стандарти:

13) ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD)

14) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010 Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

На даний момент ці нормативно-правові акти підходять для створення політики безпеки у державній організації, але для усіх інших вони не підходять. На це є декілька причин:

- Вимоги національних українських документів по інформаційній безпеці навіть по відношенню до конфіденційної інформації, яка не складає державну таємницю, дуже високі. Не обдумавши виконання всіх національних українських вимог до інформаційної безпеки по-перше дуже сильно і необґрунтовано збільшить бюджет, що витрачається на інформаційну безпеку, по-друге дуже сильно ускладнить виконання бізнес-процесів.
- Вимоги національних українських документів з інформаційної безпеки часто застарілі і неактуальні.
- Вимоги національних українських документів з інформаційної безпеки орієнтовані в першу чергу на державні структури.

1.2 Міжнародні стандарти інформаційної безпеки

ISO 27000 - один з найбільш прийнятних і поширених стандартів оцінки, що включає в себе більше 15 положень, і мають послідовну нумерацію.

Відповідно до критеріїв оцінки стандартизації ISO 27000, безпеку інформації - це не тільки її цілісність, конфіденційність і доступність, а також автентичність, надійність, відмовостійкість та ідентифікуємість. Умовно цю серію стандартів можна розділити на 4 розділи:

- огляд і введення в термінологію, опис термінів, що застосовуються в сфері забезпечення безпеки;

– обов'язкові вимоги до системи управління інформаційною безпекою, докладний опис методів і засобів управління системою. Є основним стандартом цієї групи;

– рекомендації для аудиту, керівництво по заходам забезпечення безпеки;

– стандарти, які рекомендують практики впровадження, розвитку та вдосконалення системи управління інформаційною безпекою.

В даний момент різні не державні організації використовують як раз міжнародні стандарти.

1.3 Політика інформаційної безпеки

Політика інформаційної безпеки - це сукупність правил, процедур, практичних методів і керівних принципів в області ІБ, використовуваних організацією в своїй діяльності. Іншими словами політика ІБ це не що інше як задокументовані система інформаційної безпеки підприємства

Згідно із стандартом ISO / IEC 17799-2005, політика інформаційної безпеки повинна встановлювати відповідальність керівництва, а також викладати підхід організації до управління інформаційною безпекою. Відповідно до зазначеного стандарту, необхідно, щоб політика інформаційної безпеки підприємства як мінімум включала:

- визначення інформаційної безпеки, її загальних цілей і сфери дії, а також розкриття значущості безпеки як інструменту, що забезпечує можливість спільного використання інформації;
- виклад цілей і принципів інформаційної безпеки, сформульованих керівництвом;
- короткий виклад найсуттєвіших для організації політик безпеки, принципів, правил і вимог, наприклад, таких як:

а) відповідність законодавчим вимогам та договірними зобов'язаннями;

б) вимоги щодо навчання питань безпеки;

в) запобігання появи і виявлення вірусів та іншого шкідливого програмного забезпечення;

г) управління безперервністю бізнесу;

д) відповідальність за порушення політики безпеки.

- визначення загальних і конкретних обов'язків співробітників в рамках управління інформаційною безпекою, включаючи інформування про інциденти порушення інформаційної безпеки;
- посилання на документи, що доповнюють політику інформаційної безпеки, наприклад, більш детальні політики та процедури для конкретних інформаційних систем, а також правила безпеки, яких повинні дотримуватися користувачі;

Політика інформаційної безпеки компанії повинна бути затверджена керівництвом, видана і доведена до відома всіх співробітників в доступній та зрозумілій формі.

Для того щоб політика інформаційної безпеки не залишалася тільки «на папері» необхідно, щоб вона була:

- несуперечлива - різні документи не повинні по різному описувати підходи до одного і того ж процесу обробки інформації;
- не забороняла необхідні дії - в такому випадку неминучі масові порушення приведуть до дискредитації політики інформаційної безпеки серед користувачів;
- не накладала нездійсненних обов'язків і вимог.

В організації повинна бути призначена особа, відповідальна за політику безпеки, що відповідає за її ефективну реалізацію і регулярний перегляд.

Як у кожного документу у політики ІБ є свої цілі та задачі. Основними цілями політики ІБ є:

- збереження конфіденційності критичних інформаційних ресурсів;

- забезпечення безперервності доступу до інформаційних ресурсів УЗ;
- захист цілісності інформації з метою підтримки можливості УЗ з надання послуг високої якості і прийняття ефективних управлінських рішень;
- підвищення обізнаності користувачів в області ризиків, пов'язаних з інформаційними ресурсами УЗ;
- визначення ступеня відповідальності і обов'язків співробітників із забезпечення інформаційної безпеки в управлінні;
- підвищення рівня ефективності, безперервності, контрольованості заходів щодо захисту від реальних загроз ІБ;
- запобігання і / або зниження шкоди від інцидентів ІБ;

Основні завданнями політики ІБ є:

- розробка вимог щодо забезпечення ІБ;
- контроль виконання встановлених вимог щодо забезпечення ІБ;
- підвищення ефективності, безперервності, контрольованості заходів по забезпеченню і підтримці ІБ;
- розробка нормативних документів для забезпечення ІБ УЗ;
- виявлення, оцінка, прогнозування і запобігання реалізації загроз ІБ УЗ;
- організація антивірусного захисту інформаційних ресурсів УЗ;
- захист інформації УЗ від несанкціонованого доступу (далі - НСД) і витоку технічними каналами зв'язку;
- організація періодичної перевірки дотримання інформаційної безпеки наступним поданням звіту за результатами зазначеної перевірки директору УЗ.

1.4 Постановка задачі

В цій дипломній роботі мені необхідно розробити політику інформаційної безпеки для розгорнутої ІКС з відкритою архітектурою. Для цього мені необхідно:

- визначити об’єкт захисту;
- визначити загрози та джерела загроз для об’єкту;
- скласти подель порушника ІБ;
- розробити СУІБ;
- визначити можливі збитки для об’єкта;
- скласти та задокументувати політику;

1.5 Висновки до розділу 1

В наш час важливо розуміти що інформація потребує захисту. Для цього і створюються системи інформаційної безпеки. Але щоб СІБ справно працювала кожен працівник повинен виконувати її вимоги. Тому і створюється політика інформаційної безпеки, та кожен працівник на підприємстві повинен бути ознайомлений з нею та неухильно дотримуватись.

Кожна організація володіє інформацією різного рівня, тому і політика інформаційної безпеки розробляється окроме для кожного випадку. Інакше може виники така ситуація, що компанія буде витрачати занадто багато грошей або СІБ буде слабкою.

2 ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

2.1 Визначення об’єкту захисту

Так як політика інформаційної безпеки розробляється окремо для кожного підприємства я буду розробляти політику для деякої Web-студії. В цій системі є 10 комп’ютерів, 2 сервери, WiFi-роутер.

Сервер підключений до інтернету, інший сервер та розтер приєднані послідовно до нього, комп’ютери підключені до інтернету та серверів через WiFi-роутер.

Основними об'єктами захисту системи інформаційної безпеки в студії є:

- інформаційні ресурси, що містять комерційну таємницю, персональні дані фізичних осіб, відомості обмеженого поширення, а також відкрито поширювана інформація, необхідна для роботи студії, незалежно від форми та виду її подання;
- інформаційні ресурси, що містять конфіденційну інформацію,
- співробітники Банку, які є розробниками і користувачами інформаційних систем Банку;
- інформаційна інфраструктура, що включає системи обробки і аналізу інформації, технічні та програмні засоби її обробки, передачі і відображення, в тому числі канали інформаційного обміну і телекомунікації, системи і засоби захисту інформації, об'єкти і приміщення, в яких розміщені такі системи.

2.2 Типи і види загроз

Загроза інформаційної безпеки - сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки.

Під загрозою (в загальному) розуміється потенційно можлива подія, дія (вплив), процес або явище, які можуть спричинити пошкодження чиїмось інтересам.

Під загрозою інтересам суб'єктів інформаційних відносин розуміють потенційно можлива подія, процес або явище яке за допомогою впливу на інформацію або інші компоненти інформаційної системи може прямо або побічно призвести до нанесення шкоди інтересам даних суб'єктів.

Загрози інформаційної безпеки можуть бути класифіковані за різними ознаками:

За аспекту інформаційної безпеки, на який спрямовані загрози:

Загрози конфіденційності (неправомірний доступ до інформації). Загроза порушення конфіденційності полягає в тому, що інформація стає відомою тому, хто не має в повноважень доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в обчислювальній системі чи переданої від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування того чи іншого користувачеві привілеїв іншого користувача), збоїв роботі програмних і апаратних засобів. До інформації обмеженого доступу належить державна таємниця і конфіденційна інформація (комерційна таємниця, персональні дані, професійні види таємниця: лікарська, адвокатська, банківська, службова, нотаріальна, таємниця страхування, слідства і судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця зв'язку), відомості про сутність винаходу, корисної моделі чи промислового зразка до офіційної публікації (ноу-хау) і ін.).

Загрози цілісності (неправомірне зміна даних). Загрози порушення цілісності - це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності

може бути викликано різними факторами - від навмисних дій персоналу до виходу з ладу обладнання.

Загрози доступності (здійснення дій, що унеможливлюють чи утруднюють доступ до ресурсів інформаційної системи). Порушення доступності є створення таких умов, при яких доступ до послуги або інформації буде або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.

По розташуванню джерела загроз:

- Внутрішні (джерела загроз розташовуються усередині системи);
- Зовнішні (джерела загроз знаходяться поза системою).

За розмірами завдається шкоди:

- Загальні (нанесення збитку об'єкту безпеки в цілому, заподіяння значної шкоди);
- Локальні (заподіяння шкоди окремим частинам об'єкта безпеки);
- Приватні (заподіяння шкоди окремим властивостям елементів об'єкта безпеки).

За ступенем впливу на інформаційну систему:

- Пасивні (структура і зміст системи не змінюються);
- Активні (структура і зміст системи піддається змінам).

За природою виникнення:

- Природні (об'єктивні) - викликані впливом на інформаційне середовище об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини;
- Штучні (суб'єктивні) - викликані впливом на інформаційну сферу людини. Серед штучних загроз в свою чергу виділяють:

    а) Ненавмисні (випадкові) загрози - помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної і комунікаційної техніки;

б) Навмисні (умисні) загрози - неправомірний доступ до інформації, розробка спеціального програмного забезпечення, використовуваного для здійснення незаконного втручання, розробка та поширення вірусних програм і т.д. Навмисні загрози обумовлені діями людей. Основні проблеми інформаційної безпеки пов'язані перш за все з навмисними погрозами, так як вони є головною причиною злочинів і правопорушень

2.3 Джерела загроз

Для даного підприємства можна виділити такі джерела загроз:

Внутрішні:

- працівники організації;
- програмне забезпечення;
- апаратні засоби.

Ці джерела загроз можуть проявлятися у різних формах, таких як наприклад:

- помилки користувачів і системних адміністраторів;
- порушення співробітниками фірми встановлених регламентів збору, обробки, передачі та знищення інформації;
- помилки в роботі програмного забезпечення;
- відмови і збої в роботі комп'ютерного обладнання.

До зовнішніх джерел загроз відносяться:

- комп'ютерні віруси і шкідливі програми;
- організації та окремі особи;
- стихійні лиха.

2.4 Виявлення загроз і вразливостей системи

Вся безліч потенційних загроз безпеки інформації ділиться на три класи по природі їх виникнення: антропогенні, техногенні та природні (природні).

Виникнення антропогенних загроз обумовлено діяльністю людини. Серед них можна виділити загрози, що виникають внаслідок як ненавмисних (ненавмисних) дій: загрози, викликані помилками в проектуванні інформаційної системи і її елементів, помилками в діях персоналу і т.п., так і загрози, що виникають в силу навмисних дій, пов'язані з корисливими , ідейними чи іншими прагненнями людей.

До антропогенним загроз відносяться загрози, пов'язані з нестабільністю і суперечливістю вимог регуляторів діяльності Банку і контрольних органів, з діями в керівництві і управлінні (менеджменті), неадекватними цілям і умовам, що склалися, з споживаними послугами, з людським фактором.

Виникнення техногенних загроз обумовлено впливами на об'єкт загрози об'єктивних фізичних процесів техногенного характеру, технічного стану оточення об'єкта загрози або його самого, не обумовлених безпосередньо діяльністю людини.

До техногенних загроз можуть бути віднесені збої, в тому числі в роботі, або руйнування систем, створених людиною.

Виникнення природних (природних) загроз обумовлено впливами на об'єкт загрози об'єктивних фізичних процесів природного характеру, стихійних природних явищ, станів фізичної середовища, не обумовлених безпосередньо діяльністю людини. До природним (природним) загроз відносяться загрози метеорологічні, атмосферні, геофізичні, геомагнітні і ін., Включаючи екстремальні кліматичні умови, метеорологічні явища, стихійні лиха.

2.5 Моделі порушників ІБ

По відношенню до студії порушники можуть бути розділені на зовнішніх і внутрішніх порушників.

2.5.1 Внутрішні порушники

В якості потенційних внутрішніх порушників студією розглядаються:

- співробітники студії, які мають доступ до будівлі та приміщення;
- персонал, який обслуговує технічні засоби корпоративної інформаційної системи студії;
- співробітники задіяні в розробці і супроводі веб-ресурсів;

2.5.2 Зовнішні порушники

В якості потенційних зовнішніх порушників студією розглядаються:

- колишні співробітники студії;
- представники організацій, що взаємодіють з питань технічного забезпечення Студії;
- клієнти студії;
- відвідувачі будівлі і приміщень студії;
- конкуруючі організації;
- члени злочинних організацій, співробітники спецслужб або особи, що діють за їх завданням;
- особи, випадково або навмисно проникли в корпоративну інформаційну систему Студії з зовнішніх телекомунікаційних мереж (хакери).

2.5.3Характер можливих дій порушників

- порушник приховує свої несанкціоновані дії від інших співробітників Студії;
- несанкціоновані дії порушника можуть бути наслідком помилок користувачів чи обслуговуючого персоналу, а також недоліків прийнятої технології обробки, зберігання та передачі інформації;
- в своїй діяльності ймовірний порушник може використовувати будь-який наявний засіб перехоплення інформації, впливу на інформацію та інформаційні системи, адекватні фінансові кошти для підкупу персоналу, шантаж, методи соціальної інженерії і інші засоби і методи для досягнення поставлених перед ним цілей;
- зовнішній порушник може діяти в змові з внутрішнім порушником.

2.6 Методика оцінки ризиків інформаційної безпеки

Оскільки я не можу провести точну оцінку ризиків на теоретичній веб-студії, я наведу методику оцінки ризиків інформаційної безпеки.

Основне завдання даної методики полягає в тому, щоб визначити чисельний показник ризику ІБ з метою прийняття ефективних заходів щодо захисту інформації.

Загальний алгоритм проведення оцінки ризиків ІБ складається з 5 єтапів:

1) Ідентифікація активів
2) Визначення невідповідностей вимог
3) Розробка моделей загроз
4) Процедура кількісного визначення ризиків
5) Визначення допустимого рівня ризиків

Процедура оцінки ризиків виконується працівникамі підприємства разом з керівництвом.

Єтап 1. На даному етапі проводиться інтерв'ю з персоналом кожного підрозділу або відділу з метою виявлення використовуваних активів. Активи системи інформаційних технологій є компонентом або частиною загальної системи, в яку підприємство безпосередньо вкладає кошти і які, відповідно, вимагає захисту з боку підприємства.

Можуть існувати такі типи активів:

1. Інформація / дані
2. Апаратні засоби
3. Програмне забезпечення, включаючи прикладні програми
4. Устаткування для забезпечення зв'язку
5. Програмно-апаратні засоби
6. Документи
7. Продукція підприємства.
8. Послуги
9. Конфіденційність і довіру при наданні послуг
10. Обладнання, що забезпечує необхідні умови роботи.
11. Персонал організації.
12. Престиж (імідж) організації.

Этап 2. Алгоритм визначення ризику невідповідності вимог включає в себе проведення всебічного аналізу стану системи захисту з метою виявлення виконання вимог відповідно до вимог. Потім рахується кількість виконаних вимог, і наприкінці визначається рівень ризику невідповідності вимог з ІБ, який визначається за табл. 2.1.

Єтап 3. У методиці з метою максимально точного визначення ризику ІБ необхідно розробити приватну модель загроз ІБ підприємству. Визначення ймовірності настання несприятливих подій визначається фахівцем з інформаційної безпеки. Експертним шляхом визначається і актуальність загроз ІБ. Після завершення оцінки загроз складають перелік актуальних ідентифікованих загроз на кожен ідентифікований актив або груп активів, схильних до цих погроз, а також визначають ймовірність реалізації загроз.

Таблиця 2.1 Рівень ризику невідповідності вимог.

Сума виконаних вимог	Ризик невідповідності вимогам
1	2
40-51	0,01
27-39	0,25
Менше 26	0,5
Не виконуються	0,9

Єтап 4. Процедура кількісної оцінки ризиків ІБ. Основним етапом в процесі оцінки ризиків є процедура кількісного визначення ризиків ІБ.

Процедура кількісної оцінки ризиків ІБ включає в себе наступні кроки:

Крок 1. Вибір актуальних загроз приватної моделі загроз. На даному етапі, формується перелік актуальних загроз ІБ. На даному етапі кількісного оцінювання ризиків зіставляються ідентифіковані активи з спрямованими на них погрозами. Для цього використовується перелік активів підприємства і кожному з них зіставляються актуальні загрози з моделі загроз.

Крок 2. Визначення ймовірності настання загрози. У зв'язку з тим, що на один актив можуть впливати одночасно кілька загроз, необхідно визначити ймовірність того, що хоча б одна загроза реалізується по відношенню до вибраного активу. Імовірність реалізації хоча б однієї загрози з сукупності ймовірностей загроз в1, в2, ..., уп, де п - кількість загроз,

дорівнює різниці між одиницею і добутком ймовірностей загроз.

Крок 3. Визначення цінності активу. Цінність активу визначається вартістю інформаційного активу. У зв'язку з тим, що часто неможливо визначити точні вартості активів і підприємства в цілому, рекомендується цінність активу задавати в діапазоні від 0 до 1, яка буде показувати відношення ціни активу до вартості всього бізнесу.

Так як універсальної методики оцінки активів немає, то в даній методиці оцінка активу визначається власником підприємства спільно з експертом з оцінки ризиків.

Крок 4. Визначення можливості використання організаційних і технічних вразливостей. Можливість використання організаційних вразливостей проводиться, аналізуючи застосовуються організаційні заходи захисту інформації. В ході проведення аналізу, вважаються всі організаційні заходи, які виконуються. У табл. 2.2 представлені відповідність виконаних організаційних заходів захисту інформації та коефіцієнт уразливості організаційних заходів захисту інформації.

Таблиця 2.2 Коефіцієнт вразливості організаційних заходів

Сума виконаних мір захисту	Коефіцієнт вразливості ($К_о$)
14-17	0,01
8-13	0,25
Менше 8	0,5
Не виконуються	0,9

Можливість використання технічних вразливостей проводиться експертним шляхом, аналізуючи застосовуються технічні заходи захисту інформації, які рахуються так само. В табл. 2.3 представлено відповідність виконаних технічних заходів захисту інформації та коефіцієнт уразливості технічних заходів захисту інформації.

Таблиця 2.3 Коефіцієнт вразливості технічних заходів

Сума виконаних мір захисту	Коефіцієнт вразливості ($К_о$)
15-19	0,01
9-14	0,25
Менше 9	0,5
Не виконуються	0,9

Крок 5. Обчислення чисельного значення ризику. У розробляється методикою процедура оцінки ризиків реалізації хоча б однієї загрози ґрунтується на вза-

імності декількох факторів - ймовірності події, коефіцієнта цінності активу, середньоарифметичного значення коефіцієнтів можливості використання організаційних вразливостей і можливості використання технічних вразливостей і ризику невідповідності вимогам. Під коефіцієнтом цінності активу розуміють цінність або критичність активу по відношенню до всього бізнесу.

Загальна формула (2.1) визначення реалізації загроз:

$$R = P_{\text{загр}} R_n C \frac{K_0 + K_t}{2} 100\% \qquad (2.1)$$

де R - чисельна величина ризику реалізації загроз ІБ; $P_{загр}$ - ймовірність реалізації хоча б однієї загрози з усього переліку актуальних загроз; R_n - ризик невідповідності вимогам; С - цінність активу; K_o - ймовірність використання організаційних вразливостей; K_t - ймовірність використання технічних вразливостей.

Єтап 5. Допустимий ризик прийнято вважати ризик, який в даній ситуації вважають прийнятним при існуючих суспільних цінностях. Для кожного підприємства допустимий ризик буде враховуватись самим підприємством.

2.7 Висновки до розділу 2

В цьому розділі було визначено об’єкт захисту політики інформаційної безпеки. Також я визначив типи і види загроз, основні джерела загроз. Визначив модель порушників інформаційної безпеки. Ознайомився з методикою визначення рівня ризику в організації.

Виходячи з цих даних можна буде побудувати систему інформаційної безпеки, визначити міри захисту інформації на підприємстві а також задокументувати їх.

3 ПЛАНУВАННЯ ТА РОЗРОБКА ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1 Методика розробки системи інформаційної безпеки

При виконанні робіт можна використовувати наступну модель побудови системи інформаційної безпеки (рис. 3.1), засновану на адаптації ОК (ISO 15408) і проведенні аналізу ризику (ISO 17799).

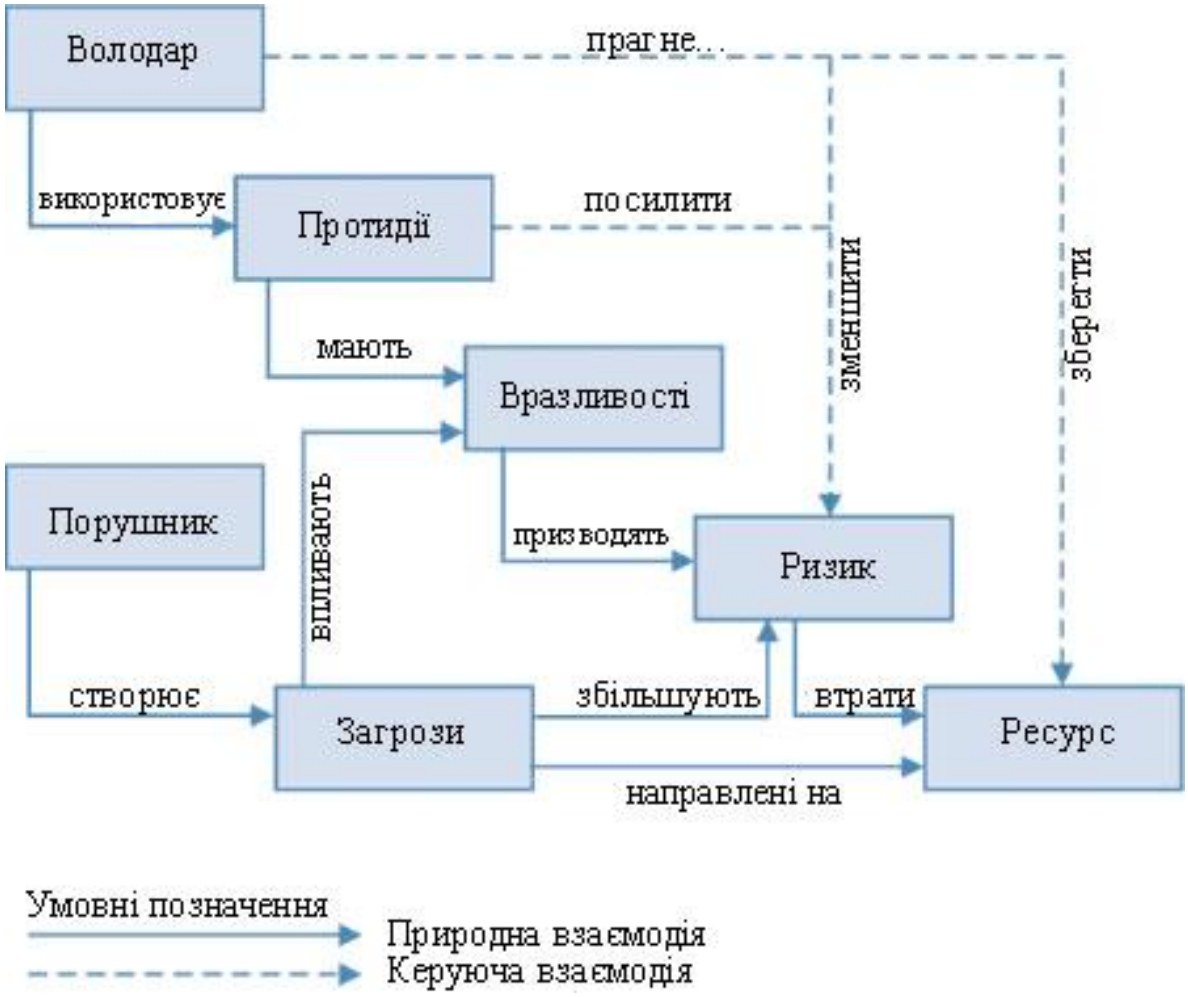


Рисунок 3.1 – Модель побудови системи інформаційної безпеки підприємства

Ця модель відповідає спеціальним нормативним документам щодо забезпечення інформаційної безпеки міжнародним стандартом ISO / IEC 15408 "Інформаційна технологія - методи захисту - критерії оцінки інформаційної безпеки", стандарту ISO / IEC 17799 "Управління інформаційною безпекою.

Представлена модель інформаційної безпеки - це сукупність об'єктивних зовнішніх і внутрішніх факторів і їх вплив на стан інформаційної безпеки на об'єкті та на збереження матеріальних або інформаційних ресурсів.

Розглядаються наступні об'єктивні фактори:

- Загрози інформаційної безпеки, які характеризуються ймовірністю виникнення і ймовірністю реалізації;
- Уразливості інформаційної системи або системи контрзаходів (системи інформаційної безпеки), що впливають на ймовірність реалізації загрози;
- Ризик - фактор, що відображає можливий збиток організації в результаті реалізації загрози інформаційної безпеки: витоку інформації і її неправомірному використанню (ризик в кінцевому підсумку відображає ймовірні фінансові втрати - прямі або непрямі).

Для побудови збалансованої системи інформаційної безпеки передбачається спочатку провести аналіз ризиків в області інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки (контрзаходи) належить побудувати таким чином, щоб досягти заданого рівня ризику.

3.1.1 Методика проведення аналітичних робіт

Запропонована методика дозволяє:

- Повністю проаналізувати і документально оформити вимоги, пов'язані із забезпеченням інформаційної безпеки;
- Уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків;

- Надати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;
- Забезпечити проведення робіт в стислі терміни;
- Уявити обгрунтування для вибору заходів протидії;
- Оцінити ефективність контрзаходів, порівняти різні варіанти контрзаходів.

3.1.2 Визначення меж дослідження

В ході робіт повинні бути встановлені межі дослідження. Для цього необхідно виділити ресурси інформаційної системи, для яких в подальшому будуть отримані оцінки ризиків Ресурсами можуть бути кошти, обчислювальнатехніка, програмне забезпечення, дані. Прикладами зовнішніх елементів є мережі зв'язку, зовнішні сервіси і т. п.

3.1.3Побудова моделі інформаційної технології

При побудові моделі будуть враховуватися взаємозв'язки між ресурсами. Наприклад, вихід з ладу будь-якого обладнання може призвести до втрати даних або виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв'язки визначають основу побудови моделі організації з точки зору ІБ.

Ця модель, в відповідність до запропонованої методики, будується наступним чином: для виділених ресурсів визначається їх цінність, як з точки зору асоційованих з ними можливих фінансових втрат, так і з точки зору шкоди репутації організації, дезорганізації її діяльності, моральної шкоди від розголошення конфіденційної інформації і т. д. Потім описуються взаємозв'язки ресурсів, визначаються загрози безпеки і оцінюються ймовірності їх реалізації.

3.1.4 Вибір контрзаходів

На основі побудованої моделі можна обґрунтовано вибрати систему контрзаходів, що знижують ризики до допустимих рівнів і володіють найбільшою цінової ефективністю. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту.

3.1.5 Управління ризиками

Забезпечення підвищених вимог до ІБ передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів проводиться після завершення етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму ІБ політиці безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

3.1.6 Оцінка захищеності системи

На завершення робіт, можна буде визначити міру гарантії безпеки інформаційного середовища Замовника, засновану на оцінці, з якої можна довіряти інформаційному середовищу об'єкта.

Даний підхід передбачає, що велика гарантія випливає з застосування великих зусиль при проведенні оцінки безпеки. Адекватність оцінки заснована на:

- Залученні в процес оцінки більшого числа елементів інформаційного середовища об'єкта Замовника;
- Глибині, що досягається за рахунок використання при проектуванні системи забезпечення безпеки більшого числа проектів і описів деталей виконання;

- Строгості, яка полягає в застосуванні більшого числа інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

3.1.7 Методологія аналізу ризиків

Мета процесу оцінювання ризиків полягає у визначенні характеристик ризиків в інформаційній системі і її ресурсах. На основі таких даних вибираються необхідні засоби управління ІБ.

Процес оцінювання ризиків містить кілька етапів:

- Опис об'єкта і заходів захисту;
- Ідентифікація ресурсу і оцінювання його кількісних показників (визначення потенційного негативного впливу на бізнес);
- Аналіз загроз інформаційної безпеки;
- Оцінювання вразливостей;
- Оцінювання існуючих і передбачуваних засобів забезпечення інформаційної безпеки;
- Оцінювання ризиків.

Ризик характеризує небезпеку, якій може піддаватися система і залежить від:

- Показників цінності ресурсів;
- Ймовірностей нанесення збитку ресурсів (які висловлюються через ймовірності реалізації загроз для ресурсів);
- Ступеня легкості, з якою уразливості можуть бути використані при виникненні загроз (уразливості системи захисту);
- Існуючих або планованих коштів забезпечення ІБ.

Розрахунок цих показників виконується на основі математичних методів, що мають такі характеристики, як обгрунтування і параметри точності методу.

3.1.8 Побудова профілю захисту

На цьому етапі розробляється план проектування системи захисту інформаційного середовища Замовника. Проводиться оцінка доступних засобів, здійснюється аналіз та планування розробки та інтеграції засобів захисту (рис. 2). Необхідною елементом роботи є твердження у Замовника допустимого ризику об'єкта захисту.

Рисунок 3.2 – Алгоритм оцінювання інформаційних ризиків

Забезпечення підвищених вимог до інформаційної безпеки передбачає відповідні заходи на всіх етапах життєвого циклу інформаційних технологій. Планування цих заходів проводиться після завершення етапу аналізу ризиків та вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму ІБ політиці безпеки, сертифікація інформаційної системи (технології) на відповідність вимогам певного стандарту безпеки.

Робота з побудови плану захисту об'єкта починається з побудови профілю захисту даного об'єкта. При цьому частина цієї роботи вже була пророблена при проведенні аналізу ризиків.

3.1.9 Формування організаційної політики безпеки

Перш ніж пропонувати будь-які технічні рішення по системі інформаційної безпеки об'єкта, належить розробити для нього політику безпеки.

Власне організаційна політика безпеки визначає порядок надання та використання прав доступу користувачів, а також вимоги звітності користувачів за свої дії в питаннях безпеки.

Система інформаційної безпеки (СІБ) об'єкта виявиться ефективною, якщо вона буде надійно підтримувати виконання правил політики безпеки, і навпаки. Кроками побудови організаційної політики безпеки є:

- Внесення в опис об'єкта автоматизації структури цінності і проведення аналізу ризику;
- Визначення правил для будь-якого процесу користування даним видом доступу до ресурсів об'єкта автоматизації, які мають даний ступінь цінності.

Організаційна політика безпеки оформляється у вигляді окремого документа, який узгоджується і затверджується Замовником.

3.1.10 Умови безпечного використання ІТ

Передбачається, що система забезпечення безпеки об'єкта Замовника, відповідна обраному профілю захисту, забезпечить необхідний рівень безпеки тільки в тому випадку, якщо вона встановлена, управляється і використовується у відповідність з виробленими правилами. Операційне середовище необхідно керуватися відповідно до прийнятої для даного профілю захисту нормативної документації, а також інструкцій адміністраторів і користувачів.

Виділяються наступні види умов безпечного використання ІТ:

- Фізичні умови;
- Умови для персоналу;
- Умови з'єднань.

Фізичні умови стосуються розміщення ресурсів об'єкта, а також захисту апаратних засобів і програмного забезпечення, критичних до порушення політики безпеки.

Умови для персоналу містять організаційні питання управління безпекою та відстеження повноважень користувачів.

Умови з'єднань не містять явних вимог для мереж і розподілених систем, але, наприклад, умова рівності положення означає наявність єдиної галузі управління всією мережею об'єкта.

Умови безпечного використання об'єкта автоматизації оформляються у вигляді окремого документа, який узгоджується і затверджується Замовником.

3.1.11 Формулювання цілей безпеки об'єкта

В цьому розділі профілю захисту дається детализованное опис загальної мети побудови системи безпеки об'єкта Замовника, яке виражається через сукупність факторів або критеріїв, уточнюючих мета. Сукупність факторів є базисом для визначення вимог до системи (вибір альтернатив).

Фактори безпеки, в свою чергу, можуть розподілятися на технологічні, технічні та організаційні.

Визначення функціональних вимог безпеки

Функціональні вимоги профілю захисту визначаються на основі набору добре відомих, відпрацьованих і узгоджених функціональних вимог безпеки. Всі вимоги до функцій безпеки можна розділити на два типи: управління доступом до інформації та управління потоками інформації.

На цьому етапі має бути правильно визначити для об'єкта компоненти функцій безпеки. Компонент функції безпеки описує певний набір вимог безпеки - найменший обираний набір вимог безпеки для включення в профіль захисту. Між компонентами можуть існувати залежності.

3.1.12 Вимоги гарантії захищеності системи

Структура вимог гарантії аналогічна структурі функціональних вимог і включає класи, сімейства, компоненти і елементи гарантії, а також рівні гарантії. Класи і сімейства гарантії відображають такі питання, як розробка, управління конфігурацією, робоча документація, підтримка етапів життєвого циклу, тестування, оцінка уразливості і інші питання.

Вимоги гарантії досягається захисту виражаються через оцінки функцій безпеки СІБ об'єкта. Оцінка сили функції безпеки виконується на рівні окремого механізму захисту, а її результати дозволяють визначити відносну здатність відповідної функції безпеки протистояти ідентифікованим загрозам. Виходячи з відомого потенціалу нападу, сила функції захисту визначається, наприклад, категоріями "базова", "середня", "висока".

Потенціал нападу визначається шляхом експертизи можливостей, ресурсів і мотивів спонукання нападника.

Рівні гарантії. Пропонується використовувати табличну зведення рівнів гарантованості захисту. Рівні гарантії мають ієрархічну структуру, де кожен наступний рівень надає більші гарантії і включає всі вимоги попереднього.

3.1.13 Формування переліку вимог

Перелік вимог до системи інформаційної безпеки, ескізний проект, план захисту (далі - технічна документація, ТД) містить набір вимог безпеки інформаційного середовища об'єкта Замовника, які можуть посилатися на відповідний профіль захисту, а також містити вимоги, сформульовані в явному вигляді.

У загальному вигляді розробка ТД включає:

- Уточнення функцій захисту;
- Вибір архітектурних принципів побудови СІБ;
- Розробку логічної структури СІБ (чіткий опис інтерфейсів);
- Уточнення вимог функцій забезпечення гарантоздатності СІБ;
- Розробку методики і програми випробувань на відповідність сформульованим вимогам.

3.1.14 Оцінка рівня захищеності системи

На цьому етапі проводиться оцінка заходи гарантії безпеки інформаційного середовища об'єкта автоматизації. Міра гарантії ґрунтується на оцінці, з якої після виконання рекомендованих заходів можна довіряти інформаційному середовищі об'єкта.

Базові положення даної методики припускають, що ступінь гарантії випливає з ефективності зусиль при проведенні оцінки безпеки.

Збільшення зусиль оцінки передбачає:

- Значне число елементів інформаційного середовища об'єкта, що беруть участь в процесі оцінювання;
- Розширення типів проектів і описів деталей виконання при проектуванні системи забезпечення безпеки;

– Строгість, яка полягає в застосуванні більшого числа інструментів пошуку і методів, спрямованих на виявлення менш очевидних вразливостей або на зменшення ймовірності їх наявності.

В цілому розглянута вище методика дозволяє оцінити або переоцінити рівень поточного стану інформаційної безпеки підприємства, виробити рекомендації щодо забезпечення (підвищення) інформаційної безпеки підприємства, знизити потенційні втрати підприємства або організації шляхом підвищення стійкості функціонування корпоративної мережі, розробити концепцію і політику безпеки підприємства, а також запропонувати плани захисту конфіденційної інформації підприємства, що передається по відкритих каналах зв'язку, захистів інформації підприємства від навмисного спотворення (руйнування), несанкціонованого доступу до неї, її копіювання або використання.

3.2 Модель системи інформаційної безпеки

Спочатку побудуємо модель керівництва інформаційною безпекою. Так як в даній студії працює всього 10 чоловік. За інформаційну безпеку буде відповідальна 1 людина тобто для даної системи буде така схема керівництва студією (рис 3.3).

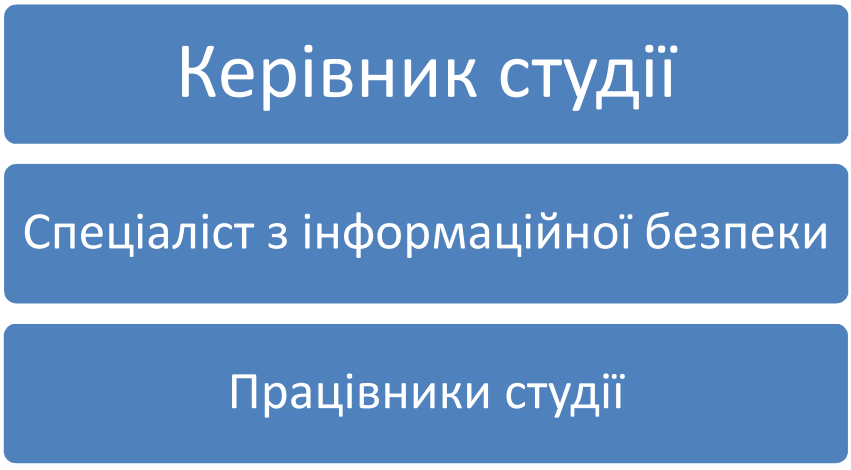


Рисунок 3.3 – Схема керівництва веб студії

Оскільки наша студія на справді не існує, уявімо що спеціаліст с інформаційної безпеки був найнятий одразу. Тому він буде використовувати цикл - «планування - реалізація - перевірка - вдосконалення - планування - ... », який спрямований на постійне вдосконалення діяльності щодо забезпечення інформаційної безпеки, вперше (рис.3.4).

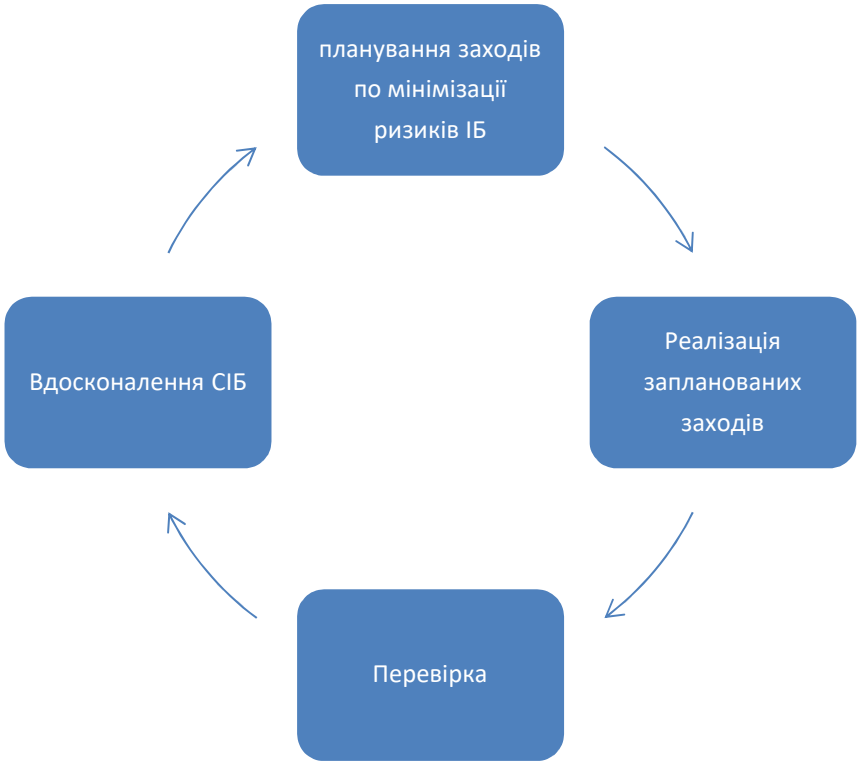


Рисунок 3.4 – Цикл вдосконалення системи інформаційної безпеки

Спочатку спеціаліст повинен побудувати систему інформаційної безпеки. Для цього потрібно визначити об’єкт захисту, джерела загроз, загрози та визначити модель порушників інформаційної безпеки. Після цього потрібно скласти політику інформаційної безпеки, а також використати всю отриману інформацію для створення системи інформаційної безпеки в організації. Після цього потрібно витратити кошти на реалізацію потрібної політики та системи.

Коли система налагоджена відповідальний за безпеку організації потрібен провести тест на проникнення для перевірки надійності системи ІБ. А потім все спочатку.

3.3 Можливі збитки

Усі можливі загрози завдають економічних збитків. Розраховуючи збитки будемо звертати свою увагу на усі можливі ризики які можуть становити загрозу для компанії.

Почнемо з антропогенних загроз. Однією з антропогенних загроз є крадіжка обладнання. Тут треба звертати свою увагу на те що саме було викрадено, якщо був викрадений комп'ютер або комп'ютери, без важливої інформації збитки компанії будуть у розмірі вартості цього комп'ютеру (комп'ютерів). Якщо був викрадений сервер, до вартості самого пристрою також додається цінність інформації яку можуть отримати шахраї.

Інший вид загроз з боку людини, це ненавмисні помилки при роботі в системі. В цьому разі треба дивитися яка помилка була допущена, і окремо розраховувати для кожного випадку. Взагалі можна сказати що такі помилки можуть задати як незначних збитків, так і фатальних.

Окремо слід сказати про навмисне втручання людей у систему. Такі дії є найбільшою проблемою захисту інформаційної безпеки, тому зазвичай вонин наносять найбільші збитки для компаній.

Також до антропогенних загроз можна додати хакерські атаки на систему. Зазвичай такі загрози наносять компаніям найбільших збитків, тому що хакери викрадають інформацію яка може бути таємницею компанії.Невеликі компанії які не витримують таких збитків, не видержують натуску з боку конкурентів і закриваються.

Техногенні загрози зазвичай бувають від невеликих збоїв програми до руйнування усієї системи. Тому для кожного окремого випадку також будуть окремі розрахунки. Наприклад при зависанні комп'ютера з втратою не збережених данних збитки будуть не великі. Якщо відбудеться руйнування усієї системи збитки будуть також величезні, і коштуватимуть вартості самої

системи з доданням суми на роботу з її відновлення, а також суми простою роботи компанії.

Природні загрози є найбільш непередбачуваними, тому вони також можуть наносити різних збитків.

3.4 Визначення заходів захисту та їх документування

Використовуючи вище надану інформацію ми можемо зробити висновки, які заходи безпеки потрібно провести для захисту системи, котрі потрібно задокументувати в політиці, або в інших документах які будуть доповнювати її.

З наведеної інформації про можливі збитки ми робим висновки що потрібно покращити систему безпеки усієї студії для цього потрібно зробити такі дії.

Для захисту від антропогенних загроз:

– Встановити систему відеонагляду та сигналізацію у приміщенні де знаходиться студія;

– Провести перевірку співробітників на їх компетентність у питанні інформаційної безпеки; Провести бесіду та підписати договір про нерозголошення комерційної таємниці;

– Розробити політику безпеки з обмеженням прав користувачів.

– Регулярно, не рідше ніж раз на 3 місяці, змінювати усі паролі

– Регулярно проводити тест на проникнення, не рідше ніж раз на пів року;

– Забезпечити робітників технічними ресурсами та засобами, які будуть відповідати рекомендованим вимогам для роботи програм;

– При збої роботи програми або системи робітник повинен одразу повідомити системного адміністратора або відповідального за систему інформаційної безпеки.

– Для зменшення ризику втрати даних всі роботи(розробки) повинні проводитися на сервері компанії

– Регулярно проводити бекап даних на сервері. Резервні копії даних повинні зберігатися окремо (на іншому сервері, у хмарному сховищі, на окремому носії інформації тощо)

– Забезпечити захист приміщення та техніки від природних загроз

– Проволити аналіз каналів витоку інформації, та прийняти міри по запобіганню цього.

Останнім кроком моєї роботи є скаладання політики інформаційної безпеки, яка є результатом документування заходів захисту інформаційної безпеки.

В результаті зібраної інформації моя політика буде складатися з таких частин:

1) Основні положення – в цій частині я буду описувати основні положення політики, чим вона є та які цілі вона переслідує
2) Опис об’єкта захисту – описує інформацію і активи які буде захищати система захисту інформації
3) Загрози інформаційної безпеки – описує можливі загрози для даної компанії
4) Заходи з забезпечення безпеки - це дії які необхідно провести для покращення системи інформаційної безпеки
5) Управління системою інформаційної безпеки – цей розділ описує модель управління системою інформаційної безпеки
6) Відповідальність – описує яку відповідальність буде нести порушник СІБ
7) Заключні положення – додаткові пункти політики які не мають відношення до захисту системи інформаційної безпеки, але мають відношення до самої політики.

3.5 Висновки до розділу 3

В цьому розділі я ознайомився з методикою розробки системи управління інформаційною безпекою. За допомогою цієї методики я побудував просту модель інформаційної безпеки для уявної веб студії. Ця модель не ідеальна тому, що методика побудови СУІБ передбачає реально визначені загрози, ризики, інформацію.

Також я намагався визначити можливі збитки. Але також вони розраховуються для реальних компаній, тому що потрібно враховувати реальні ціни на активи компанії.

Але на даних які я отримав у розділі 2 та 3 я зміг визначити деякі міри захисту для даної веб-студії. Результатом їх за документування і стала політика інформаційної безпеки яка наведена у додатку А.

4 ОХОРОНА ПРАЦІ

Завдяки досягненням сучасних технологій більшість роботи в офісі здійснюється з використанням комп'ютерної техніки. Якщо згадати, що в середньому робочий день офісного працівника становить 7-8 годин (як передбачено нормами Кодексу законів про працю України) при п'яти - або шестиденним робочим тижнем, можна зробити висновок, наскільки багато часу доводиться проводити один на один з комп'ютером.

Перелік нормативно-правових актів, які регулюють дане питання, є досить широким. Так, обов'язки роботодавця щодо забезпечення працівникам комфортних і безпечних умов для здійснення роботи, а також права працівників на такі умови передбачено частиною 2 ст. 2 і ч. 1 ст. 21 КЗпП, а також ст. 13 Закону України «Про охорону праці». Даний закон визначає основні положення щодо реалізації конституційного права працівників на охорону їх життя і здоров'я в процесі трудової діяльності, на належні, безпечні і здорові умови праці, регулює за участю відповідних органів державної влади відносини між роботодавцем і працівником з питань безпеки, гігієни праці та виробничого середовища і встановлює єдиний порядок організації охорони праці в Україні. Більшість актів в даній сфері становлять акти підзаконного рівня, а саме, численні правила, інструкції, державні санітарні правила і норми і т.п., якими регулюються окремі моменти щодо конструкції електронно-обчислювальної техніки, особливостей облаштування приміщень для роботи з нею і ряду інших подібних вимог.

4.1 Загальні питання з охорони праці

В організації/підприємстві проводиться навчання і перевірка знань з питань охорони праці відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого

наказом Держнаглядохоронпраці України від 26.01.2005 N 15, зареєстрованого в Міністерстві юстиції України 15.02.2005 за N 231/10511 [4].

Також впроваджені організаційні заходи з пожежної безпеки - навчання і перевірку знань відповідно до вимог Типового положення про інструктажі, спеціальне навчання та перевірку знань з питань пожежної безпеки на підприємствах, в установах та організаціях України, затвердженого наказом Міністерства України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи від 29.09.2003 N 368, зареєстрованого в Міністерстві юстиції України 11.12.2003 за N 1148/8469 [5].

Обов’язковими вимогами враховане наступне:

– не слід допускати до роботи осіб, що в установленому порядку не пройшли навчання, інструктаж та перевірку знань з охорони праці, пожежної безпеки та цих Правил.

– на підприємстві/організації, де експлуатуються ЕОМ з відео дисплейними терміналами (ВДТ) і периферійними пристроями (ПП), розробляється інструкція з охорони праці відповідно до Положення про розробку інструкцій з охорони праці, затвердженого наказом Держнаглядохоронпраці від 29.01.98 N 9, зареєстрованого в Міністерстві юстиції України 07.04.98 за N 226/2666 [6].

– ознайомлення з правилами безпеки праці, одержання відповідних інструктажів засвідчується у журналі інструктажів.

– перед допуском до самостійної роботи кожен працівник має право на навчання з питань охорони праці і роботодавець зобов’язаний, і проводить таке навчання у вигляді двох інструктажів з питань охорони праці:

1) вступного, який проводять працівники служби охорони праці об’єкта господарювання з усіма працівниками, яких приймають на роботу незалежно від їхньої освіти та стажу роботи за програмою, в якій подають загальні

питання охорони праці із врахуванням її особливостей на об’єкті господарювання;

2) первинного, який проводять керівники структурних підрозділів на місці праці з кожним працівником до початку їхньої роботи на цьому робочому місці.

Проходження працівником цих інструктажів з питань охорони праці підтверджується записами у відповідних журналах обліку інструктажів і скріплюється підписами осіб, які проводили інструктажі та осіб, які отримали інструктажі.

3) Повторний (не рідше одного разу в 6 місяців);

4) Позаплановий (при зміні правил охорони праці);

5) Поточний (проводять з працівниками перед виконанням робіт, на яких оформляється наряд-допуск)

– обов’язкові організаційні заходи перед початком, під час і після завершення роботи повинні включати перевірку (візуально) наявності і справності електрообладнання та його заземлення, а під час виконання роботи вимогу «не залишати без нагляду обладнання, яке працює». Після закінчення роботи - вимагається прибирання робочого місця, відключення всіх електроприладів від електромережі.

Не допускається:

– виконувати обслуговування, ремонт та налагодження ЕОМ з ВДТ і ПП безпосередньо на робочому місці оператора;

– зберігати біля ЕОМ з ВДТ і ПП папір, дискети, інші носії інформації, запасні блоки, деталі тощо, якщо вони не використовуються для поточної роботи;

– відключати захисні пристрої, самочинно проводити зміни у конструкції та складі ЕОМ з ВДТ і ПП або їх технічне налагодження;

– працювати з ВДТ, у яких під час роботи з'являються нехарактерні сигнали, нестабільне зображення на екрані тощо;

– працювати з матричним принтером за відсутності вібраційного килимка та зі знятою (піднятою) верхньою кришкою.

4.2Аналіз стану умов праці

Робота над створенням даної дипломної роботи бакалавра, та розробка політикі інформаційної безпеки проводилися мною у кімнаті багатоквартирного дому.

4.2.1 Вимоги до приміщень

Геометричні розміри приміщення наведені в таблиці 4.1.

Таблиця 4.1 – Розміри приміщення

Найменування	Значення
Довжина, м	5
Ширина, м	3
Висота, м	3
Площа, $м^2$	15
Об’єм, $м^3$	45

Згідно з [7] розмір площі для одного робочого місця оператора персонального комп’ютера має бути не менше 6 кв. м, а об’єм — не менше 20 куб. м. Отже, дане приміщення цілком відповідає зазначеним нормам.

Для забезпечення потрібного рівного освітленості кімната має вікно та систему загального рівномірного освітлення, що встановлена на стелі.

4.2.2 Вимоги до організації місця праці

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця за [8] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 - Характеристики робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибина сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні	500	не менше

спинки, мм		380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700 ÷800

Робочий стіл на досліджуваному місці також містить достатньо простору для ніг. Крісло, що використовується в якості робочого сидіння, є підйомно поворотним, має підлокітники і можливість регулювання за висотою і кутом нахилу спинки, також воно м'яке і виконане з екологічної шкіри, що дає можливість працювати у комфорті. Екран монітору знаходиться на відстані 0.8 м, клавіатура має можливість регулювання кута нахилу 5-15°. Отже, за всіма параметрами робоче місце відповідає нормативним вимогам.

Температура в приміщенні протягом року коливається у межах 18–24°C, відносна вологість — близько 50%. Швидкість руху повітря не перевищує 0,2 м/с. Шум в лабораторії знаходиться на рівні 50 дБА. Система вентилювання приміщення — природно організована, а опалення — централізоване.

Розміщення вікон забезпечує природне освітлення з коефіцієнтом природного освітлення не менше 1,5%, а загальне штучне освітлення, яке здійснюється за допомогою восьми люмінесцентних ламп, забезпечує рівень освітленості не менше 200 Лк.

У кабінеті є електрична мережа з напругою 220 В, яка створює небезпеку ураження електричним струмом. ПК та периферійні пристрої можуть бути джерелами електромагнітних випромінювань, аерозолів та шкідливих речовин (часток тонеру, оксидів нітрогену та озону).

4.2.3 Навантаження та напруженість процесу праці

За фізичним навантаженням робота відноситься до категорії легкі роботи (Іа), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав’язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Під час виконання робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що призводить до навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м’язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Тобто наявне психофізіологічні небезпечні та шкідливі фактори:

а) фізичного перевантаження:

- статичного;

- динамічного;

б) нервово-психічного перевантаження:

- розумового перенапруження;

- монотонності праці;

- перенапруження аналізаторів;

- емоційних перевантажень.

Рекомендовано застосування екранних фільтрів, локальних світлофільтрів (засобів індивідуального захисту очей) та інших засобів захисту, а також інші профілактичні заходи на ведені в [9].

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви:

- 15 хв через кожну годину роботи;

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.3 Виробнича санітарія

4.3.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3). Роботу, пов'язану з ЕОМ з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00.-1.28-10 «Правил охорони праці під час експлуатації електронно-обчислювальних машин», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і

ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої. Основними робочими характеристиками персонального комп'ютера є:

– робоча напруга U=+220В +-5%;

– робочий струм I=2А;

– споживана потужність Р=350 Вт.

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	4
Фізичні			
- підвищена температура поверхонь обладнання	експлуатація ЕОМ, принтерів, сканерів чи/або серверного обладнання для роботи	2	ДСН 3.3.6.042-99
- підвищений рівень вібрації	-//-	2	ДСН 3.3.6.039-99 ДСТУ ГОСТ 12.1.012-90
- підвищена або знижена вологість повітря	-//-	2	ДСН 3.3.6.042-99

- підвищена або знижена рухливість повітря	-//-	1	ДСН 3.3.6.042-99
- підвищений рівень іонізуючого випромінення в робочій зоні	-//-	2	ДСН 3.3.6.042-99 ГОСТ 12.1.006-84
- підвищений рівень електромагнітного випромінення	-//-	2	ГОСТ 12.1.006-84
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	ГОСТ 12.1.030-81 ГОСТ 13109-97
- підвищений рівень статичної електрики	-//-	2	ГОСТ 12.1.030-81
- підвищена напруженість електричного поля	-//-	2	ГОСТ 12.1.006-84
- підвищена напруженість	-//-	2	ГОСТ 12.1.006-84

магнітного поля			
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015
- підвищена яскравість світла	порушення умов праці (організації місця праці-налагодження моніторів)	1	ДСанПіН 3.3.2.007-98
- понижена контрастність	-//-	1	ДСанПіН 3.3.2.007-98
психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-1.28-10 ДСанПіН 3.3.2.007-98
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці-сидіння користувача,) та	2	НПАОП 0.00-1.28-10

	організації робочого часу - безпервна робота)		ДСанПіН 3.3.2.007-98

Робочі місця мають відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [9]. За умов роботи з ПК виникають наступні небезпечні та шкідливі чинники: несприятливі мікрокліматичні умови, освітлення, електромагнітні випромінювання, шум, вібрація, електричний струм, електростатичне поле, напруженість трудового процесу та інше.

4.3.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання,. Небезпека загоряння пов'язана з особливістю комп'ютерів - із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Висока щільність елементів в електронних схемах призводить до значного підвищення температури окремих вузлів (80…100 ℃). При проходженні електричного струму по провідниках і деталей виділяється тепло, що в умовах їх високої щільності може привести до перегріву, і може служити причиною запалювання ізоляційних матеріалів. Слабкий опір ізоляційних

матеріалів дії температури може викликати порушення ізоляції і привести до короткого замикання між струмоведучими частинами обладнання (шини, електроди). Також ймовірна небезпека внаслідок перевантаження напруги, розрядки зарядів статичної електрики, пошкодження обладнання та електропроводки. Електростатичний розряд виникає під час тертя двох ізольованих матеріалів. Розряд статичної електрики може виникнути під час роботи вентилятора або комп'ютера. Кабельні лінії є найбільш пожежонебезпечними місцем. Наявність пального ізоляційного матеріалу, ймовірних джерел запалювання у вигляді електричних іскор і дуг, розгалуженість і недоступність роблять кабельні лінії місцем найбільш ймовірного виникнення і розвитку пожежі. Для зниження займистості і здатності поширювати полум'я кабелі покривають вогнезахисними покриттями. Проектом передбачено прокладати проводку: приховано, під знімною підлогою розділяючи негорючими діафрагмами, в малодоступних місцях.

Заземлені конструкції, що знаходяться в приміщеннях, де розміщені робочі місця (батареї опалення, водопровідні труби, кабелі із заземленим відкритим екраном), надійно захищені діелектричними щитками та/або сітками з метою недопущення потрапляння працівника під напругу. Проходи до засобів пожежогасіння вільні, не захаращуються та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщенні через один евакуаційний вихід з дверима на шляху евакуації, що відчинятися в напрямку виходу з будівлі від робочого місця. В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Запобігти утворенню горючого середовища (замінити горючі речовини і матеріали на негорючі і важкогорючі) не надається технічно можливим. Тому проектом передбачаються способи і засоби запобігання утворення (або внесення) в горюче середовище джерел запалювання, таких як:

1) застосування електроустаткування, відповідної пожежонебезпечної і вибухонебезпечної зонам відповідно до ПУЕ;

2) застосування в конструкції швидкодійних засобів захисного відключення можливих джерел запалення;

3) виключення можливості появи іскрового розряду в горючому середовищі з енергією, рівної і вище мінімальної енергії запалення.

Згідно [10] таке приміщення, площею 15 м^2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено застосування первинних засобів пожежогасіння. Відповідно до норм первинних засобів пожежогасінні пропонується використовувати:

- повсть 1 1 м^2, кошму 2×1,5 м^2 або азбестове полотно 2×2 м^2 в кількості 1 шт.

Виникнення пожежі можливе, якщо на об'єкті є горючі речовини, окислювач і джерела запалювання. Вірогідність пожежної небезпеки приймається значною, якщо ймовірна взаємодія цих трьох чинників. Горючими компонентами є: будівельні матеріали для акустичної і естетичної обробки приміщень, перегородки, підлоги, двері, ізоляція силових, сигнальних кабелів і т.д.

Горючими матеріалами в приміщенні, де розташовані ЕОМ, є:

1) поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420 ˚С,

2) полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335˚С, температура самозаймання 530 ˚С,

3) склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.74, не схильний до температурного самозаймання,

4) пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

5) деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255 ℃, температура самозаймання 399 ˚С.

Для відводу теплоти від ЕОМ діє потужна система кондиціонування. Тому кисень, як окиснювач процесів горіння, є в будь-якій точці приміщень обчислювального центру.

Простори усередині приміщень в межах, яких можуть утворюватися або знаходиться пожежонебезпечні речовини і матеріали відповідно до [10] відносяться до пожежонебезпечної зони класу П-IIа. Це обумовлено тим, що в приміщенні знаходяться тверді горючі та важкозаймисті речовини та матеріали. Приміщенню, у якому розташоване робоче місце, присвоюється II ступень вогнестійкості.

Потенційними джерелами запалювання можуть бути:

1) іскри і дуги короткого замикання;

2) електрична іскра при замиканні і розмиканні ланцюгів;

3) перегріви від тривалого перевантаження,

4) відкритий вогонь і продукти горіння,

5) наявність речовин, нагрітих вище за температуру самозаймання,

6) розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

1) несправність електроустановки;

2) конструктивні недоліки устаткування;

3) коротке замикання в електричних мережах;

4) запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол [11].

4.3.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за ПУЕ (правила улаштування електроустановок), мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Штепсельні з'єднання та електророзетки крім контактів фазового та нульового робочого провідників мають спеціальні контакти для підключення нульового захисного провідника. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання. Металеві труби та гнучкі металеві рукави заземлені. Захисне заземлення включає в себе заземлюючих пристроїв і провідник, який з'єднує заземлюючий пристрій з обладнанням, яке заземлюється - заземлюючий провідник.

4.4 Гігієнічні вимоги до параметрів виробничого середовища

4.4.1 Мікроклімат

Мікроклімат робочих приміщень – це клімат внутрішнього середовища цих приміщень, що визначається діючої на організм людини з'єднанням температури, вологості, швидкості переміщення повітря. В даному приміщенні проводяться роботи, що виконуються сидячи і не потребують динамічного фізичного напруження, то для нього відповідає категорія робіт Іа. Отже оптимальні значення для температури, відносної вологості й рухливості повітря для зазначеного робочого місця відповідають [7] і наведені в табл. 4.4:

Таблиця 4.4 – Норми мікроклімату робочої зони об’єкту

Період року	**Категорія робіт**	**Температура C^0**	**Відносна вологість %**	**Швидкість руху повітря, м/с**
Холодна	легка-1 а	22 – 24	40 – 60	0,1
Тепла	легка-1 а	23 – 25	40 – 60	0,1

Дане приміщення обладнане системами опалення, кондиціонування повітря або припливно-витяжною вентиляцією. У приміщенні на робочому місці забезпечуються оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря у відповідності до [7]. Рівні позитивних і негативних іонів у повітрі мають відповідати [7]. Для забезпечення оптимальних параметрів мікроклімату в приміщенні проводяться перерви в роботі співробітників, з метою його провітрювання.

Контроль параметрів мікроклімату в холодний і теплий період року здійснюється не менше 3-х разів на зміну (на початку, середині, в кінці).

4.4.2 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче, створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

Збільшення освітленості сприяє поліпшенню працездатності навіть в тих випадках, коли процес праці практично не залежить від зорового сприйняття. При поганому освітленні людина швидко втомлюється, працює менш продуктивно, виникає потенційна небезпека помилкових дій і нещасних випадків.

Освітленість приміщення має велике значення при роботі на ПЕОМ. Вона багато в чому визначається колірною і мережевий обстановкою. Для зменшеного поглинання світла стеля і стіни вище панелей (1,5-1,7м.). Якщо вони не облицьовані звукопоглинальним матеріалом, фарбуються білою водоемульсійною фарбою (коефіцієнт відбиття повинен бути не менше 0,7). Для забарвлення стіни панелей рекомендується віддавати перевагу світлим фарбам.

Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працівника на ПЕОМ.

Робота на ПЕОМ може здійснюватися за таких видах освітлення:

- загальному штучному освітленні, коли відео монітори розташовуються по периметру приміщення або при центральному розташуванні робочих місць у два ряди по довжині кімнати з екранами, звернені в протилежні сторони;

- суміщене освітлення (природне + штучне) тільки при одному і трьох рядном розташуванні робочих місць, коли екран і поверхню робочого столу знаходяться перпендикулярно світла несучій стіні. При цьому штучне освітлення буде виконане стельовими або підвісними люмінесцентними світильниками, рівномірно розміщеними по стелі рядами паралельно світловим прорізам так, щоб екран відео монітора знаходився в зоні захисного кута світильника, і його проекції не доводилися на екран. Працюючі на ПЕОМ не повинні бачити відображення світильників на екрані. Застосовувати місцеве освітлення при роботі на ПЕОМ не рекомендується.

Природне освітлення, коли робочі місця з ПЕОМ розташовуються в один ряд по довжині приміщення на відстані 0,8 - 1,0 м від стіни з віконними прорізами, і екрани знаходяться перпендикулярно цієї стіни. Основний потік природного світла при цій повинен бути зліва. Не допускається спрямування основного світлового потоку природного світла праворуч, ззаду і спереду працює на ПЕОМ. Оптимальна відстань очей до екрана відео монітора повинна становити 60-70 см, допустиме не менше 50 см. Розглядати інформацію ближче 50 см не рекомендується.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

Штучне освітлення в робочому приміщенні передбачається здійснювати з використанням розжарювальних джерел світла в світильниках загального освітлення. При експлуатації ЕОМ виконується зорова робота IVв розряду точності (середня точність). При цьому нормована освітленість на робочому місці (Ен) рівна 200 лк. Джерелом природного освітлення є сонячне світло.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає [12]. Джерелом природного освітлення є

сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє ДБН і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше -1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \cdot S_n, \tag{4.1}$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

$S_n = a \cdot b = 5 \cdot 3 = 15$ м^2,

$S = 1/10 \cdot 15 = 1{,}5$ м^2.

Приймаємо 1 вікно площею S=1,5 м^2

Світильники загального освітлення розташовуються над робочими поверхнями в рівномірно-прямокутному порядку. Для організації освітлення в темний час доби передбачається обладнати приміщення, довжина якого складає 5 м, ширина 5 м, світильниками ЛПО2П, оснащеними лампами типа Б (100 Вт) з світловим потоком 1350 лм. Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M}, \tag{4.2}$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 15 м^2;

Z – поправочний коефіцієнт світильника (Z = 1,15 для ламп розжарювання та ДРЛ; Z = 1,1 для люмінесцентних ламп) приймаємо рівним 1,15;

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 1;

F – світловий потік лампи – 1350лм (для Б-100).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 * 15 * 1.15 * 1.5}{1350 * 0.575 * 1} = 10$$

Приймаємо освітлювальну установку, яка складається з 10 світильників, які складаються з однієї розжарювальної лампи загальною потужністю 100 Вт, напругою – 220 В.

4.4.3 Шум та вібрація, електромагнітне випромінювання

Рівень шуму, що супроводжує роботу користувачів персональних комп’ютерів (зумовлений як роботою системних блоків, клавіатури, а також

зовнішніми чинниками), коливається у межах 50–65 дБА [7]. Шум такої інтенсивності на тлі високого ступеня напруженості праці негативно впливає на функціональний стан користувачів. Тому на практиці рекомендують знижувати фактичний рівень шуму у приміщеннях, де створюють комп'ютерні програми, виконують теоретичні та творчі роботи, проводять навчання до 40 дБА, а в приміщеннях, де виконують роботу, що потребує зосередженості, — до 55 дБА. У залах опрацювання інформації та комп'ютерного набору рівні шуму не повинні перевищувати 65 дБА.

Шум часто є причиною зниження рівня працездатності, підвищення рівня загальної та професійної захворюваності, частоти виробничих травм. Шум є загальнобіологічним подразником, який негативно впливає на всі органи і системи організму. У разі тривалого систематичного впливу шуму може виникнути патологія з переважним ураженням слуху, центральної нервової і серцево- судинної систем.

Для зниження шуму на шляху його поширення передбачається розміщення в приміщенні штучних поглиначів. Для зниження рівня шуму стелю або стіни вище 1.5 - 1.7 метра від підлоги повинні облицьовуватися звукопоглинальним матеріалом з максимальним коефіцієнтом звукопоглинання в області частот 63-8000 Гц. Додатковим звукопоглинанням в КВТ можуть бути фіранки, підвішені в складку на відстані 15-20 см. Від огорожі, виконані з щільної, важкої тканини. У приміщенні з ЕОМ коректований рівень звукової потужності не перевищує 45 дБА. Оскільки рівень шуму не перевищує гранично допустимих величин, які встановлені санітарними нормами, заходи для зниження шуму не проводяться.

Віброізоляція можливо здійснювати за допомогою спеціальної прокладки під системний блок, який послаблює передачу вібрацій робочого столу. Вібрація на робочому місці в приміщенні, що розглядається, відповідає нормам [7]. Допустимий рівень вібрацій на робочому місці: - для 1 ступеня шкідливості до 3 дБ; - для 2-3 - 1-6 дБ; - для 3 - більше 6 дБ.

Для захисту від електромагнітного випромінювання передбачаються наступні заходи:

1) віддалення робочого місця не менше, ніж на 0,4 – 0,5 м, оскільки напруженість електричного поля зменшується при віддаленні від джерела поля,

2) встановлення раціональних режимів роботи персоналу (обмеження часу перебування),

3) раціональне розміщення в робочому приміщенні устаткування, що випромінює електромагнітну енергію.

4.4.4 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції (вентиляційні шахти), тобто при V приміщення > 40 $м^3$ на одного працюючого допускається природна вентиляція. Цей метод забезпечує приток потрібної кількості свіжого повітря, що визначається в СНіП.

Також має здійснюватися провітрювання приміщення, в залежності від погодних умов, тривалість повинна бути не менше 10 хв. Найкращий обмін повітря здійснюється при наскрізному провітрюванні.

4.5 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

- правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

- експлуатацію сертифікованого обладнання;

- дотримання заходів електробезпеки;

- забезпечення оптимальних параметрів мікроклімату;

- забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);

- облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

а) якщо об'єм приміщення 20 м^3, то потрібно подати не менш як 30 м^3/год повітря;

б) якщо об'єм приміщення у межах від 20 до 40 м^3, то потрібно подати не менш як 20 м^3/год повітря;

в) якщо об'єм приміщення становить понад 40 м^3, допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

- зниження рівня шуму та вібрації:

а) у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

б) звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

в) використання засобів індивідуального захисту).

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

- постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під'єднують до електромережі;

- постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

- не тягнути за мережевий кабель, щоб витягти вилку з розетки;

- не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

- не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

- не залишати включені електроприлади без нагляду;

- не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

- не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

Вимоги безпеки при надзвичайних ситуаціях:

1) При раптовому припиненні подачі електричної енергії вимкнути всі пристрої ПК в такій послідовності: периферійні пристрої, ВДТ, системний блок, стабілізатор (або блок безперервного живлення). Витягнути вилки з розеток. При наявності ознак горіння (дим, запах горілого) необхідно вимкнути

всі пристрої ПК, знайти місце загоряння і виконати всі можливі заходи для його ліквідації, попередивши терміново про це керівництво. У випадку виникнення пожежі негайно попередити про це пожежну частину та керівництво, виконати усі можливі заходи по евакуації людей з приміщення і розпочати гасіння пожежі первинними засобами пожежогасіння.

2) При замиканні, перевантаженні електричного струму на електричному обладнанні, внаслідок ураження грозової блискавки та ймовірної небезпеки ураженням електричним струмом, приймають наступне:

- попередження замикання здійснюється правильним вибором, монтажем експлуатації мереж;

- застосування захисту схем у вигляді швидкодіючих реле, а також вимикачів, плавких запобіжників, автоматичних вимикачів.

а) У випадку дотику до корпусу та інших струмоведучих частин електроустановки, що опинилися під напругою використовують захисне заземлення - зниження до безпечних значень напруги дотику і кроку, обумовлених замиканням на корпус та ін. Це досягається шляхом, зменшення потенціалу заземленого обладнання (за рахунок підйому потенціалу підстави, на якому стоїть людина, до значення, близького до значення потенціалу заземленого обладнання) та відключення від загальної електромережі ураженого обладнання.

б) У випадку замикання фази на корпус, зниження ізоляції мережі нижче визначеної межі і, нарешті, в разі дотику людини безпосередньо до частини, що знаходиться під напругою. Основними елементами пристрою захисного відключення є прилад захисного відключення і автоматичний вимикач.

Прилад захисного відключення - сукупність окремих елементів, які приймають вхідну величину, реагує на її зміни і при заданому значенні дають сигнал на її відключення вимикача:

- датчику - вхідна ланка пристрою, що сприймають впливу ззовні і здійснюють перетворення цього впливу в відповідний сигнал;

- підсилювача, призначений для посилення сигналу датчика, якщо він виявляється недостатньо потужним;

- ланцюгів контролю, службовці періодичної перевірки справності захисного відключення;

- допоміжних елементів - сигнальні лампи і вимірювальні прилади, що характеризують стан електроустановки.

Автоматичний вимикач - апарат, призначений для включення і вимикання від ланцюгів під навантаженням і при коротких замиканнях. Він повинен включати ланцюг автоматично при надходженні сигналу від приладу захисного відключення.

Також застосовують різні **електричні захисні засоби від ураження струмом**:

а) Ізолюючі - ізолюють людини від струмоведучих або заземлених частин, а так-же від землі. Вони діляться на основні та додаткові.

б) Основні - володіють ізоляцією, здатної довго витримувати робоче напругу електроустановки і тому ними дозволяється стосуватися струмоведучих частин, знаходячи-трудящих під напругою. До них відносяться: в електроустановках до 1000 Вт - діелектричної рукавички, ізолюючі штанги, ізолюючі і електровимірювальні кліщі і т.д .; понад 1000 Вт - ізолюючі штанги, і електровимірювальні кліщі, а також кошти для ремонтних робіт під напругою понад 1000Вт.

в) Запобіжні - володіють ізоляцією нездатною витримати робоча напруга електроустановки, і тому вони не можуть самостійно захищати людину від ураження струмом під цим напругою. Їх значення - посилити захисні дії

основних і ізолюючих засобів, разом з якими вони повинні застосовуватися, при чому при використання основних захисних засобів достатньо застосування одного запобіжного захисного засобу. До запобіжних відносяться засоби в електроустановках до 1000 Вт - діелектричні калоші килимки, а також ізолюючі підставки.

Розрахунок захисного заземлення (забезпечення електробезпеки будівлі).

1. Згідно з класифікацією приміщень за ступенем небезпеки ураження електричним струмом [13], приміщення в якому проводяться всі роботи відноситься до першого класу (без підвищеної небезпеки). Під час роботи використовуються електроустановки з напругою живлення 36 В, 220 В, та 360 В. Опір контура заземлення повинен мати не більше 4 Ом.

Розрахунок проводять за допомогою методу коефіцієнта використання (екранування) електродів. Коефіцієнт використання групового заземлювача η – це відношення діючої провідності цього заземлювача до найбільш можливої його провідності за нескінченно великих відстаней між його електродами. Коефіцієнт використання вертикальних заземлювачів $\eta_в$ в залежності від розміщення заземлювачів та їх кількості знаходиться в межах 0,4…0,99. Взаємну екрануючу дію горизонтального заземлювача (з'єднувальної смуги) враховують за допомогою коефіцієнта використання горизонтального заземлювача η_c.

Послідовність розрахунку.

1) Визначається необхідний опір штучних заземлювачів $R_{шт.з.}$:

$$R_{шт.з.} = \frac{R_д \cdot R_{пр.з.}}{R_{пр.з.} - R_д}, \qquad (4.3)$$

де $R_{пр.з.}$ – опір природних заземлювачів; $R_д$ – допустимий опір заземлення. Якщо природні заземлювачі відсутні, то $R_{шт.з.}=R_д$.

Підставивши числові значення у формулу (4.3), отримуємо:

$$R_{шт.з.} = \frac{4 \cdot 40}{40 - 4} \approx 4 \text{ Ом}$$

2) Опір заземлення в значній мірі залежить від питомого опору ґрунту ρ, Ом·м. Приблизне значення питомого опору глини приймаємо ρ=40 Ом•м (табличне значення).

3) Розрахунковий питомий опір ґрунту, $\rho_{розр}$, Ом·м, визначається відповідно для вертикальних заземлювачів $\rho_{розр.в}$, і горизонтальних $\rho_{розр.г}$, Ом·м за формулою:

$$\rho_{розр..} = \psi \cdot \rho, \qquad (4.4)$$

де ψ – коефіцієнт сезонності для вертикальних заземлювачів I кліматичної зони з нормальною вологістю землі, приймається для вертикальних заземлювачів $\rho_{розр.в}$=1,7 і горизонтальних $\rho_{розр.г}$=5,5 Ом·м.

$$\rho_{розр.в} = 1,7 \cdot 40 = 68 \text{ Ом•м}$$

$$\rho_{розр.г} = 5,5 \cdot 40 = 220 \text{ Ом•м}$$

4) Розраховується опір розтікання струму вертикального заземлювача $R_в$, Ом, за (4.5).

$$R_в = \frac{\rho_{розр.в}}{2 \cdot \pi \cdot l_в} \cdot \left(\ln \frac{2 \cdot l_в}{d_{ст}} + \frac{1}{2} \cdot \ln \frac{4 \cdot t + l_в}{4 \cdot t - l_в} \right), \qquad (4.5)$$

де $l_в$ – довжина вертикального заземлювача (для труб - 2–3 м; $l_в$=3 м);

$d_{ст}$ – діаметр стержня (для труб - 0,03−0,05 м; $d_{ст}$=0,05 м);

t – відстань від поверхні землі до середини заземлювача, яка визначається за ф. (4.6):

$$t = h_{в} + \frac{l_{в}}{2}, \tag{4.6}$$

де $h_{в}$ – глибина закладання вертикальних заземлювачів (0,8 м); тоді $t = 0,8 + \frac{3}{2} = 2,3$ м

$$R_{в} = \frac{68}{2 \cdot \pi \cdot 3} \cdot \left(\ln \frac{2 \cdot 3}{0,05} + \frac{1}{2} \cdot \ln \frac{4 \cdot 2,3 + 3}{4 \cdot 2,3 - 3} \right) = 18,5 \text{ Ом}$$

5) Визначається теоретична кількість вертикальних заземлювачів n штук, без урахування коефіцієнта використання $\eta_{в}$:

$$n = \frac{2 \cdot R_{в}}{R_{д}} = \frac{2 \cdot 18,5}{4} = 9,25 \tag{4.7}$$

І визначається коефіцієнт використання вертикальних електродів групового заземлювача без врахування впливу з'єднувальної стрічки $\eta_{в}$ =0,57 (табличне значення).

6) Визначається необхідна кількість вертикальних заземлювачів з урахуванням коефіцієнта використання $n_{в}$, шт:

$$n_{в} = \frac{2 \cdot R_{в}}{R_{д} \cdot \eta_{в}} = \frac{2 \cdot 18,5}{4 \cdot 0,57} = 16,2 \approx 16 \tag{4.8}$$

7) Визначається довжина з'єднувальної стрічки горизонтального заземлювача $l_с$, м:

$$l_с = 1,05 \cdot L_в \cdot (n_в - 1), \quad (4.9)$$

де $L_в$ – відстань між вертикальними заземлювачами, (прийняти за $L_в$ = 3м);

$n_в$ – необхідна кількість вертикальних заземлювачів.

$$l_с = 1,05 \cdot 3 \cdot (16 - 1) \approx 48 \text{ м}$$

8) Визначається опір розтіканню струму горизонтального заземлювача (з'єднувальної стрічки) $R_г$, Ом:

$$R_г = \frac{\rho_{розр.г}}{2 \cdot \pi \cdot l_с} \cdot \ln \frac{2 \cdot l_с^2}{d_{см} \cdot h_г}, \quad (4.10)$$

де $d_{см}$ – еквівалентний діаметр смуги шириною b, $d_{см}$ =0,95b, b = 0,15 м;

$h_г$ – глибина закладання горизантальних заземлювачів (0,5 м);

$l_с$ - довжина з'єднувальної стрічки горизонтального заземлювача $l_с$, м

$$R_г = \frac{220}{2 \cdot \pi \cdot 48} \cdot \ln \frac{2 \cdot 48^2}{0,95 \cdot 0,15 \cdot 0,5} = 8,1 \text{ Ом}$$

9) Визначається коефіцієнт використання горизонтального заземлювача $\eta_{с.}$ відповідно до необхідної кількості вертикальних заземлювачів $n_в$.

Коефіцієнт використання з'єднувальної смуги $\eta_с$=0,3 (табличне значення).

10) Розраховується результуючий опір заземлювального електроду з урахуванням з'єднувальної смуги:

$$R_{заг} = \frac{R_в \cdot R_г}{R_в \cdot \eta_с + R_г \cdot n_в \cdot \eta_в} \le R_д. \quad (4.11)$$

Висновок: дане захисне заземлення буде забезпечувати електробезпеку будівлі, так як виконується умова: $R_{заг}$ <4 Ом, а саме:

$$R_{заг} = \frac{18,5 \cdot 8,1}{18,5 \cdot 0,3 + 8,1 \cdot 16 \cdot 0,57} = 1,9 \le R_д$$

3) При виникненню пожеж при роботі на ПЕОМ від таких можливими джерел запалювання як:

– іскри і дуги коротких замикань;

– перегрів провідників, резисторів та інших радіодеталей ПЕОМ, від тривалої перевантаження та наявність перехідного опору;

– іскри при розмиканні і розмиканні ланцюгів;

– розряди статичної електрики;

– необережному поводженню з вогнем, а також вибухи газо-повітряних і паро-повітряних сумішей.

Важливу увагу слід звернути на пожежну безпеку підприємства в цілому і окремих його приміщень. В приміщеннях не повинно накопичуватися сміття, непотрібний папір, мотлох та ін. речі, які не використовуються у виробничому процесі. Наявний вільний аварійний вихід за межі приміщення в разі пожежі, бути передбачені вогнегасники. Вони повинні бути в робочому стані і перевірятися згідно з нормами. У приміщеннях повинна бути пожежна сигналізація, вогнегасник. У разі виникнення пожежі необхідно повідомити в найближчу пожежну частину, убезпечити інших працівників і по можливості прийняти кроки по запобіганню можливих наслідків та усуненню пожежі.

4.6 Висновки до розділу 4

В результаті проведеної роботи було зроблено аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Було визначено параметри і певні характеристики приміщення для роботи над

запропонованим проектом написаному в кваліфікаційній роботі, описано, які заходи потрібно зробити для того, щоб дане приміщення відповідало необхідним нормам і було комфортним і безпечним для робітника.

Приведені рекомендації щодо організації робочого місця, а також важливу інформацію щодо пожежної та електробезпеки. Була наведена схема, розміри приміщення та наведено значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, а також – наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

ВИСНОВКИ

В ході даної дипломної роботи я визначив якими нормативно-правовими документами регулюється інформаційна безпека в Україні. Також я ознайомився із сімейством стандартів ISO/IEC 27000.

Визначив типи і види загроз, джерела загроз, отримав навички розробки моделей порушників, визначення ризиків інформаційної безпеки підприємста.

Ознайомився з методикою створення СІБ, та отримав навички її створення. Визначив які контрміри треба провести для того щоб зменшити ризики інформаційної безпеки, після чого розробив політику інформаційної безпеки.

В 4 розділі я ознайомився з вимогами охорони праці для підприємств, та зробив висновки що також треба враховувати і їх як при розробці СІБ так і при розробці політики інформаційної безпеки.

В майбутньому, знання отримані під час роботи над дипломним проектом, я зможу застосувати на посаді спеціаліста з інформаційної безпеки, при розробці як СІБ так і політик як для однієї так і для різних компаній.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1) ISO/IEC 27001 «Інформаційна технологія. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги»
2) ISO 15408 "Критерії оцінки безпеки інформаційних технологій"
3) ISO 17799 «Інформаційні технології - Технології безпеки - Практичні правила менеджменту інформаційної безпеки»
4) НПАОП 0.00-4.12-05 Типове положення про порядок проведення навчання і перевірки знань з питань охорони праці
5) НПАОП Б.02.005-2003 Про інструктаж, спецнавчання з питань пожежної безпеки
6) НПАОП 0.00-4.15-98 Про розробку інструкцій з охорони праці
7) ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень»
8) ДСанПіН 3.3.2.007-98 «Правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин»
9) ДСанПіН 3.3.2.007-98 Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин
10) НАПБ Б.03.002-2007 Норми визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою
11) ГОСТ 12.1.044-89 ССБТ. Пожаровзрывоопасность веществ и материалов. Номенклатура показателей и методы их определения
12) ДБН В.2.5-28:2015 Природнє і штучне освітлення
13) НПАОП 40.1-1.01-97 Правила безопасной эксплуатации электроустановок

ДОДАТОК А
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Політика інформаційної безпеки

1 Основні положення

1.1 Дана Політика розроблена в відповідності з міжнародними стандартами ISO/IEC 27000 та нормами права в сфері інформаційної безпеки.

1.2 Дана Політика є нормативно-правовим актом який регулює дії компанії у сфері інформаційної безпеки.

1.3 Дана Політика направлена на досягнення наступних цілей:

- забезпечення безперервності основних бізнес-процесів Компанії;
- мінімізація можливих втрат і збитків від порушень у сфері інформаційної безпеки.

2 Опис об’єкта захисту

Основними об’єктами захисту системи інформаційної безпеки Компанії є:

- інформаційні ресурси які є комерційною таємницею, персональні дані клієнтів компанії, а також відкрита інформація яка потрібна для роботи Компанії;
- інформаційні ресурси та розробки Компанії які є її інтелектуальною власністю.
- працівники Компанії, які є розробниками та користувачами систем Компанії;
- інформаційна інфраструктура яка включає в себе системи обробки та аналізу інформації, технічні та програмні засоби обробки інформації, а також канали інформаційного обміну і телекомунікації, системи і засоби захисту інформації, об’єкти та приміщення в яких розміщені такі системи.

3 Джерела загроз інформаційної безпеки

Компанія поділяє усі джерела загроз на внутрішні та зовнішні.

3.1 До внутрішніх джерел загроз Компанія відносить:

- працівники організації;
- програмне забезпечення;
- апаратні засоби.

Ці джерела загроз можуть проявлятися у різних формах, таких як наприклад:

- помилки користувачів і системних адміністраторів;
- порушення співробітниками фірми встановлених регламентів збору, обробки, передачі та знищення інформації;
- помилки в роботі програмного забезпечення;
- відмови і збої в роботі комп'ютерного обладнання.

3.2 До зовнішніх джерел загроз Компанія відносить:

- колишніх працівників Компанії;
- комп'ютерні віруси і шкідливі програми;
- організації та окремі особи;
- стихійні лиха.

Їх проявлення можуть бути такими, як наприклад:

- хакерська атака з цілями викрадення інформації;
- зараження комп’ютерів або систем Компанії вірусом;
- пожежі та інші стихійні (природні) лиха;
- викрадення різноманітних активів Компанії.

4 Заходи з забезпечення безпеки

Для захисту студії від загроз інформаційної безпеки потрібно:

4.1 Встановити систему відео-нагляду та сигналізацію у приміщенні де знаходиться студія та забезпечити її підтримку;

4.2 Проводити перевірку співробітників на їх компетентність у питанні інформаційної безпеки; Провести бесіду та підписати договір про нерозголошення комерційної таємниці;

4.3 Розробити політику безпеки з обмеженням прав користувачів.

4.4 Регулярно, не рідше ніж раз на 3 місяці, змінювати усі паролі

4.5 Регулярно проводити тест на проникнення, не рідше ніж раз на пів року;

4.6 Забезпечити робітників технічними ресурсами та засобами, які будуть відповідати рекомендованим вимогам для роботи програм;

4.7 При збої роботи програми або системи робітник повинен одразу повідомити системного адміністратора або відповідального за систему інформаційної безпеки.

4.8 Для зменшення ризику втрати даних всі роботи(розробки) повинні проводитися на сервері компанії

4.9 Регулярно проводити бекап даних на сервері. Резервні копії даних повинні зберігатися окремо (на іншому сервері, у хмарному сховищі, на окремому носії інформації тощо)

4.10 Забезпечити захист приміщення та техніки від природних загроз

4.11 Проводити аналіз каналів витоку інформації, та прийняти міри по запобіганню цього.

5 Управління системою інформаційної безпеки

5.1 Кожен працівник Компанії слідкує за станом інформаційної безпеки Компанії.

5.2 Кожен працівник при знаходженні вразливості або загрози системи інформаційної безпеки повинен повідомити відповідального за систему інформаційної безпеки.

5.3 Відповідальний за систему інформаційної безпеки є системний адміністратор компанії або окремо найнята людина.

5.4 Усі дії які пов’язані з системою інформаційної безпеки узгоджуються відповідальним за систему інформаційної безпеки та керівником Компанії.

5.5 Головним відповідальним за управління системою інформаційної безпеки є керівник Компанії.

6 Відповідальність

6.1 Кожен працівник відповідальний за свої дії щодо порушення даної політики або системи інформаційної безпеки Компанії.

6.2 За порушення інформаційної безпеки кожен буде покараний згідно з законом та трудовим договором.

7 Заключні положення

7.1 Вимоги даної Політики можуть розвиватися та доповнюватися іншими внутрішніми нормативно-правовими документами, які доповнюють та уточнюють її.

7.2 Дана Політика переглядається, змінюється або доповнюється не рідше ніж раз на 12 місяців.

7.3 Політика може змінюватися, уточнюватися або переглядатися по результатам аналізу стану інформаційної безпеки Компанії.

7.4 У разі внесення змін керівництво Компанії повинно проінформувати кожного працівника Компанії.

7.5 Дана політика є загальнодоступним документом, з яким кожен може ознайомитися, та розміщений на сайті Компанії.

ДОДАТОК Б
КОМП’ЮТЕРНА ПРЕЗЕНТАЦІЯ

СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ

ДИПЛОМНА РОБОТА

НА ТЕМУ

«Розробка політики безпеки розподіленої ІКС із відкритою архітектурою»

Виконав: Гончар А.О.
Керівник: доц. Скарга-Бандурова І.С.

Сєвєродонецьк - 2017

Актуальність теми

- В наш час дуже важливо забезпечити безпеку інформації. Але для цього потрібно дотримуватись якихось правил. Ці правила і описує політика інформаційної безпеки.
- Політика інформаційної безпеки є задокументованою системою інформаційної безпеки і призначена для захисту інформації від порушників. Вона забезпечує її цілісність, конфіденційність та доступність, що є основними властивостями інформації.

ОБ'ЄКТ ТА МЕТА ДОСЛІДЖЕННЯ

3

Об'єкт дослідження

- Нормативно-правові документи які регулюють сферу інформаційної безпеки
- Політика інформаційної безпеки
- Системи інформаційної безпеки
- Загрози та ризики інформаційної безпеки

4

Мета дипломної роботи

- Ознайомлення з нормативно-правовими документами в сфері інформаційної безпеки
- Визначення загроз, джерел загроз та ризиків інформаційних систем
- Визначення заходів для забезпечення цілісності, доступності та конфіденційності інформації
- Ознайомлення з методикою створення інформаційних систем
- Створення політики інформаційної безпеки

5

Для досягнення мети було поставлено наступні завдання:

- Ознайомитись з основними поняттями інформаційної безпеки
- Ознайомитись з нормативно-правовими документами в сфері інформаційної безпеки
- Ознайомитись з методикою створення СІБ
- Визначити типи, джерела загроз
- Ознайомитися з методикою розрахунку рівня ризику ІС
- Визначити заходи з покращення рівня інформаційної безпеки системи
- Задокументувати дані заходи у політику інформаційної безпеки

6

Основні поняття

ІНФОРМАЦІЯ

7

Нормативно-правові акти в Україні

- Закони України
- Постанови Кабінету міністрів України
- Нормативні документи в галузі технічного захисту інформації (НД ТЗІ) та державні стандарти України (ДСТУ) стосовно створення і функціонування КСЗІ
- Галузеві стандарти

8

Міжнародні стандарти ISO/IEC 27000

- огляд і введення в термінологію, опис термінів, що застосовуються в сфері забезпечення безпеки;
- обов'язкові вимоги до системи управління інформаційною безпекою, докладний опис методів і засобів управління системою. Є основним стандартом цієї групи;
- рекомендації для аудиту, керівництво по заходам забезпечення безпеки;
- стандарти, які рекомендують практики впровадження, розвитку та вдосконалення системи управління інформаційною безпекою.

9

Політика інформаційної безпеки

- Згідно із стандартом ISO / IEC 17799-2005, політика інформаційної безпеки повинна встановлювати відповідальність керівництва, а також викладати підхід організації до управління інформаційною безпекою.
- Політика інформаційної безпеки компанії повинна бути затверджена керівництвом, видана і доведена до відома всіх співробітників в доступній та зрозумілій формі.
- Для того щоб політика інформаційної безпеки не залишалася тільки «на папері» необхідно, щоб вона була: несуперечлива, не забороняла необхідні дії, не накладала неможливих вимог

10

Об’єкт захисту

Основними об'єктами захисту системи інформаційної безпеки в студії є:

- інформаційні ресурси, що містять комерційну таємницю, персональні дані фізичних осіб, відомості обмеженого поширення, а також відкрито поширювана інформація, необхідна для роботи студії, незалежно від форми та виду її подання;
- інформаційні ресурси, що містять конфіденційну інформацію,
- співробітники Банку, які є розробниками і користувачами інформаційних систем Банку;
- інформаційна інфраструктура, що включає системи обробки і аналізу інформації, технічні та програмні засоби її обробки, передачі і відображення, в тому числі канали інформаційного обміну і телекомунікації, системи і засоби захисту інформації, об'єкти і приміщення, в яких розміщені такі системи.

11

Типи і види загроз

- За аспекту інформаційної безпеки, на який спрямовані загрози: загрози конфіденційності, цілісності, доступності інформації;
- По розташуванню джерела загроз: внутрішні, зовнішні;
- За розмірами нанесених збитків: загальні, локальні, приватні;
- За ступенем впливу на інформаційну систему: пасивні, активні;
- За природою виникнення: природні, штучні;

12

Джерела загроз

Для різних організацій можна виділити такі джерела загроз:

- Внутрішні:
  - працівники організації;
  - програмне забезпечення;
  - апаратні засоби.
- Зовнішні:
  - Інтернет;
  - організації та окремі особи;
  - стихійні лиха

13

Характер дій можливих порушників

- порушник приховує свої несанкціоновані дії від інших співробітників Студії;
- несанкціоновані дії порушника можуть бути наслідком помилок користувачів чи обслуговуючого персоналу, а також недоліків прийнятої технології обробки, зберігання та передачі інформації;
- в своїй діяльності ймовірний порушник може використовувати будь-який наявний засіб перехоплення інформації, впливу на інформацію та інформаційні системи, адекватні фінансові кошти для підкупу персоналу, шантаж, методи соціальної інженерії і інші засоби і методи для досягнення поставлених перед ним цілей;
- зовнішній порушник може діяти в змові з внутрішнім порушником

14

Методика оцінки ризиків

- Етап 1 • Ідентифікація активів
- Етап 2 • Визначення невідповідностей вимог
- Етап 3 • Розробка моделей загроз
- Етап 4 • Процедура кількісного визначення ризиків
- Етап 5 • Визначення допустимого рівня ризиків

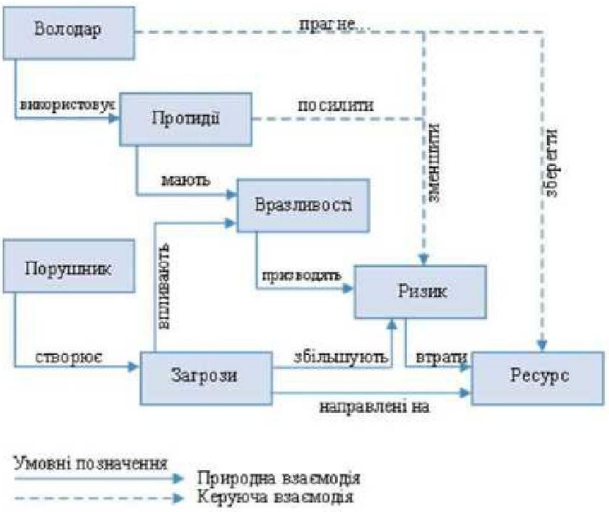
15

Методика розробки СІБ

- Проведення аналітичних робіт
- Визначення меж дослідження
- Побудова моделі інформаційної технології
- Вибір контрзаходів
- Управління ризиками
- Оцінка захищеності системи
- Методологія аналізу ризиків
- Побудова профілю захисту
- Формування організаційної політики безпеки
- Умови безпечного використання ІТ
- Формулювання цілей безпеки об'єкта
- Вимоги гарантій захищеності системи
- Формування переліку вимог
- Оцінка рівня захищеності системи

16

Модель побудови системи ІБ



17

Модель системи ІБ

- Керівник студії
- Спеціаліст з інформаційної безпеки
- Працівники студії

18

Цикл покращення СІБ

19

План політики

- Основні положення – в цій частині я буду описувати основні положення політики, чим вона є та які цілі вона переслідує
- Опис об'єкта захисту – описує інформацію і активи які буде захищати система захисту інформації
- Загрози інформаційної безпеки – описує можливі загрози для даної компанії
- Заходи з забезпечення безпеки - це дії які необхідно провести для покращення системи інформаційної безпеки
- Управління системою інформаційної безпеки – цей розділ описує модель управління системою інформаційної безпеки
- Відповідальність – описує яку відповідальність буде нести порушник СІБ
- Заключні положення – додаткові пункти політики які не мають відношення до захисту системи інформаційної безпеки, але мають відношення до самої політики.
-

20

Висновки

- В ході даної дипломної роботи я визначив якими нормативно-правовими документами регулюється інформаційна безпека в Україні. Також я ознайомився із сімейством стандартів ISO/IEC 27000.
- Визначив типи і види загроз, джерела загроз, отримав навички розробки моделей порушників, визначення ризиків інформаційної безпеки підприємста.
- Ознайомився з методикою створення СІБ, та отримав навички її створення. Визначив які контрміри треба провести для того щоб зменшити ризики інформаційної безпеки, після чого розробив політику інформаційної безпеки.
- В 4 розділі я ознайомився з вимогами охорони праці для підприємств, та зробив висновки що також треба враховувати і їх як при розробці СІБ так і при розробці політики інформаційної безпеки.
- В майбутньому, знання отримані під час роботи над дипломним проектом, я зможу застосувати на посаді спеціаліста з інформаційної безпеки, при розробці як СІБ так і політик як для однієї так і для різних компаній

21

ДЯКУЮ ЗА УВАГУ!

22