Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студентки *Маркіної Марії Володимирівни*

академічної групи *УБіт-15-1*

спеціальності *6.170103 Управління інформаційною безпекою*

спеціалізації[1]

за освітньо-професійною програмою

на тему *Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «АртКасл»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	к.т.н., доц. Флоров С.В.			
розділів:				
спеціальний	к.т.н., доц. Флоров С.В.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2019

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студентці ***Маркіній Марії Володимирівні*** **академічної групи** ***УБіт-15-1***
(прізвище ім'я по-батькові) (шифр)

напряму підготовки ***6.170103 Управління інформаційною безпекою***
(код і назва спеціальності)

на тему ***Розробка політики безпеки інформації інформаційно-телекомунікаційної системи ТОВ «АртКасл»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 21.05.2019 № 771-л.

Розділ	Зміст	Термін виконання
Розділ 1	*Обстеження інформаційно-телекомунікаційної системи ТОВ «АртКасл». Розробка моделі загроз.*	20.03.2019
Розділ 2	*Аналіз стану захищеності інформаційно-телекомунікаційної системи ТОВ «АртКасл». Розробка політики безпеки інформації.*	30.05.2019
Розділ 3	*Техніко-економічне обґрунтування доцільності запровадження запропонованих в роботі рішень.*	15.06.2019

Завдання видано _____ Флоров С.В
(підпис керівника) (прізвище, ініціали)

Дата видачі: 08.01.2019р.

Дата подання до екзаменаційної комісії: 21.06.2019р.

Прийнято до виконання _____ Маркіна М.В.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 85 с., 9 рис., 14 табл., 4 додатка, 15 джерел.

Об'єкт розробки: політика безпеки інформації інформаційно-телекомунікаційної системи ТОВ "АртКасл".

Мета проекту: підвищення рівня безпеки інформації в ІТС ТОВ «АртКасл», розробка рішень для захисту від загроз інформаційної безпеки.

У першому розділі описаний об'єкт: рід діяльності, фізичне середовище, в якому знаходиться об’єкт, устаткування, інформаційна система, програмне забезпечення, інформаційні потоки. Виконано класифікацію інформації, що циркулює в ІТС, визначений перелік джерел загроз, перелік вразливостей та перелік актуальних для ІТС загроз.

У другому розділі описано наявні в ІТС критерії захищеності та виконано вибір нових додаткових рекомендованих критеріїв захищеності, були розроблені рекомендації щодо розділів політики безпеки, що забезпечують реалізацію рекомендованих критеріїв захищеності та захист від актуальних для підприємства загроз.

В третьому розділі були розраховані витрати на впровадження та щорічну підтримку засобів та заходів, описаних у запропонованих розділах політики безпеки, оцінено можливі збитки від реалізації актуальних загроз. Була визначена економічна доцільність введення в експлуатацію рекомендацій щодо політики безпеки, розроблених в другому розділі.

Практичне значення проекту полягає в підвищенні інформаційної безпеки ТОВ "АртКасл".

ПОЛІТИКА БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, ІНФОРМАЦІЙНА БЕЗПЕКА, ВРАЗЛИВОСТІ.

РЕФЕРАТ

Пояснительная записка: 85 с., 9 рис., 14 табл., 4 приложения, 15 источников.

Объект разработки: политика безопасности информации информационно-телекоммуникационной системы ООО "АртКасл".

Цель проекта: повышение уровня безопасности информации в ИТС ООО «АртКасл», разработка решений для защиты от угроз информационной безопасности.

В первом разделе описан объект: род деятельности, физическая среда, в которой находится объект, оборудование, информационная система, программное обеспечение, информационные потоки. Выполнена классификация информации, которая циркулирует в ИТС, определен список источников угроз, список уязвимостей и перечень актуальных для ИТС угроз.

Во втором разделе описаны присутствующие в ИТС критерии защищенности и осуществлен выбор новых дополнительных рекомендованных критериев защищенности, были разработаны рекомендации касательно разделов политики безопасности, которые обеспечивают реализацию рекомендованных критериев защищенности и защиту от актуальных для предприятия угроз.

В третьем разделе были рассчитаны затраты на внедрение и ежегодную поддержку средств и мероприятий, описанных в предложенных разделах политики безопасности, оценены возможные убытки от реализации актуальных угроз. Была определена экономическая целесообразность введения в эксплуатацию рекомендаций касательно политики безопасности, разработанных во втором разделе.

Практическое значение проекта состоит в повышении информационной безопасности ООО "АртКасл".

ПОЛИТИКА БЕЗОПАСНОСТИ, МОДЕЛЬ УГРОЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УЯЗВИМОСТИ.

THE ABSTRACT

Explanatory note: 85 p., 9 fig., 14 tab., 4 appendices, 15 sources.

Object of elaboration: information security policy for information and telecommunication system of "ArtCastle" LLC.

The purpose of the project: increasing the level of information security in ITS "ArtCastle" LLC, creation of solutions for protection against threats to information security.

In the first section the object has been described: type of activity, the physical environment in which the object is located, equipment, information system, software, information flows. The classification of information that circulates in the ITS has been made, the list of threats sources, the list of vulnerabilities and the list of threats relevant to ITS have been defined.

In the second section has been described the security criteria available in the ITS and selected new additional recommended security criteria, have been created recommendations for security policy sections that ensure the implementation of the recommended security criteria and protection from current threats.

In the third section, the costs of implementation and annual support of the means and measures, described in the proposed sections of the security policy, have been calculated, and possible losses from the realization of relevant threats have been defined. The economic benefit of safety policy recommendations, developed in the second section, implementation has been determined.

The practical significance of the project is to increase information security of "ArtCastle" LLC.

SECURITY POLICY, MODEL OF THREATS, INFORMATION SECURITY, VULNERABILITIES.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ІТС – інформаційно-телекомунікаційна система;

КСЗІ – комплексна система захисту інформації;

НД ТЗІ – нормативний документ в галузі технічний захист інформації;

ОІД – об'єкт інформаційної діяльності;

ПЗ – програмне забезпечення;

ТОВ – товариство з обмеженою відповідальністю.

ЗМІСТ

ВСТУП

В кожній ІТС існує така інформація, властивості якої, а саме конфіденційність, цілісність та/або доступність, потрібно зберегти згідно з законодавством України або згідно з інтересами власника системи. Для того, щоб захистити інформацію від небажаного ознайомлення, модифікації, видалення, тощо, в організаціях в тому числі створюється політика безпеки інформації. Створенням такої політики повинен займатись фахівець з інформаційної безпеки.

Для того, щоб створити політику безпеки, необхідно спочатку проаналізувати існуючі на ОІД умови, зробити висновок щодо можливих вразливостей, джерел загроз та загроз, оцінити їх критичність та визначити умови, за яких можна ними знехтувати. На основі цих досліджень можна буде зробити висновок, які питання мають бути розглянуті в політиці безпеки.

Для забезпечення ефективності політики безпеки, необхідно, щоб у ній були зазначені чіткі правила та інструкції для кожного відповідального робітника, вказана відповідальність та можливі штрафні санкції у разі невиконання вимог. Політика повинна бути завжди актуальною, тому її необхідно періодично оновлювати, розробляти нові її розділи, тощо, у відповідності до нових умов функціонування ІТС, нових викликів та нових потреб.

Таким чином, мета цієї роботи зводиться до розробки необхідних розділів політики безпеки, що забезпечуватимуть захист від існуючих в ІТС загроз. Для того, щоб створити такі розділи, необхідно, як вже було зазначено, проаналізувати існуючі на ОІД умови і зробити відповідні висновки, що і було зроблено. Отримані результати показують, з якими загрозами інформаційній безпеці можуть зіткнутися, зокрема, дизайнерські компанії, як можуть бути знижені відповідні ризики та які профілактичні заходи можуть бути застосовані.

Процес створення КСЗІ, у тому числі обстеження ОІД та розробку політики безпеки інформації, описано в НД ТЗІ 3.7-003 -2005 «Порядок

проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». Для визначення функціонального профілю АС використовується НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» та НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу».

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загальні відомості про ОІД

Об`єктом інформаційної діяльності є дизайнерське агентство ТОВ «ArtCastle», що спеціалізується на мобільному та веб-дизайні, брендингу, і знаходиться за адресою: Дніпропетровська область, м. Дніпро, пр. Гагаріна, буд. 21, 3 поверх. Будівля, де розташована організація – чотириповерхова. Організація надає наступні послуги:

– web & mobile design (веб-дизайн та дизайн мобільних додатків) – компанія створює ефективний UX у поєднанні з інтерфейсом для додатків і веб-сайтів. При розробці цих продуктів організація виконує функції аутсорсингової компанії і працює з зовнішніми компаніями розробників, які надають вимоги до продуктів і з якими обговорюються дані проекти;

– branding (брендинг) - логотипи, образи і брендинг. Продукту надається власний образ.

Організація працює з понеділка по п'ятницю. Вихідні дні – субота та неділя. Графік роботи з понеділка по п’ятницю з 9.00 до 18.00 (з перервами по півгодини у 12:00 та у 15:30). Прибирання приміщення проводиться з понеділка по п`ятницю з 15:30 до 16:00.

Ключі від офісу знаходяться у директора та у системного адміністратора. На неробочий час приміщення здається під охорону охоронному агентству «Орлан».

1.2 Обґрунтування необхідності створення КСЗІ

Згідно з НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі»:

«6.1.1.1 Підставою для визначення необхідності створення КСЗІ є норми та вимоги чинного законодавства, які встановлюють обов’язковість обмеження доступу до певних видів інформації або забезпечення її цілісності чи

доступності, або прийняте власником інформації рішення щодо цього, якщо нормативно-правові акти надають йому право діяти на власний розсуд.

6.1.1.2 Вихідні дані для обґрунтування необхідності створення КСЗІ у загальному випадку одержуються за результатами:

– аналізу нормативно-правових актів (державних, відомчих та таких, що діють в межах установи, організації, підприємства), на підставі яких може встановлюватися обмеження доступу до певних видів інформації чи заборона такого обмеження, або визначатися необхідність забезпечення захисту інформації згідно з іншими критеріями;

– визначення наявності у складі інформації, яка підлягає автоматизованій обробці, таких її видів, що потребують обмеження доступу до неї або забезпечення цілісності чи доступності відповідно до вимог нормативно-правових актів;

– оцінки можливих переваг (фінансово-економічних, соціальних і т.п.) експлуатації ІТС у разі створення КСЗІ.» [1]

Отже, згідно з прийнятим власником інформації рішенням, на підприємстві необхідно створити КСЗІ, оскільки в ІТС обробляється інформація, що є комерційною таємницею, та інформація, захист якої передбачається договорами між клієнтами та компанією. Також, необхідно захищати інформацію, що становить персональні дані клієнтів та робітників, згідно з Законом України «Про захист персональних даних»:

«Стаття 24. Забезпечення захисту персональних даних

1 Володільці, розпорядники персональних даних та треті особи зобов’язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних.» [2]

Крім того, компанія планує розширювати ринок збуту, співпрацювати, в тому числі, з закордонними компаніями. Тому необхідно впроваджувати захист інформації на належному рівні для підвищення рівня довіри з боку клієнтів.

1.3 Обстеження ОІД

1.3.1 Обстеження фізичного середовища ОІД

Стіни будівлі, в якій знаходиться ОІД, – цегляні та покриті армованим бетоном. Фундамент – плитний, дах – покритий руберойдом, територія навколо будівлі покрита асфальтом. Ситуаційний план наведено на рисунку 1.1. На рисунку 1.2 наведено комунікації у будівлі, де розташовано ІТС.

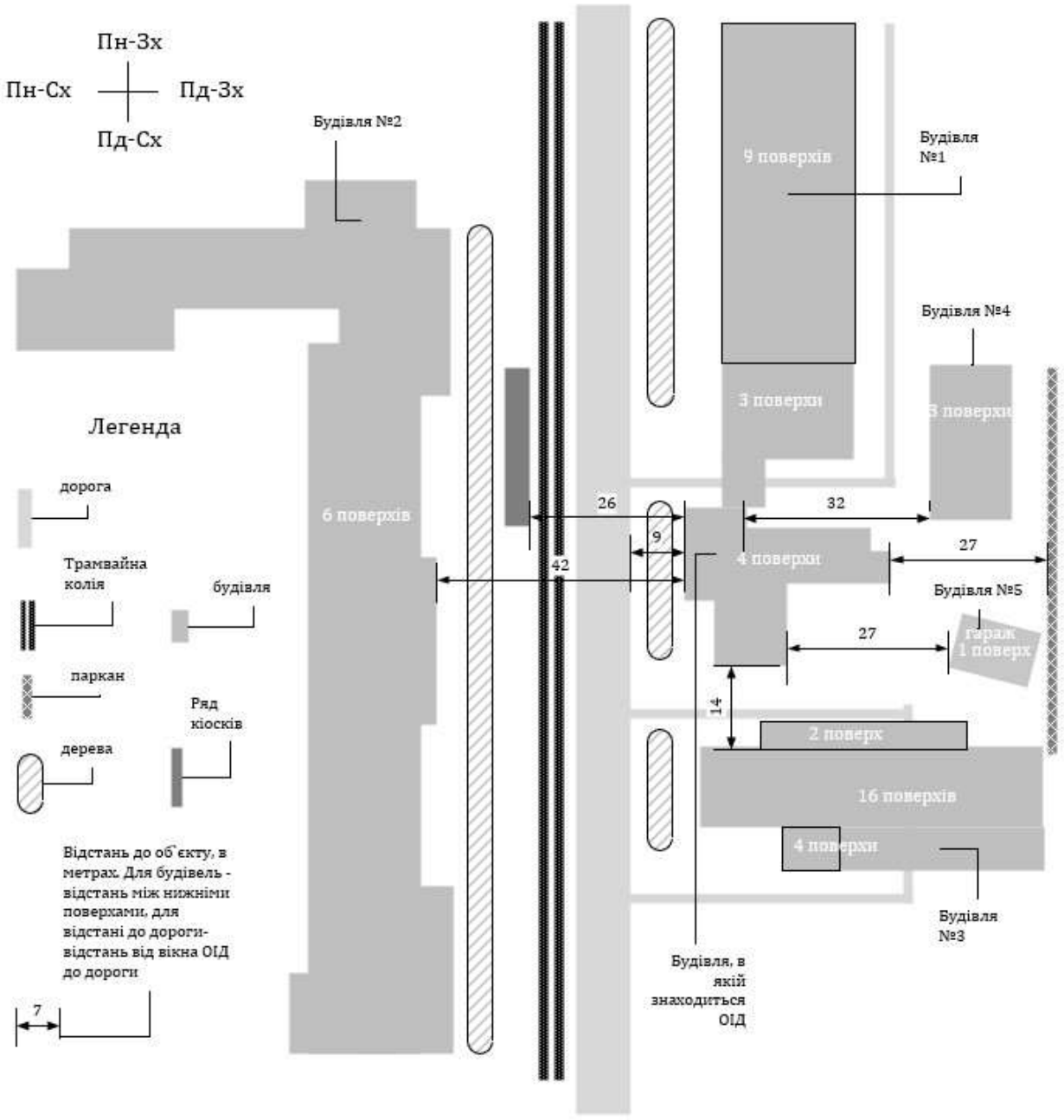

Рисунок 1.1 – Ситуаційний план

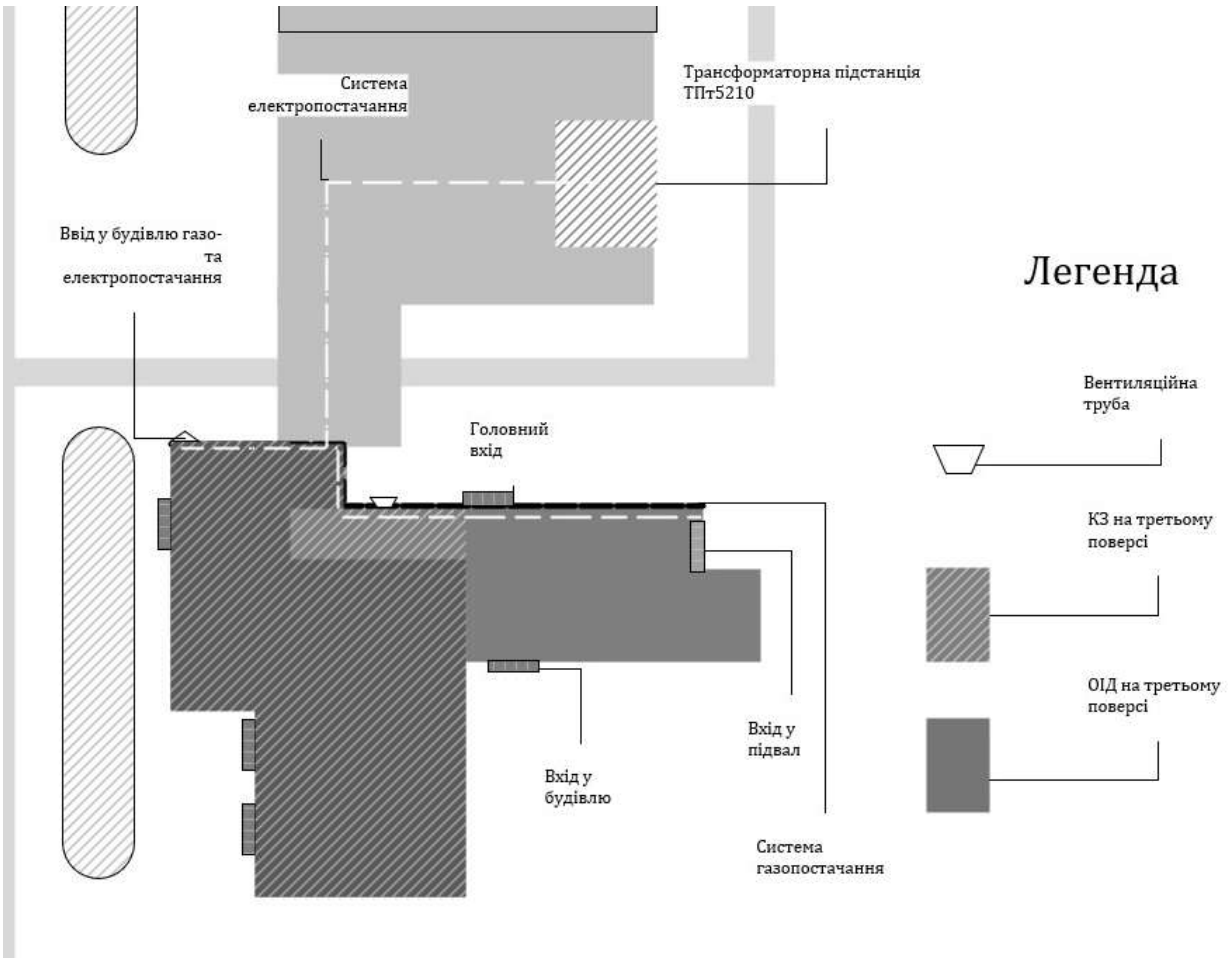

Рисунок 1.2 – Комунікації

На заході від ОІД знаходиться проспект Гагаріна, найкоротша відстань до нього - 9м. На проспекті інтенсивно рухається транспорт, ширина проїзної частини – близько 10м, 2 полоси руху в кожний бік. В таблиці 1.1 наведено будівлі, що знаходяться поруч з ОІД.

Таблиця 1.1 – Будівлі, що знаходяться поруч з ОІД

Порядковий номер	Тип об`єкту	Адреса	Розташування відносно ОІД	Мінімальна відстань до ОІД	Додатково
1	Національна металургійна академія України	пр. Гагаріна,17	Пн-Сх	0м	

Продовження таблиці 1.1

Порядковий номер	Тип об`єкту	Адреса	Розташування відносно ОІД	Мінімальна відстань до ОІД	Додатково
2	Український державний хіміко-технологічний університет	пр. Гагаріна, 8	Зх	42м	
3	Адміністративно-житловий комплекс	пр. Гагаріна, 23	Пд	10м	В будівлі знаходиться кафе «Пузата хата», його вікна виходять на ОІД
4	Покинута будівля	пр. Гагаріна, 19	Сх	32м	
5	Гараж		Пд-Сх	27м	

Внутрішні та зовнішні стіни офісу -цегляні. Товщина зовнішніх стін -380 мм, внутрішніх несних стін -250 мм, внутрішніх перегородок – 65 мм. Вікна - металопластикові, подвійні, 2100 х 1500 мм. Вхідні двері – алюмінієві – 1000 мм шириною і висотою 2100 мм. Замок - моноблок тринаправленого закривання зі сталі, закривається вбудованим циліндром з унікальним розміщенням пінів в трьох площинах. Міжкімнатні двері – дерев`яні 90 х 2100 мм і 80 х 2100 мм. Офіс має висоту 3 м (від підлоги до стелі), присутня натяжна стеля. Підлога на підприємстві – ковролін і плитка.

На південному заході від офісу знаходяться магазин одягу і сервісний центр, що спеціалізується на ремонті комп`ютерів. На другому поверсі (знизу ОІД) знаходиться салон краси. На четвертому (зверху ОІД) – приміщення ремонтується (планується офіс).

У нічний час на підприємстві працює відеоспостереження – камери спрямовані на двері всередині будівлі і по периметру будівлі ззовні. На підприємстві у нічний час працюють інфрачервоні датчики руху.

Сигналізація передає сигнал про несанкціонований доступ на пульт охоронного агентства «Орлан». На рисунку 1.3 наведено генеральний план ОІД. На рисунку 1.4 представлено комунікації, що знаходяться всередині будівлі.

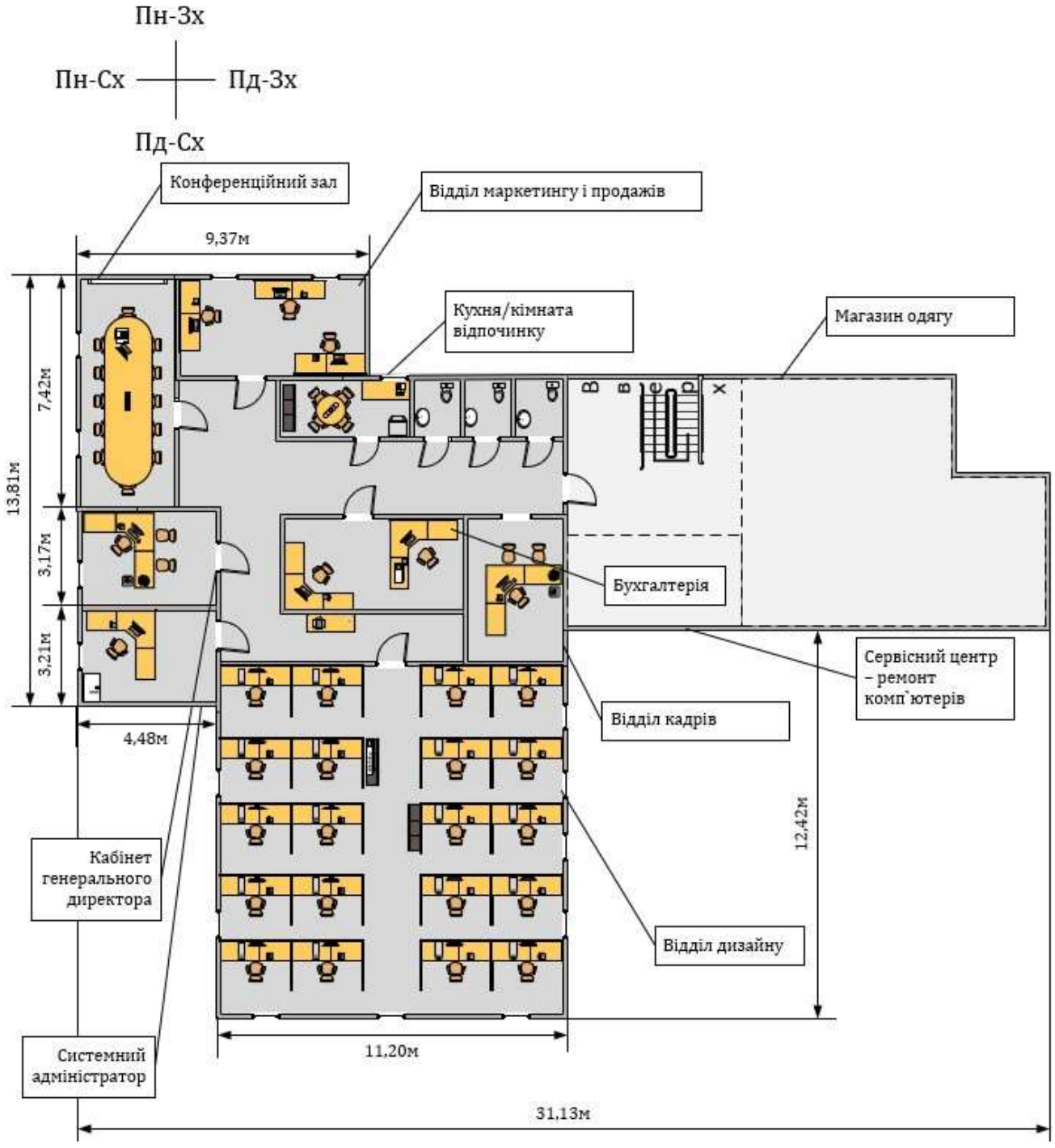

Рисунок 1.3 – Генеральний план ОІД

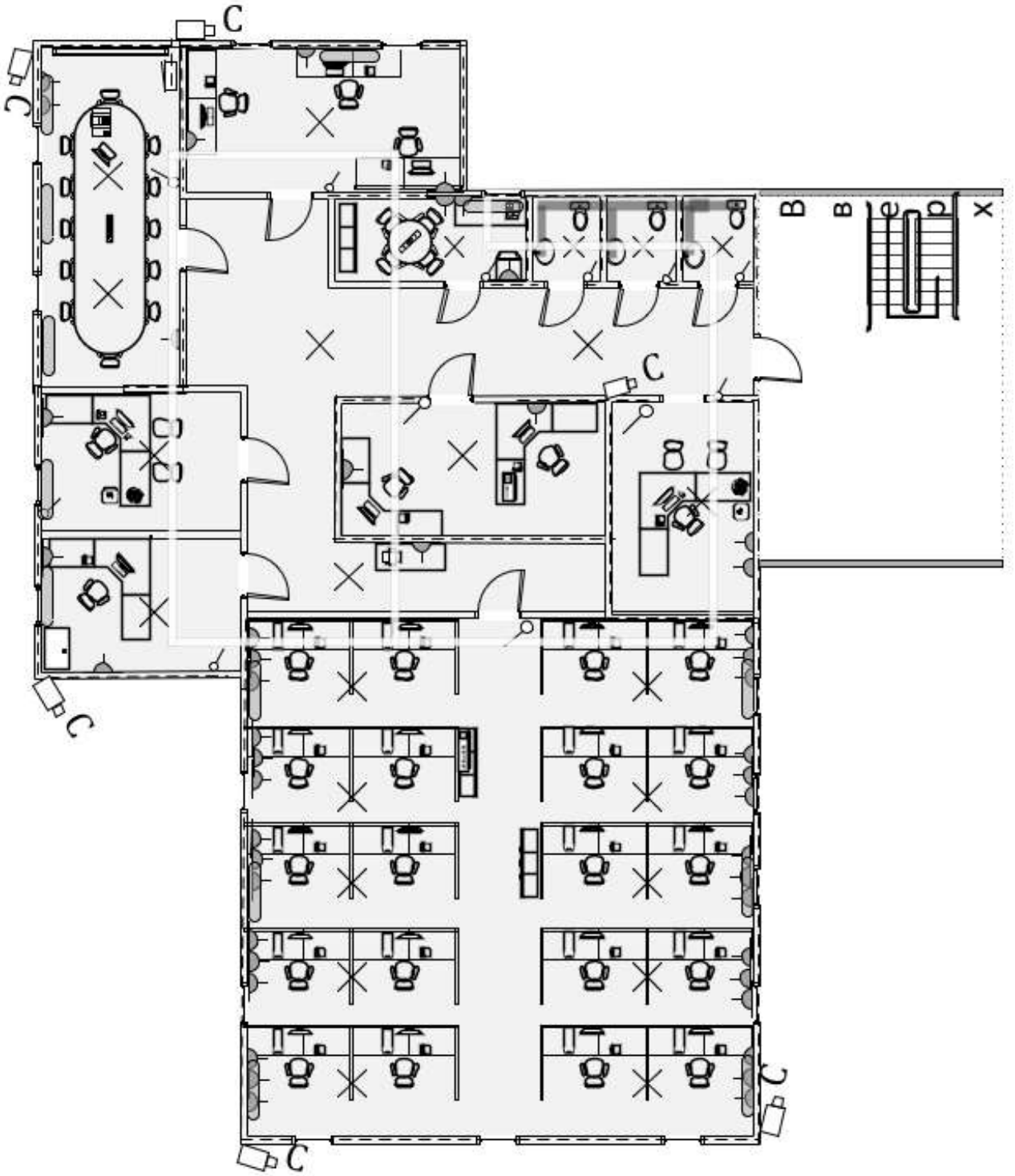

Рисунок 1.4 – Комунікації всередині будівлі

На рисунку 1.5 представлено легенду генерального плану ОІД.

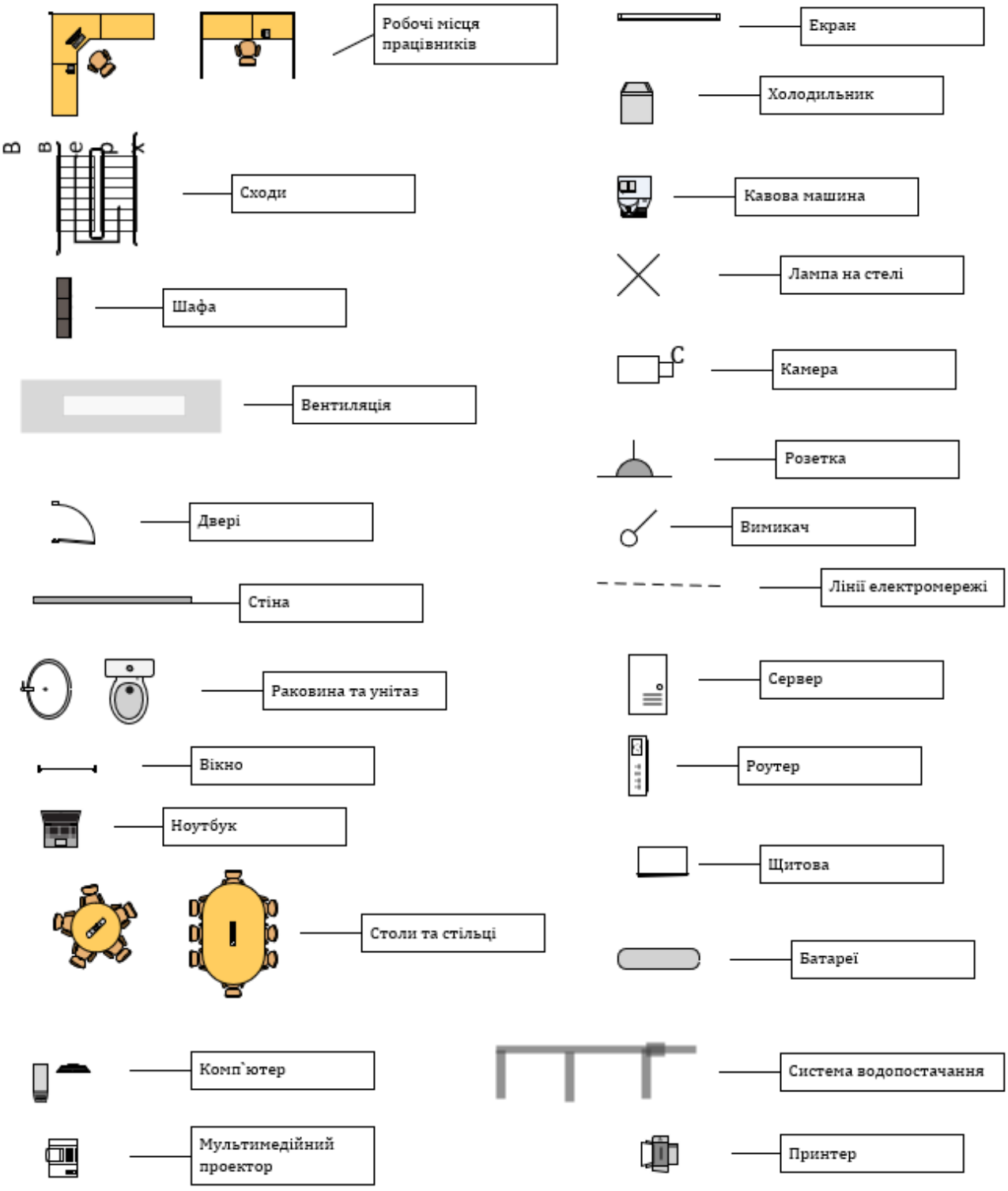

Рисунок 1.5 – Легенда генерального плану

На рисунку 1.6 зображено систему сигналізації на ОІД.

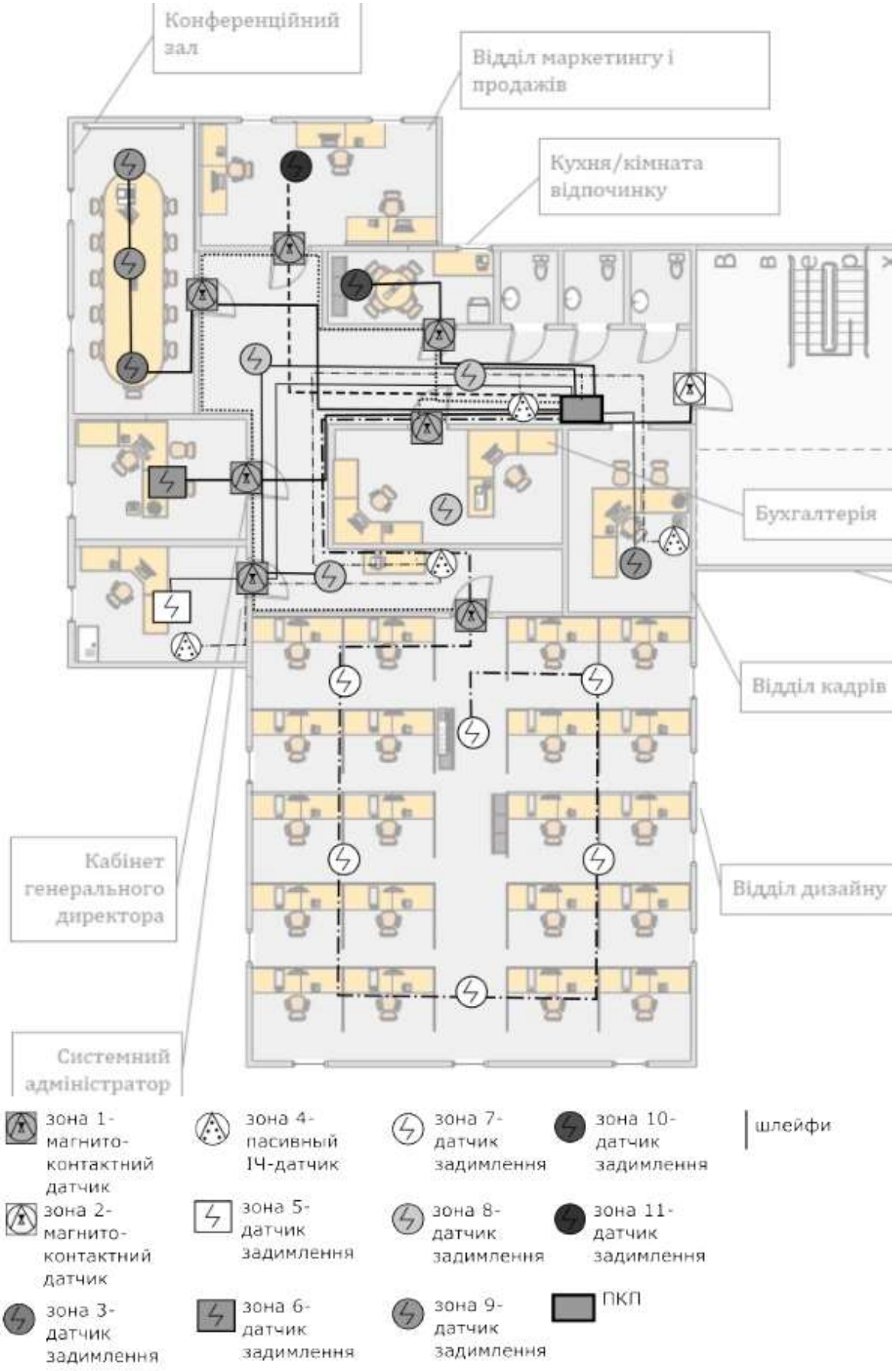

Рисунок 1.6 – система сигналізації

У таблиці 1.2 наведено опис основних технічних засобів, що присутні на ОІД.

Таблиця 1.2 – Опис основних технічних засобів

Тип	Модель	Місцезнаходження	Мінімальна відстань до межі ОІД або ліній, що виходять за межі ОІД, м	Кількість	Серійний номер
Системний блок	Patriot Optim Mini N3150/60	Відділ дизайну	0,5	20	333233451-333233471
Клавіатура	HyperX Alloy Core RGB	Відділ дизайну	1	20	333233463-333233483
Ноутбук	HP 250 G6 (4LT72ES) Dark Ash	Відділ кадрів	1,5	9	123233460-123233469
		бухгалтерія	2,5		
		кабінет генерального директора	1,5		
		відділ маркетингу і продажів	0,5		
		конференційний зал	1		
		кабінет системного адміністратора	1,5		

Продовження таблиці 1.2

Тип	Модель	Місцезнаходження	Мінімальна відстань до межі ОІД або ліній, що виходять за межі ОІД	Кількість	Серійний номер
Миша	Logitech B100 USB Black	Відділ кадрів	1,5	9	123233423-123233432
		бухгалтерія	2,5		
		кабінет генерального директора	1,5		
		відділ маркетингу і продажів	0,5		
		конференційний зал	1		
		кабінет системного адміністратора	1		
Принтер	Принтер лазерный Samsung SL-C430W с Wi-Fi	Коридор	0,5	1	456789345
Миша	Asus ROG Strix Impact USB Black	Відділ дизайну	0,5	20	333233458-333233478
Роутер	TP-LINK TL-WR940N	Бухгалтерія	1	1	223454567

Продовження таблиці 1.2

Тип	Модель	Місцезнаходження	Мінімальна відстань до межі ОІД або ліній, що виходять за межі ОІД	Кількість	Серійний номер
Комутатор	TP-LINK TL-SF1024D	Відділ дизайну	1,5	1	445786578
Графічний планшет	Wacom Intuos Pro L	Відділ дизайну	1	20	113233460-113233480
Монітор	PHILIPS 328E9FJAB	Відділ дизайну	1	20	121233451-121233471
Мультимедійний прооектор	Epson EB-X05	Конференційний зал	1,5	1	123654245
Сервер	Сервер DELL PowerEdge T30 (210-T30-PR-3Y)	Кабінет системного адміністратора	0,5	1	431246909

Паперові носії інформації знаходяться у ящиках столів і в шафах в дизайнерському відділі, знімні носії та бездротові мережеві адаптери для підключення до wi-fi знаходяться в ящиках столів. Знімні носії та бездротові мережеві адаптери забороняється виносити з організації.

1.3.2 Обстеження обчислювальної системи ОІД

На підприємстві використовуються 20 комп`ютерів, 9 ноутбуків, 1 wi-fi роутер, 1 сервер, 1 мультимедійний проектор, 1 принтер. З ноутбуками і комп`ютерами працюють закріплені за ними користувачі (окрім ноутбуку в конференційній залі – за нього відповідає системний адміністратор або працівник, що бере його для проведення презентацій чи конференцій). Компанія

використовує хмарні сховища OneDrive для роботи з клієнтами і для внутрішньої роботи. Віддалені користувачі – відсутні за нормального режиму роботи компанії. На рисунку 1.3 зображено структурну схему мережі організації, взаємозв'язок пристроїв та мереж між собою.

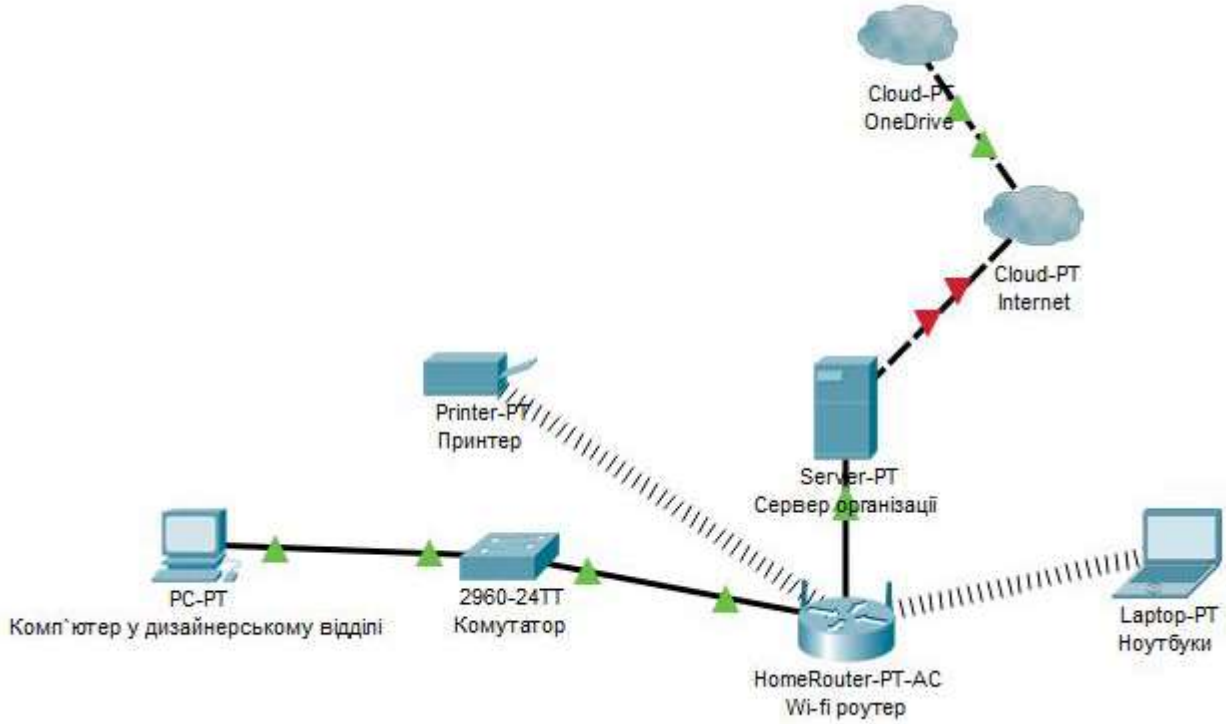

Рисунок 1.7 – Структурна схема мережі організації

Усі користувачі мають доступ в Інтернет, користувачі комп`ютерів використовують провідне підключення для зв'язку з мережею. Топологія мережі – «зірка», усі ноутбуки, комутатор, сервер та принтер підключені до одного wi-fi роутеру. Усі комп'ютери підключені до комутатора за допомогою витої пари. Структурна схема мережі приведена на рис.3. Сервер є контролером домену і керує протоколами: DNS, FTP, роутер керує протоколом DHCP. Як правило, DHCP вимкнено і IP-адреси статичні, дозволено підключення до wi-fi саме для цих адрес. Пароль від wi-fi відомий лише системному адміністратору. У таблиці 1.3 наведено опис пристроїв, що наявні в ІТС, а також їх компонентів.

Таблиця 1.3 – Опис пристроїв та їх компонентів

Комп`ютер	Процесор: Intel Celeron N3150 (1.6 ГГц) Кількість ядер: 4 Об`єм оперативної пам`яті: 4 ГБ DDR 4 SSD: 60 ГБ, HDD: 940 ГБ Порти: 3 USB, вихід для навушників, вхід для мікрофону, порт для підключення клавіатури, порт для миші, HDMI, LAN Додаткові компоненти: блок безперебійного живлення Відеокарта: GeFore 1050
Ноутбук	Процесор: Intel Core i3-7020U (2.3 ГГц) Кількість ядер: 2 Об`єм оперативної пам`яті: 4 ГБ DDR 4 HDD: 1 ТБ Порти: 3 USB, VGA, HDMI, LAN, вихід для навушників. Додаткові можливості: веб-камера, мікрофон, стерео динаміки -вбудовані Мережеві адаптери: Wi-Fi 802.11ac, Bluetooth 4.2, Gigabit Ethernet
Сервер	Процесор: Intel Xeon E3-1225v5 Кількість ядер: 4 Частота процесора: 3.3GHz Пам`ять: 8GB DDR4 Жорсткий диск: 1 TB SATA
Роутер	Захист інформації: WPA, WPA-PSK, WPA2 Наявні мережеві функції: DHCP-сервер, підтримка VPN, віддалене керування
Комутатор	Інтерфейси: 24 x RJ-45 10/100 Мбіт/с з авто-MDI/MDIX

Операційна система на комп`ютерах і ноутбуках: Windows 10 Enterprise (версія 10.0.17763), операційна система на сервері: Windows Server 2016. Ці операційні системи є ліцензійними. На підприємстві є 10 знімних носіїв (9 USB-накопичувачів і 1 зовнішній жорсткий диск) У таблиці 1.4 наведено опис встановленого ПЗ та зазначені його характеристики.

Таблиця 1.4 – Опис встановленого в ІТС ПЗ

Тип ПЗ	Повна назва	Версія	Ліцензія	Де встановлено
Системне, спеціалізоване	Windows Defender	10.0.17763.1	корпоративна	Всі комп`ютери і ноутбуки
Прикладне	Adobe Photoshop	20.0	корпоративна	Комп`ютери у відділі дизайну
Прикладне	Adobe Illustrator	23.0.1	-	Комп`ютери у відділі дизайну
Прикладне	Inkskape	0.92.4	GNU	Комп`ютери у відділі дизайну

Продовження таблиці 1.4

Тип ПЗ	Повна назва	Версія	Ліцензія	Де встановлено
Спеціалізоване	Wireshark	2.6.5	GNU GPL	Ноутбук системного адміністатора
Спеціалізоване	CCleaner	5.50.0.6911	Free Edition	Ноутбук системного адміністатора
Спеціалізоване	Total Network Inventory 3	3.6.0	-	Ноутбук системного адміністатора
Спеціалізоване	Total Software Deployment 2	1.1.2	-	Ноутбук системного адміністатора
Прикладне	Microsoft SharePoint	3.6.0	корпоративна	Сервер
Прикладне	Microsoft Teams	1416	корпоративна	Всі комп`ютери і ноутбуки
Прикладне	Microsoft Outlook	3.0.34	корпоративна	Всі комп`ютери і ноутбуки
Системне, прикладне	Microsoft Edge	44.17763.1.0	корпоративна	Всі комп`ютери і ноутбуки
Прикладне	MS Office 365 ProPlus	1808	корпоративна	Всі комп`ютери і ноутбуки
Прикладне	Microsoft OneDrive	19.012.0121.0011	корпоративна	Всі комп`ютери і ноутбуки
Прикладне	1С: Бухгалтерія	8.1	однокористувачева ліцензія – 2 шт.	Ноутбуки бухгалтерів

1.3.3 Інформаційне середовище ОІД

В таблиці 1.5 вказано документи, що зберігаються та циркулюють на підприємстві, режим доступу до них, правовий режим та місце їх зберігання (в електронному та паперовому вигляді).

Таблиця 1.5 – Інформація, що циркулює на об`єкті

№	Інформація	Режим доступу	Правовий режим	Де зберігається

№	Інформація	Режим доступу	Правовий режим	Де зберігається
1	Накази директора	Відкрита	Відкрита	В електронному вигляді: сервер, ноутбук генерального директора. У паперовому вигляді: у шафі генерального директора
2	Інформація щодо нових замовлень	З обмеженим доступом	Комерційна таємниця	В електронному вигляді: сервер, ноутбуки у відділі маркетингу і продажів, комп`ютери у відділі дизайну, за якими працюють виконавці проекту У паперовому вигляді: у шухлядах виконавців
3	Статистика продажів	З обмеженим доступом	Комерційна таємниця	В електронному вигляді: сервер, ноутбук генерального директора, ноутбуки у відділі маркетингу та продажів
4	Документи щодо проведених фінансових операцій	З обмеженим доступом	Конфіденційна	В електронному вигляді: ноутбуки у бухгалтерії, знімні носії у бухгалтерії, ноутбук генерального директора
5	Готова продукція	З обмеженим доступом	Комерційна таємниця	В електронному вигляді: комп`ютери виконавців у відділі дизайну, хмарне сховище OneDrive (також використовується для передачі цієї інформації клієнтам), сервер

Продовження таблиці 1.5

№	Інформація	Режим доступу	Правовий режим	Де зберігається

№	Інформація	Режим доступу	Правовий режим	Де зберігається
6	Готова продукція через певний період після передачі клієнту, за домовленості з клієнтом	Відкрита	Відкрита	Сервер, хмарне сховище OneDrive
7	Ескізи, роботи в процесі	З обмеженим доступом	Комерційна таємниця	В електронному вигляді: комп`ютери виконавців у відділі дизайну, хмарне сховище OneDrive, сервер, знімні носії у дизайнерському відділі
8	Дані щодо стану локальної мережі, журнали подій	З обмеженим доступом	Конфіденційна	В електронному вигляді: ноутбук системного адміністратора
9	Дані щодо замовників	З обмеженим доступом	Конфіденційна	В електронному вигляді: ноутбуки у відділі маркетингу і продажів, сервер
10	Персональні дані працівників	З обмеженим доступом	Конфіденційна	В електронному вигляді: ноутбук у відділі кадрів
11	Дані про зарплату	З обмеженим доступом	Конфіденційна	В електронному вигляді: ноутбуки у бухгалтерії, знімні носії у бухгалтерії, ноутбук генерального директора. У паперовому вигляді: шафа генерального директора.
12	Дані ідентифікації та аутентифікації	З обмеженим доступом	Конфіденційна	В електронному вигляді: всі комп`ютери і ноутбуки, сервер

Продовження таблиці 1.5

№	Інформація	Режим доступу	Правовий режим	Де зберігається
13	Договори з клієнтами	З обмеженим доступом	Комерційна таємниця	В електронному вигляді: комп`ютери виконавців у відділі дизайну, ноутбуки у відділі маркетингу і продажів У паперовому вигляді: у шухлядах столів у відділі маркетингу і продажів, знімні носії у відділі маркетингу і продажів
14	Звіт системного адміністратора	З обмеженим доступом	Конфіденційна	В електронному вигляді: ноутбук системного адміністратора, ноутбук генерального директора

На підприємстві відсутні правила зберігання, використання, переміщення знімних носіїв інформації. Відсутні також спеціальні місця зберігання знімних носіїв – сейфи або шафи, тощо.

Таблиця 1.6 – Визначення рівня конфіденційності, цілісності та доступності інформації

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Накази генерального директора	К0	Ц3	Д2
Інформація щодо нових замовлень	К1	Ц4	Д4
Статистика продажів	К1	Ц1	Д1
Документи щодо проведених фінансових операцій	К3	Ц4	Д3
Готова продукція	К4	Ц4	Д4
Готова продукція через певний період після передачі клієнту, за домовленості з клієнтом	К0	Ц3	Д1

Продовження таблиці 1.6

Інформація	Рівень конфіденційності	Рівень цілісності	Рівень доступності
Ескізи, роботи в процесі	К4	Ц1	Д3
Дані щодо стану локальної мережі, журнали подій	К3	Ц3	Д3
Дані щодо замовників	К4	Ц3	Д3
Персональні дані працівників	К4	Ц2	Д2
Дані про зарплату	К2	Ц4	Д4
Дані ідентифікації та аутентифікації	К3	Ц3	Д3
Договори з клієнтами	К3	Ц4	Д4
Звіт системного адміністратора	К2	Ц1	Д1

Рівні конфіденційності:

– К0- рівень, при якому можна знехтувати втратою конфіденційності, або при якому інформація не є конфіденційною;

– К1- рівень, при якому компанія зазнає незначних збитків при втраті конфіденційності;

– К2- рівень, при якому організація зазнає відчутних збитків;

– К3- рівень, що може призвести до значних матеріальних втрат або до значної втрати репутації організації;

– К4- рівень, що може призвести до закриття компанії.

Рівні цілісності:

– Ц0- рівень, при якому можна знехтувати втратою цілісності інформації;

– Ц1- рівень, при якому компанія зазнає незначних збитків при втраті цілісності;

– Ц2- рівень, при якому організація зазнає відчутних збитків;

– Ц3- рівень, що може призвести до значних матеріальних втрат або до значної втрати репутації організації;

– Ц4- рівень, що може призвести до закриття компанії.

Рівні доступності:

– Д0- рівень, при якому можна знехтувати втратою доступності інформації;

– Д1- рівень, при якому компанія зазнає незначних збитків при втраті доступності;

– Д2- рівень, при якому організація зазнає відчутних збитків;

– Д3- рівень, що може призвести до значних матеріальних втрат або до значної втрати репутації організації;

– Д4- рівень, що може призвести до закриття компанії.

1.3.4 Середовище користувачів ІТС

Обов`язки працівників та відділів:

Генеральний директор:

– затвердження документів на оплату праці працівників;

– прийняття рішень щодо приймання на роботу, звільнення та заохочення працівників, поліпшення їх мотивації;

– забезпечення ефективної взаємодії всіх структурних підрозділів організації, контроль їх діяльності;

– прийняття рішень щодо зміни вектору розвитку підприємства, відстеження місця, яке посідає компанія на ринку;

– контроль та гарантування виконання зобов`язань компанії перед клієнтами;

– вживання заходів щодо покращення умов праці на підприємстві.

Системний адміністратор:

– слідкування за станом локальної мережі, підтримання її в належному стані;

– встановлення необхідного ПЗ, його оновлення;

– перевірка журналів подій;

– відповідальність за інформаційну безпеку на підприємстві, проведення необхідних заходів та відповідна модернізація системи;

– відповідальність за резервне копіювання, відновлення системи після збоїв;

– встановлення і конфігурування оновлень операційної системи;

– керування сервером.

Бухгалтерія:

– ведення обліку фінансової діяльності підприємства – документації щодо закупівель та продажу на підприємстві, оформлення накладних;

– співпраця з податковими органами;

– нарахування заробітньої платні, перерахування коштів за виконання робіт, тощо. Ведення відповідної документації.

Менеджер по персоналу:

– забезпечення компанії новими працівниками за необхідності, проведення відповідних конкурсів та співбесід;

– перевірка профілів у соціальних мережах з метою виявлення несанкціоновано завантажених конфіденційних матеріалів (зокрема, робіт дизайнерів, ескізів і т.д.);

– контроль виконання внутрішнього трудового розпорядку організації;

– підвищення кваліфікації робітників, їх навчання, за необхідності – перекваліфікація;

– надання рекомендацій щодо підвищення та звільнення робітників.

Відділ маркетингу і продажів:

– визначення цін на продукцію компанії;

– реклама продукції та послуг підприємства, розповсюдження відповідної інформації;

– контроль виконання зобов`язань компанії перед клієнтами;

– аналіз ситуації на ринку, аналіз перспектив компанії, а також ризиків;

– укладання угод з клієнтами;

– проведення заходів щодо забезпечення своєчасного надходження коштів за реалізовану продукцію організації.

Відділ дизайну:

– виконання зобов`язань перед клієнтом, створення продукції компанії-логотипів, макетів веб-сторінок, необхідних ілюстрацій та анімації, іконок, тощо (голова відділу дизайну та проджект-менеджери контролюють виконання робіт та спілкуються з клієнтами для затвердження ескізів та внесення правок).

Прибиральниця:

– прибирання приміщення підприємства у встановлений час.

Переміщення документів на підприємстві здійснюється за допомогою електронної пошти, знімних носіїв або засобами серверу та хмарного сховища.

На рисунку 1.4 зображено як, від кого і до кого передається інформація (документи) на підприємстві.

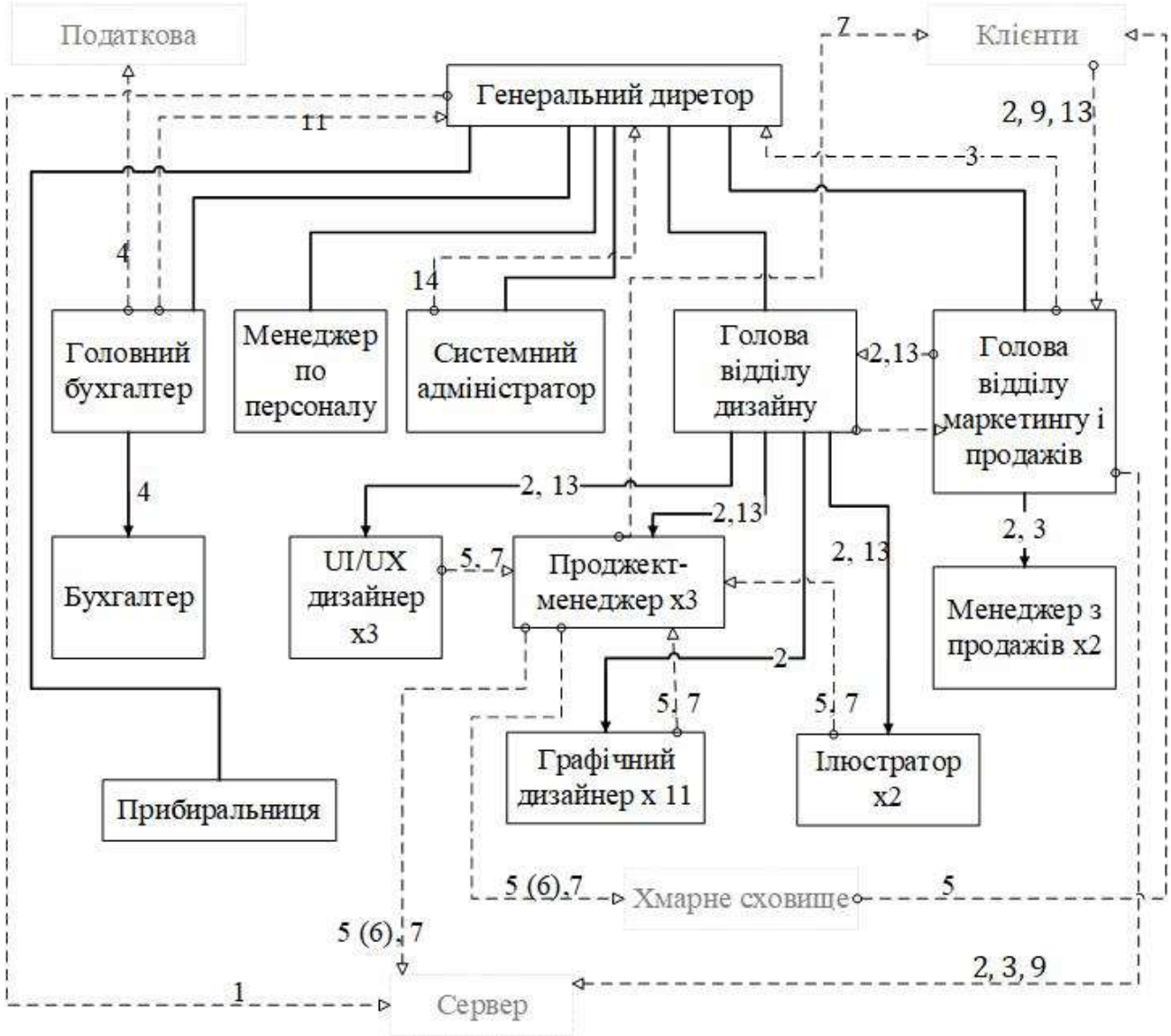

Рисунок 1.8 - Інформаційні потоки на підприємстві

Перелік документів та ПЗ (див. Рисунок 1.8, Таблиця 1.7):

1 Перелік документів;

1.1 Накази директора;

1.2 Інформація щодо нових замовлень;

1.3 Статистика продажів;

1.4 Документи щодо проведених фінансових операцій;

1.5 Готова продукція;

1.6 Готова продукція через певний період після передачі клієнту, за домовленості з клієнтом;

1.7 Ескізи, роботи в процесі;

1.8 Дані щодо стану локальної мережі, журнали подій;

1.9 Дані щодо замовників;

1.10 Персональні дані працівників;

1.11 Дані про зарплату;

1.12 Дані ідентифікації та аутентифікації;

1.13 Договори з клієнтами;

1.14 Звіт системного адміністратора;

2 Перелік ПЗ;

2.1 Windows Defender;

2.2 Adobe Photoshop;

2.3 Adobe Illustrator;

2.4 Inkskape;

2.5 Microsoft Edge;

2.6 MS Office 365 ProPlus;

2.7 Microsoft OneDrive;

2.8 1С: Бухгалтерія;

2.9 Wireshark;

2.10 CCleaner;

2.11 Total Network Inventory 3;

2.12 Total Software Deployment 2;

2.13 Microsoft SharePoint;

2.14 Microsoft Teams;

2.15 Microsoft Outlook.

У таблиці 1.7 наведено матрицю доступу до інформації та ПЗ в ІТС.

Таблиця 1.7 Матриця доступу

Користувачі	Інформація	ПЗ	Елементи КС
Генеральний директор	1.1- с, в, к, ч, з, д, м 1.2- к, ч, з 1.3- к, з, ч 1.6- ч, к, з 1.11- ч, к, з, д 1.12- з 1.14- ч, к, з	2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним ноутбуком, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером
Головний бухгалтер	с, к, ч, з 6- ч, к, з 11- с, к, ч, з, м 12- з	2.5- вик 2.6- вик 2.7- вик 2.8- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним ноутбуком, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі
Бухгалтер	4- с, к, ч, з 6- ч, к, з 11- к, ч, з, м 12- з	2.5- вик 2.6- вик 2.7- вик 2.8- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним ноутбуком, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі
Системний адміністратор	6- ч, к, з 8- ч, з 12- з 14- с, в, к, ч, з, м	2.1- вик, о, вст 2.2- о, вст 2.3-о, вст 2.4- о, вст 2.5- вик, о 2.6- вик, о, вст 2.7-вик, о, вст 2.8- о, вст 2.9- вик, о, вст 2.10- вик, о, вст 2.11- вик, о, вст 2.12- вик, о, вст	Користування одним ноутбуком, доступ в Інтернет, за необхідності – використання проектора та ноутбуку в конференційній залі, адміністрування сервера, налаштування роутера

Користувачі	Інформація	ПЗ	Елементи КС
		2.13 -вик, о, вст 2.14- вик, о, вст 2.15- вик, о, вст	

Продовження таблиці 1.7

Користувачі	Інформація	ПЗ	Елементи КС
Голова відділу маркетингу і продажів	2- к, ч, з, м с, к, ч, з, м 6- ч, к, з, в 9-с, к, ч, з, м 12- з 13- с, к, ч, з, д, в	2.5 -вик 2.6 -вик 2.7- вик 2.13- вик 2.15- вик 2.15- вик	Користування одним ноутбуком, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером
Менеджер з продажів х2	2- к, з, ч 3- к, з, ч 6- ч, к, з 9-с, к, ч, з, м 12- з 13- к, ч, з	2.5 -вик 2.6 -вик 2.7- вик 2.13- вик 2.15- вик 2.15- вик	Користування одним ноутбуком, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі
Менеджер по персоналу	6- ч, к, з 10- с, в, ч, з, м 12- з	2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним ноутбуком, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі
Голова відділу дизайну	2- к, ч, з, м, д, в 6- ч, к, з 7- к, ч, з, д 12- з 13-к, ч, з, д	2.2- вик 2.3- вик 2.4- вик 2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним комп`ютером і одним графічним планшетом, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером
Проджект-менеджер х3	2- в, к, ч, з, м, д 5- с, к, ч, з ч, к, з в, к, ч, з, м, д, с 12- з 13-к, ч, з, д	2.2- вик 2.3- вик 2.4- вик 2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним комп`ютером і одним графічним планшетом, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером

Продовження таблиці 1.7

Користувачі	Інформація	ПЗ	Елементи КС
Графічний дизайнер х11	2- к, ч, з 5- с, к, ч, з 6- ч, к, з 7- в, к, ч, з, м, д, с 12- з 13-к, ч, з	2.2- вик 2.3- вик 2.4- вик 2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним комп`ютером і одним графічним планшетом, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером
UI/UX дизайнер х3	2- к, ч, з 5- с, к, ч, з 6- ч, к, з 7- в, к, ч, з, м, д, с 12- з 13-к, ч, з	2.2- вик 2.3- вик 2.4- вик 2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним комп`ютером і одним графічним планшетом, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером
Ілюстратор х2	2- к, ч, з 5- с, к, ч, з 6- ч, к, з 7- в, к, ч, з, м, д, с 12- з 13-к, ч, з	2.2- вик 2.3- вик 2.4- вик 2.5- вик 2.6- вик 2.7- вик 2.13- вик 2.14- вик 2.15- вик	Користування одним комп`ютером і одним графічним планшетом, доступ в Інтернет, доступ до сервера по локальній мережі, за необхідності – використання проектора та ноутбуку в конференційній залі, дозволено користування принтером
Прибиральниця	1- ч	-	-

В – видалення/знищення;

К – копіювання;

Ч – читання;

З – зберігання;

М – модифікація;

Д – друк;

С – створення;

Вик – використання (для ПЗ та техніки);

О – оновлення;

Вст – встановлення.

Доступ до ресурсів регламентується наказами директора (зокрема, Наказом «Про доступ до інформації з обмеженим доступом №123 від 02.02.2015» та Наказом «Про доступ до елементів комп`ютерної системи №125 від 05.02.2015», які є частиною існуючої політики безпеки), засобами надання доступу Windows Server 2016 та OneDrive.

Для процесів та програм не встановлено ніяких обмежень щодо взаємодії з інформацією, взаємодії з іншими процесами, операційною системною та апаратною складовою.

1.4 Аналіз загроз інформації

1.4.1 Перелік джерел загроз

Для інформації, що обробляється в ІТС можуть бути характерними такі види джерел загроз:

1 антропогенні;

1.1 внутрішні;

1.1.1 Відділ дизайну;

1.1.2 Бухгалтерія;

1.1.3 Системний адміністратор;

1.1.4 Відділ маркетингу і продажів;

1.1.5 Генеральний директор;

1.1.6 Відділ кадрів;

1.1.7 Прибиральниця;

1.2 Зовнішні;

1.2.1 Конкуренти;

1.2.2 Несумлінні клієнти;

1.2.3 Злочинці і хакери;

2 Техногенні;

2.1 Сервер та ПЗ, що встановлене на ньому;

2.2 Хмарне сховище;

2.3 Ноутбуки та комп’ютери, ПЗ, встановлене на них;

3 Стихійні;

3.1 Пожежа;

3.2 Форс-мажорні обставини – громадські заворушення, воєнні дії, тощо.

У Таблиці 1.8 проводиться аналіз ступеню небезпеки з боку того чи іншого джерела загроз.

Таблиця 1.8 - Ранжування джерел загроз

Джерело загрози	К1	К2	К3	К загальне
Відділ дизайну	5	2	5	0,40
Бухгалтерія	5	2	4	0,32
Системний адміністратор	5	3	4	0,48
Відділ маркетингу і продажів	5	2	5	0,40
Генеральний директор	4	2	3	0,19
Відділ кадрів	4	2	4	0,26
Прибиральниця	3	1	1	0,02
Конкуренти	2	5	5	0,40
Несумлінні клієнти	2	2	2	0,06
Злочинці і хакери	2	4	4	0,26
Сервер та ПЗ, що встановлене на ньому	5	2	4	0,32
Хмарне сховище	5	1	4	0,16
Ноутбуки та комп’ютери, ПЗ, встановлене на них	5	2	3	0,24
Пожежа	2	2	4	0,13
Форс-мажорні обставини – громадські заворушення, воєнні дії, тощо	2	3	3	0,14

К1 – визначає ступінь доступності до об’єкта:

1 – джерело дуже віддалене від об’єктів захисту і не може впливати на нього (для техногенних) / немає доступу до об’єкта (для антропогенних) / на ОІД відсутні будь-які передумови виникнення джерела загрози (для стихійних);

2 – джерело дуже віддалене від об’єктів захисту, але все ще може впливати на нього (для техногенних) / можливо отримати віддалений доступ до об’єкта (для антропогенних) / на ОІД є деякі передумови виникнення джерела загрози, але імовірність їх прояву дуже мала (для стихійних);

3 – джерело знаходиться поблизу будівлі, де знаходиться ОІД, або в тій самій будівлі (для техногенних) / джерело має обмежений доступ до технічних і програмних засобів обробки інформації, що захищається, завдяки введеним обмеженням (для антропогенних) / довгий час не було жодного прояву джерела загрози, втім, є передумови для його появи (для стихійних);

4 – джерело знаходиться в тому ж приміщенні (для техногенних) / джерело має доступ до технічних і програмних засобів обробки інформації, що захищається, але це не є його функціональним обов’язком (для антропогенних) / ОІД не знаходиться у зоні дії катаклізмів, втім, імовірність прояву джерела загрози висока (для стихійних);

5 – сам об’єкт містить джерело загрози (для техногенних) / джерело має повний доступ до технічних і програмних засобів обробки інформації, що захищається, а також максимальні повноваження доступу. (для антропогенних) / ОІД знаходиться у зоні дії катаклізмів (для стихійних).

К2 – присутність необхідних умов, ступінь кваліфікації виконавця та ступінь його бажання реалізувати загрозу:

1 – виконавець постраждає при реалізації загрози; він не має ніяких відповідних можливостей / техніка та ПЗ постійно оновлюються, встановлюється належним чином та постачається надійним виробником / на ОІД немає жодних можливостей для виникнення джерела загрози;

2 – виконавець не постраждає через загрозу, але її виконання не є вигідним для виконавця; він має недостатній рівень знань для реалізації загрози / ПЗ та

техніка оновлюється не постійно / на об’єкті є умови, що запобігають прояву джерела загрози;

3 – виконавцю вигідна реалізація загрози; він може навчитися методам, що реалізують загроз / ПЗ та техніка вразливі для деяких атак / прояв джерела загрози можливий, але швидше за все він не зможе проявити себе;

4 – виконавцю дуже вигідна реалізація загрози; він володіє методами, що реалізують загрози / відсутність оновлень ПЗ або застарілі елементи техніки, ненадійні їх виробники, неякісна техніка / прояв джерела загрози можливий;

5 – мета виконавця; виконавець є експертом у методах, що реалізують загрозу (наприклад, він працює у відповідній сфері); стара або зламана техніка; піратське ПЗ, тощо / умови сприяють прояву джерела загрози.

К3 – фатальність наслідків:

1 – ОІД нічого не втратить, або наслідки будуть позитивними;

2 – Наслідками можна знехтувати;

3 – Наслідки відчутні, але несуттєві;

4 – Наслідки можуть призвести до проблем, вирішення яких потребуватиме значну кількість матеріальних витрат та значну кількість часу;

5 – Наслідки можуть призвести до втрати репутації компанії, недовіри клієнтів та збитків, що можуть призвести до закриття організації.

Проаналізувавши обчислення, можна зробити висновок, що можна знехтувати такими джерелами загроз (К загальне <= 0,20):

- генеральний директор;
- прибиральниця;
- несумлінні клієнти;
- хмарне сховище;
- пожежа;
- форс-мажорні обставини – громадські заворушення, воєнні дії, тощо.

1.4.2 Аналіз вразливостей

На ІТС можуть бути наявні такі вразливості:

1 Об’єктивні;

1.1. Технічні канали витоку інформації;

1.2. Можливість несанкціонованого підключення до бездротової мережі (злам wi-fi);

1.3. Використання неліцензійного ПЗ;

1.4. Відсутність датчиків відкриття вхідних дверей, датчиків відкриття чи розбиття вікон;

2 Суб’єктивні;

2.1 Помилки робітників;

2.2 Відсутність контролю за переміщенням відвідувачів у денний час - відсутність відповідальності певних осіб за несанкціонованим доступом сторонніх осіб до об’єктів, що потребують захисту;

2.3 Здійснення передачі внутрішньої інформації через незахищене середовище, відсутність регламенту щодо каналів передачі інформації між робітниками (сприятливі умови для здійснення фішингу);

2.4 Відсутність відповідальності за невчасне або неналежне встановлення оновлень ПЗ;

2.5 Відсутність регламенту щодо збереження, переміщення, знищення знімних носіїв та користування ними;

3 Випадкові;

3.1 Збій;

3.2 Відмова;

3.3 Псування матеріальних носіїв інформації (наприклад, розмагнічування жорстких дисків).

У таблиці 1.9 наведено вразливості та проведено їх оцінку.

Таблиця 1.9 - Ранжування вразливостей

Вразливість	К1	К2	К3	К загальне
Технічні канали витоку інформації	4	1	3	0,09
Можливість несанкціонованого підключення до бездротової мережі (злам wi-fi)	3	4	1	0,09

Вразливість	К1	К2	К3	К загальне
Використання неліцензійного ПЗ	4	3	2	0,19

Продовження таблиці 1.9

Вразливість	К1	К2	К3	К загальне
Відсутність датчиків відкриття вхідних дверей, датчиків відкриття чи розбиття вікон	3	3	5	0,36
Помилки робітників	2	3	5	0,24
Відсутність контролю за переміщенням відвідувачів у денний час	4	5	5	0,80
Здійснення передачі внутрішньої інформації через незахищене середовище	3	3	5	0,36
Відсутність відповідальності за невчасне або неналежне встановлення оновлень ПЗ	3	2	5	0,24
Відсутність регламенту щодо збереження, переміщення, знищення знімних носіїв та користування ними	5	4	5	0,80
Збій	3	3	5	0,36
Відмова	4	2	5	0,32
Псування матеріальних носіїв інформації	2	2	5	0,16

К1 – ступінь впливу вразливості на фатальність наслідків:

1 – використання вразливості не призведе до серйозних наслідків;

2 – вразливість може призвести до реалізації загрози, але ймовірність цього досить мала;

3 – використання вразливості може призвести до реалізації загрози;

4 – використання вразливості швидше за все призведе до реалізації загрози;

5 – використання вразливості точно призведе до реалізації загрози.

К2 – можливість та зручність використання вразливості:

1 – вразливість неможливо або надзвичайно важко використати;

2 – використання вразливості потребує великої кількості часу та ресурсів;

3 – для використання вразливості необхідні певні умови;

4 – вразливість може використати будь-яка людина, яка володіє необхідними знаннями, вміннями чи привілеями;

5 –вразливість може використати практично будь-хто.

К3 – кількість елементів об’єкта , яким характерна вразливість:

1 – вразливість характерна одному елементу;

2 – вразливість характерна декільком елементам;

3 – вразливість характерна п’ятьом – десятьом елементам;

4 – вразливість характерна десятьом -п’ятнадцятьом ;

5 – вразливість характерна більше ніж п’ятнадцятьом елементам в ІТС.

Проаналізувавши обчислення, можна зробити висновок, що можна знехтувати такими вразливостями (К загальне <= 0,16):

- технічні канали витоку інформації;
- можливість несанкціонованого підключення до бездротової мережі;
- псування матеріальних носіїв інформації.

1.4.3 Аналіз актуальних загроз

У таблиці 1.10 наведено зв'язок загроз безпеці інформації в ІТС з джерелами загроз та порушниками, а також коефіцієнти небезпеки.

Таблиця 1.10 – Матриця загроз

Джерела загроз / Вразливості	Ноутбуки та комп’ютери, ПЗ на них	Бухгалтерія	Системний адміністратор	Відділ маркетингу і продажів	Відділ дизайну	Відділ кадрів	Конкуренти	Злочинці і хакери	Сервер та ПЗ на ньому

Джерела загроз / Вразливості	Ноутбуки та комп'ютери, ПЗ на них	Бухгалтерія	Системний адміністратор	Відділ маркетингу і продажів	Відділ дизайну	Відділ кадрів	Конкуренти	Злочинці і хакери	Сервер та ПЗ на ньому
Використання неліцензійного ПЗ							0,07	0,05	

Продовження таблиці 1.10

Джерела загроз / Вразливості	Ноутбуки та комп'ютери, ПЗ на них	Бухгалтерія	Системний адміністратор	Відділ маркетингу і продажів	Відділ дизайну	Відділ кадрів	Конкуренти	Злочинці і хакери	Сервер та ПЗ на ньому
Відсутність датчиків відкриття вхідних дверей, датчиків відкриття чи розбиття вікон							0,17	0,09	
Помилки робітників		0,07	0,10	0,09	0,09	0,06			
Відсутність контролю за переміщенням							0,32	0,20	

відвідувачів у денний час									
Здійснення передачі внутрішньої інформації через незахищене середовище							0,14	0,09	
Відсутність відповідальності за невчасне або неналежне встановлення оновлень ПЗ	0,05								0,07

Продовження таблиці 1.10

Джерела загроз / Вразливості	Ноутбуки та комп'ютери, ПЗ на них	Бухгалтерія	Системний адміністратор	Відділ маркетингу і продажів	Відділ дизайну	Відділ кадрів	Конкуренти	Злочинці і хакери	Сервер та ПЗ на ньому
Відсутність регламенту щодо збереження, переміщення, знищення знімних носіїв та користування ними		0,26	0,38	0,32	0,32	0,20	0,32	0,20	
Збій	0,08								0,12

Відмова	0,07								0,10

Таким чином, для ІТС актуальними є такі загрози:

– проникнення у приміщення злочинців або конкурентів у неробочий час через відсутність датчиків відкриття чи розбиття вікон (К = 0,17);

– проникнення у приміщення злочинців або конкурентів у робочий час через відсутність контролю за переміщенням відвідувачів у робочий час (К = 0,32);

– фішинг та інші загрози, пов’язані з використанням електронної пошти та передачею внутрішніх документів через незахищене середовище. Можливість перехоплення інформації через відсутність регламенту щодо каналів передачі інформації між робітниками (К= 0,14);

– можливість крадіжки паперових та електронних (знімних) носіїв інформації, несанкціонованого знищення, або несанкціонованого ознайомлення з відповідною інформацією завдяки відсутності регламенту щодо збереження, переміщення, знищення знімних носіїв та користування ними (К = 0,38);

– збій серверу та втрата інформації, що знаходиться на ньому, у результаті збою та відсутності належної системи резервного копіювання (К = 0,12).

У таблиці 1.11 наведено перелік актуальних загроз із зазначенням їх впливу на властивості інформації, яка може бути уражена цими вразливостями (якщо загроза впливає на властивість, на перетині відповідної загрози та властивості стоїть знак +).

Таблиця 1.11 Вплив актуальних загроз на властивості інформації

Загроза	Властивості інформації, що порушуються		
	К	Ц	Д
Проникнення у приміщення злочинців або конкурентів у неробочий час через відсутність датчиків відкриття чи розбиття вікон	+	+	+
Проникнення у приміщення злочинців або конкурентів у робочий час	+	+	+

через відсутність контролю за переміщенням відвідувачів у робочий час			
Фішинг та інші загрози, пов'язані з використанням електронної пошти та передачею внутрішніх документів через незахищене середовище. Можливість перехоплення інформації через відсутність регламенту щодо каналів передачі інформації між робітниками	+		
Можливість крадіжки паперових та електронних (знімних) носіїв інформації, несанкціонованого знищення, або несанкціонованого ознайомлення з відповідною інформацією завдяки відсутності регламенту щодо збереження, переміщення, знищення знімних носіїв та користування ними	+		+
Збій серверу та втрата інформації, що знаходиться на ньому, у результаті збою та відсутності належної системи резервного копіювання		+	+

К- конфіденційність інформації;

Ц- цілісність інформації;

Д -доступність інформації.

1.5 Висновок і постановка задач

У першому розділі було описано ОІД: загальні відомості щодо його діяльності, фізичне розташування ОІД та об'єктів ІТС, характеристики обчислювальної системи , охарактеризована інформація, що обробляється та її носії, охарактеризовано середовище користувачів ІТС.

На основі отриманих даних була побудована характеристика можливих джерел загроз інформації та характеристика вразливостей. На основі аналізу цих характеристик було виділено актуальні для підприємства загрози інформації. Метою створення нових розділів політики інформаційної безпеки є побудова механізмів захисту від виділених загроз шляхом усунення або зменшення вразливостей. Тобто, необхідно створити розділи щодо:

- доступу сторонніх осіб в приміщення в робочий час;
- передачі документів в електронному вигляді, тобто, регламентування каналів передачі інформації;
- резервного копіювання;
- обліку знімних носіїв, правил поводження з ними;
- збереження матеріальних носіїв.

А також необхідно створити рекомендації щодо поліпшення системи сигналізації для того, щоб запобігти виникненню загрози проникнення порушників у неробочий час.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Оцінка існуючого стану захищеності.

Згідно з НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу»:

«Критерії є методологічною базою для визначення вимог з захисту інформації в комп'ютерних системах від несанкціонованого доступу; створення захищених комп'ютерних систем і засобів захисту від несанкціонованого доступу; оцінки захищеності інформації в комп'ютерних системах і їх придатності для обробки критичної інформації (інформації, що вимагає захисту).

Критерії надають:

1 Порівняльну шкалу для оцінки надійності механізмів захисту інформації від несанкціонованого доступу, реалізованих в комп'ютерних системах.

2 Базу (орієнтири) для розробки комп'ютерних систем, в яких мають бути реалізовані функції захисту інформації.» [3]

Згідно з НД ТЗІ 2.5-005 -99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу»:

«Стандартний функціональний профіль захищеності являє собою перелік мінімально необхідних рівнів послуг, які повинен реалізовувати КЗЗ обчислювальної системи АС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній АС.» [4]

Необхідно визначити послуги інформаційної безпеки, що реалізуються в АС підприємства на даний момент, а також визначити критерії захищеності, що необхідно додатково реалізувати в системі. Оскільки для передачі інформації в АС використовується мережа Інтернет (який є незахищеним середовищем), дана АС відноситься до третього класу.

Існуючі в системі критерії захищеності: { КА-2, КО-1, ЦА-2, ДР-1, НР-2, НИ-2, НК-1, НО-1, НТ-2, НА-2, НП-1}.

Рекомендовані критерії захищеності: { КА-2, КО-1, ЦА-2, ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НТ-2, НА-2, НП-1}.

У таблиці 2.1 наведено критерії захищеності інформації та механізми, якими вони реалізуються або мають реалізовуватися (якщо їх реалізація тільки планується у рекомендованому профілі).

Таблиця 2.1 Критерії захищеності інформації

Критерії	Механізми реалізації
КД-2	Розмежування прав доступу за допомогою засобів Active Directory та OneDrive
КО-1	Вбудовані засоби Windows
ЦД-1	Розмежування прав доступу за допомогою засобів Active Directory та OneDrive
ЦО-1	Засоби Active Directory – засоби для створення резервних копій інформації на сервері та засоби для відновлення групових політик та інших параметрів
ДР-1	Засоби Active Directory
ДВ-1	Засоби Active Directory – засоби для створення резервних копій інформації на сервері та засоби для відновлення групових політик та інших параметрів
НР-2	Вбудовані засоби Windows – журнал подій
НИ-2	Вбудовані засоби Windows
НК-1	Вбудовані засоби Windows
НО-1	Вбудовані засоби Windows
НТ-2	Вбудовані засоби Windows defender
НА-2	Засоби OneDrive та електронної пошти Outlook
НП-1	Засоби OneDrive

«Базова довірча конфіденційність (КД-2). В системі, яка реалізує послугу довірча конфіденційність на рівні КД-2, атрибути доступу об'єктів і користувачів повинні містити інформацію, що використовується КЗЗ для розмежування доступу до об'єктів з боку конкретного користувача. Додатково повинна існувати можливість встановлювати, які користувачі можуть активізувати конкретний процес, що дозволяє одержати можливість обмеженого керування потоками інформації. Керування правами доступу на даному рівні має невисоку вибірковість. Користувач, домену якого належить об'єкт (процес) може вказати, які групи користувачів і, можливо, які конкретні користувачі мають право одержувати інформацію від об'єкта (ініціювати процес). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів і процесів. Прикладом реалізації даного рівня послуги є реалізоване в UNIX керування доступом на підставі тріад власник / група / всі інші.

КО-1. Повторне використання об'єктів. Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС

Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані. Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною.

Мінімальна довірча цілісність (ЦД-1). На даному рівні користувач, домену якого належить об'єкт, може накладати обмеження на доступ до об'єктів з боку інших користувачів. Керування правами має грубу вибірковість (на рівні розподілу потоків інформації між групами користувачів). Для такої системи можна побудувати часткову матрицю доступу користувачів до захищених об'єктів.

ЦО-1. Обмежений відкат. Політика відкату, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься. Повинні існувати автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкотити або відмінити певний набір (множину) операцій, виконаних над захищеним об'єктом за певний проміжок часу.

ДР-1. Найслабкішою формою контролю за використанням ресурсів є використання квот. Всі захищені об'єкти КС (наприклад, дисковий простір, тривалість сеансу, час використання центрального процесора і т. ін.) повинні ідентифікуватись і контролюватись диспетчером доступу шляхом накладення обмежень на максимальний обсяг даного ресурсу, що може бути виділений користувачу. На даному рівні послуги немає гарантій, що користувач не зможе повністю захопити решту певного ресурсу, обмежуючи тим самим доступ до нього інших користувачів.

ДВ-1. Ручне відновлення. Політика відновлення, що реалізується КЗЗ, повинна визначати множину типів відмов КС і переривань обслуговування, після яких можливе повернення у відомий захищений стан без порушення

політики безпеки. Повинні бути чітко вказані рівні відмов, у разі перевищення яких необхідна повторна інсталяція КС. Після відмови КС або переривання обслуговування КЗЗ повинен перевести КС до стану, із якого повернути її до нормального функціонування може тільки адміністратор або користувачі, яким надані відповідні повноваження. Повинні існувати ручні процедури, за допомогою яких можна безпечним чином повернути КС до нормального функціонування.

НР-2. Захищений журнал. Політика реєстрації, що реалізується КЗЗ, повинна визначати перелік подій, що реєструються. КЗЗ повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Журнал реєстрації повинен містити інформацію про дату, час, місце, тип і успішність чи неуспішність кожної зареєстрованої події. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. КЗЗ повинен забезпечувати захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

НИ-2. Одиночна ідентифікація і автентифікація. Політика ідентифікації і автентифікації, що реалізується КЗЗ, повинна визначати атрибути, якими характеризується користувач, і послуги, для використання яких необхідні ці атрибути. Кожний користувач повинен однозначно ідентифікуватися КЗЗ. Перш ніж дозволити будь-якому користувачу виконувати будь-які інші, контрольовані КЗЗ дії, КЗЗ повинен автентифікувати цього користувача з використанням захищеного механізму. КЗЗ повинен забезпечувати захист даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

НК-1. Однонаправлений достовірний канал. Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Політика достовірного каналу, що реалізується КЗЗ, повинна визначати механізми

встановлення достовірного зв'язку між користувачем і КЗЗ. Достовірний канал повинен використовуватися для початкової ідентифікації і автентифікації. Зв'язок з використанням даного каналу повинен ініціюватися виключно користувачем.

НО-1. Виділення адміністратора. Політика розподілу обов'язків, що реалізується КЗЗ, повинна визначати ролі адміністратора і звичайного користувача і притаманні їм функції. Користувач повинен мати можливість виступати в певній ролі тільки після того, як він виконає певні дії, що підтверджують прийняття їм цієї ролі.

НТ-2. Самотестування при старті. Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Політика самотестування, що реалізується КЗЗ, повинна описувати властивості КС і реалізовані процедури, які можуть бути використані для оцінки правильності функціонування КЗЗ. КЗЗ має бути здатним виконувати набір тестів з метою оцінки правильності функціонування своїх критичних функцій. Тести повинні виконуватися за запитом користувача, що має відповідні повноваження, при ініціалізації КЗЗ.

НА-2. Автентифікація відправника з підтвердженням. Політика автентифікації відправника, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем. Додатково повинні бути визначені ті властивості, атрибути і процедури, які можуть використовуватися для однозначного підтвердження належності об'єкта незалежною третьою стороною. Встановлення належності має виконуватися на підставі затвердженого протоколу автентифікації. Використовуваний протокол автентифікації повинен забезпечувати можливість однозначного підтвердження належності об'єкта незалежною третьою стороною.

НП-1. Базова автентифікація отримувача. Ця послуга дозволяє забезпечити захист від відмови від одержання і дозволяє однозначно встановити факт

одержання певного об'єкта певним користувачем. Політика автентифікації одержувача, що реалізується КЗЗ, повинна визначати множину властивостей і атрибутів об'єкта, що передається, користувача-одержувача і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був одержаний певним користувачем. Встановлення одержувача має виконуватися на підставі затвердженого протоколу автентифікації.» [3]

2.2 Проектні рішення – політика інформаційної безпеки

Згідно з НД ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»:

«Під політикою безпеки інформації слід розуміти набір законів, правил, обмежень, рекомендацій і т. ін., які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз. Термін "політика безпеки" може бути застосовано щодо організації, АС, ОС, послуги, що реалізується системою (набору функцій), і т. ін. Чим дрібніше об'єкт, відносно якого застосовується даний термін, тим конкретнішими і формальніше стають правила.

Політика безпеки повинна визначати ресурси АС, що потребують захисту, зокрема установлювати категорії інформації, оброблюваної в АС. Мають бути сформульовані основні загрози для ОС, персоналу, інформації різних категорій і вимоги до захисту від цих загроз. Як складові частини загальної політики безпеки інформації в АС мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації. Відповідальність персоналу за виконання положень політики безпеки має бути персоніфікована.

Політика безпеки інформації, що реалізуються різними КС будуть відрізнятися не тільки тим, що реалізовані в них функції захисту можуть забезпечувати захист від різних типів загроз, але і в зв'язку з тим, що ресурси КС можуть істотно відрізнятись. Так, якщо операційна система оперує файлами, то СУБД має справу із записами, розподіленими в різних файлах.

Частина політики безпеки, яка регламентує правила доступу користувачів і процесів до ресурсів КС, складає правила розмежування доступу.» [5]

Таким чином, надалі буде вирішуватися завдання розробки частин політики інформаційної безпеки, які б забезпечували захист інформації в ІТС від актуальних загроз, визначених у першому розділі цієї роботи, а також забезпечували виконання рекомендованих послуг інформаційної безпеки.

На організаційному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо:

– організації проведення обстеження середовищ функціонування АС (здійснення профілактичних заходів), особливо це стосується стану сервера та вироблення плану дій у випадку його збою;

– виконання робіт з модернізації АС (окремих компонентів) – а саме, системи сигналізації;

– регламентації доступу сторонніх користувачів до ресурсів АС, зокрема доступу сторонніх осіб в приміщення;

– регламентації доступу власних користувачів і персоналу до ресурсів АС, зокрема регламентації доступу до паперових та знімних (електронних) носіїв інформації, правил їх зберігання, передачі, знищення, тощо;

– використання мереж передачі даних загального користування, зокрема Інтернет;

– регламентації засобів та схем передачі інформації між робітниками.

На технічному рівні забезпечення безпеки інформації повинні бути вироблені підходи щодо застосування технічних і програмно-технічних засобів, які реалізують задані вимоги з захисту інформації:

– виявлення і реєстрація небезпечних подій з метою здійснення повсякденного контролю або проведення службових розслідувань;

– резервне копіювання критичних даних;

– відновлення роботи АС після збоїв, відмов.

2.2.1 Політика доступу сторонніх осіб в приміщення в робочий час

Метою цієї політики є:

Створення регламенту доступу сторонніх користувачів до ресурсів АС, захист від проникнення у приміщення злочинців або конкурентів у робочий час через відсутність контролю за переміщенням відвідувачів у робочий час.

Область дії:

Політика встановлює порядок організації пропускного режиму в організацію, порядок контролю за переміщенням відвідувачів, а також встановлює відповідальність за порушення відповідних правил.

Ця політика стосується, перш за все, робітників організації, які запрошують до організації відвідувачів (наприклад, голова відділу кадрів, згідно зі своєю посадовою інструкцією, має спілкуватися з кандидатами на посади в організації, поводити презентації для відвідувачів, тощо). Також ця політика стосується безпосередньо відвідувачів.

Політика безпеки:

Для забезпечення контролю доступу в приміщення, на підприємстві встановлюються електронні замки на вхідні двері та на двері у відділі дизайну, що використовують як ключі смарт-картки. Кожний робітник отримує персональну картку, яку забороняється передавати третім особам (за виключенням обставин, зазначених у цій політиці). Для відвідувачів, що мають часто приходити на підприємство, але не є повноправними робітниками компанії, можливе виготовлення тимчасових карток. Для забезпечення доступу до приміщення необхідно надати системі свою картку та ввести PIN-код на допоміжній клавіатурі.

Якщо робітника було звільнено, системний адміністратор має заблокувати його картку, а звільнений робітник зобов’язаний віддати свою картку менеджеру по персоналу. За видачу карток новим робітникам, за видачу тимчасових карток відповідальний також менеджер по персоналу, що має бути відображено у його посадовій інструкції.

Доступ відвідувачів до відділу дизайну надається у виняткових випадках та за наявності письмового дозволу генерального директора. Дозволяється неконтрольоване перебування відвідувачів (тобто, відсутність супроводу відповідальної особи) у тих приміщеннях організації, де не ведеться інформаційна діяльність (наприклад, кухня).

Відповідальність:

Відвідувача має пропустити робітник, що запросив його, він також має супроводжувати відвідувача, поки той знаходиться на території підприємства. У разі порушення політики безпеки підприємства, відповідальність за дії відвідувача несе, у тому числі, робітник, що пропустив його на ОІД. Відповідальність за невиконання цих правил полягає у сплаті штрафу або позбавлення премії в залежності від присутності та серйозності наслідків.

2.2.2 Політика каналів передачі документів в електронному вигляді

Метою цієї політики є:

Створення регламенту обігу інформації на підприємстві, тобто встановлення правил щодо того, як мають передаватися документи від однієї особи до іншої, захист від перехоплення цих документів та захист від загроз, що виникають при передачі інформації через незахищене середовище (Інтернет).

Область дії:

Політика встановлює порядок та методи передачі документів в електронному вигляді між робітниками, а також правила, пов’язані з передачею інформації.

Ця політика стосується всіх робітників організації, які залучені в інформаційну діяльність компанії, мають передавати чи отримувати документи. Також ця політика стосується клієнтів організації, які передають чи отримують певну інформацію.

Політика безпеки:

Накази директора мають передаватися від директора до робітників компанії через сервер – генеральний директор створює документ на своєму

ноутбуку, копіює його у відповідну папку на сервері і надає іншим користувачам відповідний матриці доступу тип доступу.

Інформація щодо нових замовлень поступає від клієнтів до відділу маркетингу за допомогою електронної пошти, від цього відділу документи передаються засобами OneDrive і дублюються на сервері (тут і надалі механізм розповсюдження інформації на сервері такий самий як з наказами директора).

Статистика продажів, дані щодо замовників, звіти системного адміністратора передаються між робітниками за допомогою сервера.

Документи щодо проведених фінансових операцій використовуються тільки робітниками бухгалтерії, тому для їх передачі використовуються знімні носії. Виключення становить інформація, що передається бухгалтерією до податкової через Інтернет.

Готова продукція (тобто, роботи дизайнерів) передається між робітниками за допомогою серверу, а до клієнтів передається засобами OneDrive.

Готова продукція через певний період після передачі клієнту, за домовленості з клієнтом, є відкритою інформацією і може передаватися будь-якими методами, за виключенням знімних носіїв (оскільки на них може знаходитися інша, критична інформація).

Ескізи, роботи в процесі передаються за допомогою засобів OneDrive, дозволяється передавати їх за допомогою сервера (за рішенням проджект-менеджерів).

Дані щодо стану локальної мережі, журнали подій, персональні дані працівників, дані ідентифікації та аутентифікації не передаються.

Дані про зарплату передаються у бухгалтерії за допомогою знімних носіїв.

Договори з клієнтами передаються від клієнтів до робітників і навпаки за допомогою засобів OneDrive, а між робітниками передаються за допомогою серверу.

При цьому той чи інший вид доступу надається робітникам згідно з Наказом «Про доступ до інформації з обмеженим доступом №123 від 02.02.2015» та Наказом «Про доступ до елементів комп`ютерної системи №125

від 05.02.2015», якими регламентується матриця доступу. Зберігаються документи на сервері та на хмарному сховищі OneDrive також згідно з вищезазначеними документами та враховуючи правила, встановлені у цій політиці. Дозволяється зберігати створені робітником документи або передані йому іншим робітником на власній робочій станції.

Для виконання правил цієї політики та контролю за їх виконанням рекомендується застосовувати засоби Active Directory (а саме, групові політики) та створювати технологічні схеми, тобто, встановлювати обмеження щодо відкриття певних документів окремими програмами. Для зменшення загрози фішингу при користуванні електронною поштою рекомендується контактувати з клієнтом щодо відправлених електронних листів та перевіряти вкладення. Також необхідно блокувати користувачам ресурси, які не потрібні їм для виконання їх обов’язків.

Відповідальність:

Контроль за виконанням правил, встановлених цією політикою, покладається на системного адміністратора та генерального директора організації.

2.2.3 Політика резервного копіювання

Метою цієї політики є:

Створення регламенту резервного копіювання документів та технологічної інформації (тобто групових політик і т.п.) на підприємстві, зокрема інформації, що знаходиться на сервері. Тобто встановлення правил щодо того, яким чином та де має бути створено відповідні резервні копії і хто має слідкувати за станом цих копій, а також відновлювати інформацію за необхідністю. Також метою політики є регламентування робіт з профілактики збоїв та відмов серверу – встановлення плану аналітики програмних та апаратних засобів серверу, встановлення методів цієї аналітики.

Область дії:

Ця політика стосується робітників організації, що є відповідальними за відновлення системи після збоїв та створення резервних копій – тобто, системного адміністратора. Відповідальність за виконання відповідних робіт також покладається на нього.

Політика безпеки:

При резервному копіюванні рекомендується використовувати правило «3-2-1», згідно з яким має бути створено 3 резервні копії, які мають бути збережені у двох різних форматах зберігання, і одна з копій має зберігатися поза офісом. Нижче буде описано, як саме має бути реалізовано це правило.

Шаблони групових політик та інша важлива технологічна інформація необхідно копіювати на окремий знімний носій, який має право використовувати лише системний адміністратор. Також резервна копія повинна бути на ноутбуці системного адміністратора, дозволяється зберігати одну копію у OneDrive (доступ має бути лише у системного адміністратора). Резервне копіювання цих даних має проводитися як мінімум раз на місяць.

Документи, що передаються за допомогою серверу, повинні також зберігатися там у відповідних каталогах (у тих самих, через які передаються). Таким же чином повинні зберігатися документи у OneDrive, які передаються за його допомогою.

Резервне копіювання документів має обов’язково виконуватись до всіх встановлених місць при кожному оновленні документів (тобто, у той самий день, коли документ було створено чи оновлено) або, принаймні раз на тиждень (за рішенням генерального директора).

Необхідно, в першу чергу, забезпечити створення резервних копій документів, забезпечення доступності яких є критичним (рівень критичності доступності Д3 та Д4). У таблиці 2.2 наведено місця резервного копіювання документів і місця знаходження оригіналів цих документів (позначка + означає, що резервна копія документа повинна бути наявна на відповідному ресурсі).

Таблиця 2.2 – місцезнаходження документів

Документ	Місцезнаходження документів

	Знімні носії	Сервер	One Drive	Робоча станція власника документа (особи, що його створила або отримала ззовні)	Робочі станції робітників, яким було передано документ
Накази генерального директора	-	+	+	+	-
Інформація щодо нових замовлень	-	+	+	+	+
Статистика продажів	-	+	-	+	-
Документи щодо проведених фінансових операцій	+	-	-	+	+
Готова продукція	-	+	+	+	+
Готова продукція через певний період після передачі клієнту, за домовленості з клієнтом	-	+	+	+	-
Ескізи, роботи в процесі	+	+	+	+	+
Дані щодо стану локальної мережі, журнали подій	+	-	-	+	-
Дані щодо замовників	-	+	-	+	-
Персональні дані працівників	-	-	-	+	-
Дані про зарплату	+	-	+	+	+
Дані ідентифікації та аутентифікації	+	-	-	+	-
Договори з клієнтами	-	+	+	+	+
Звіт системного адміністратора	-	+	-	+	-

Також рекомендується використовувати засоби Active Directory для резервного копіювання та відновлення системи. Для відновлення даних при їх втраті можна також використовувати безкоштовну програму Recuva. При зникненні даних треба одразу запустити цю програму, для копіювання відновлених даних використовувати знімний носій.

Необхідно проводити періодичну аналітику серверу: використовувати вбудовані засоби Windows Server, безкоштовну програму Viktoria для перевірки стану жорстких дисків.

Програми Total Network Inventory 3 та Total Software Deployment 2 (які не є ліцензійними) для аналізу мережі мають бути замінені на Spiceworks Inventory, що э безкоштовною і може виконувати ті ж самі функції і дозволяє більш ефективно виконувати моніторинг мережі і робочих станцій в ній.

Відповідальність:

Відповідальність за виконання зазначених робіт покладається на системного адміністратора.

2.2.4 Політика обліку знімних носіїв та збереження матеріальних носіїв інформації

Метою цієї політики є:

Створення механізмів захисту від загроз крадіжки паперових та знімних носіїв інформації, несанкціонованого знищення, або несанкціонованого ознайомлення з відповідною інформацією.

Область дії:

У цій політиці описується регламент обліку знімних носіїв, а також правила їх переміщення, зберігання, використання, знищення, тощо. Крім того цією політикою встановлюються правила щодо збереження паперових носіїв інформації. Ця політика стосується всіх робітників організації, які працюють з інформацією.

Політика безпеки:

Усі знімні носії, що знаходяться в організації, підлягають обліку. Кожний такий носій повинен мати унікальний ідентифікатор. За видачу знімних носіїв відповідають керівники відділів, в яких дозволено використання знімних носіїв. Факт видачі носія, а також факт його повернення фіксується в спеціальному журналі, де вказується прізвище та ім’я особи, що отримала/повернула носій,

час видачі/повернення та ідентифікатор знімного носія. Журнали зберігаються у відділах, де зберігаються знімні носії у керівників цих відділів.

Використання носіїв дозволяється тільки для виконання робітниками своїх прямих обов'язків. Забороняється передавати носії третім особам або виносити носії з території підприємства без відома керівника відділу. У разі втрати або несанкціонованого знищення носія, робітник повинен повідомити про це свого керівника.

За рішенням керівників відділів дозволяється знищувати знімні носії (наприклад, ушкоджені носії) – для цього необхідно знищити всі дані на цьому носії (перезаписуючи значення кожної ланки пам'яті) і нанести фізичні ушкодження, що забезпечать відсутність можливості відновлення даних.

Знімні носії зберігаються і використовуються у наступних підрозділах:

– бухгалтерія (2 USB-накопичувачі);

– відділ системного адміністрування (2 USB-накопичувачі і 1 зовнішній жорсткий диск);

– відділ графічного дизайну (5 USB-накопичувачів).

Знімні носії повинні зберігатися в сейфах, ключі від сейфів повинні знаходитися у керівників відповідних відділів. У тих самих сейфах повинні зберігатися паперові носії інформації. Додатково сейф потрібно встановити в кабінеті генерального директора – для збереження паперових носіїв інформації. Необхідно заборонити зберігання паперових носіїв інформації з обмеженим доступом у відділах, де немає сейфів для їх зберігання і, відповідно, заборонити можливість друку для робітників, що працюють у цих відділах (це стосується відділу маркетингу і продажів). За видачу друкованих матеріалів робітникам відповідальні керівники відділів, в яких зберігаються ці матеріали.

Групові політики Active Directory мають бути налаштовані таким чином, щоб робітники, які не мають права використовувати знімні носії, не мали можливості підключення будь-яких знімних носіїв (окрім, наприклад, миші). Для робітників, які мають використовувати знімні носії у своїй роботі, необхідно заборонити використання будь-яких носіїв, окрім дозволених.

Рекомендується налаштувати групові політики наступним чином:

Активувати політику «дозволити встановлення пристроїв, що відповідають якому-небудь з цих кодів пристроїв». Відповідні коди можна подивитись в «Диспетчері пристроїв» у вкладці Відомості, параметр «ID обладнання».

Разом з цією політикою необхідно неодмінно активувати «Заборонити встановлення пристроїв, що не описані іншими параметрами політики». Таким чином, при підключенні незареєстрованого носія, він буде заблокований, а користувач отримає системне попередження.

Рекомендовано також застосовувати для знімних носіїв технологію BitLocker, що доступна у Windows системах. Технологія дозволяє шифрувати дані на USB-накопичувачах та знімних дисках – доступ може отримати користувач, що знає відповідний пароль, можна дозволити зчитування інформації лише з певних комп'ютерів чи ноутбуків. Це рішення може захистити інформацію, перш за все, від зовнішніх порушників, наприклад, конкурентів. Активація політики «Керування використанням BitLocker для знімних носіїв» дозволяє шифрування для зовнішніх носіїв.

Щоб користувачі не могли самостійно вимикати BitLocker, необхідно неодмінно зняти відмітку «Дозволити користувачам тимчасово призупиняти захист BitLocker і розшифрувати диски з даними».

Відповідальність:

Відповідальність за збереження знімних носіїв, а також паперових носіїв покладається на керівників відділів. Відповідальність за налаштування групових політик покладається на системного адміністратора.

2.2.5 Рекомендації щодо покращення системи сигналізації

Метою застосування цих рекомендацій є створення механізмів захисту від загрози проникнення у приміщення злочинців або конкурентів через відсутність датчиків відкриття чи розбиття вікон.

Оскільки ОІД знаходиться на третьому поверсі, на вікнах відсутні решітки і поблизу є дерева - необхідно встановити на кожному вікні датчик відкриття, а також встановити датчики розбиття вікон у кожній кімнаті, де ведеться обробка інформації.

Рекомендована схема сигналізації зображена на рисунку 2.1.

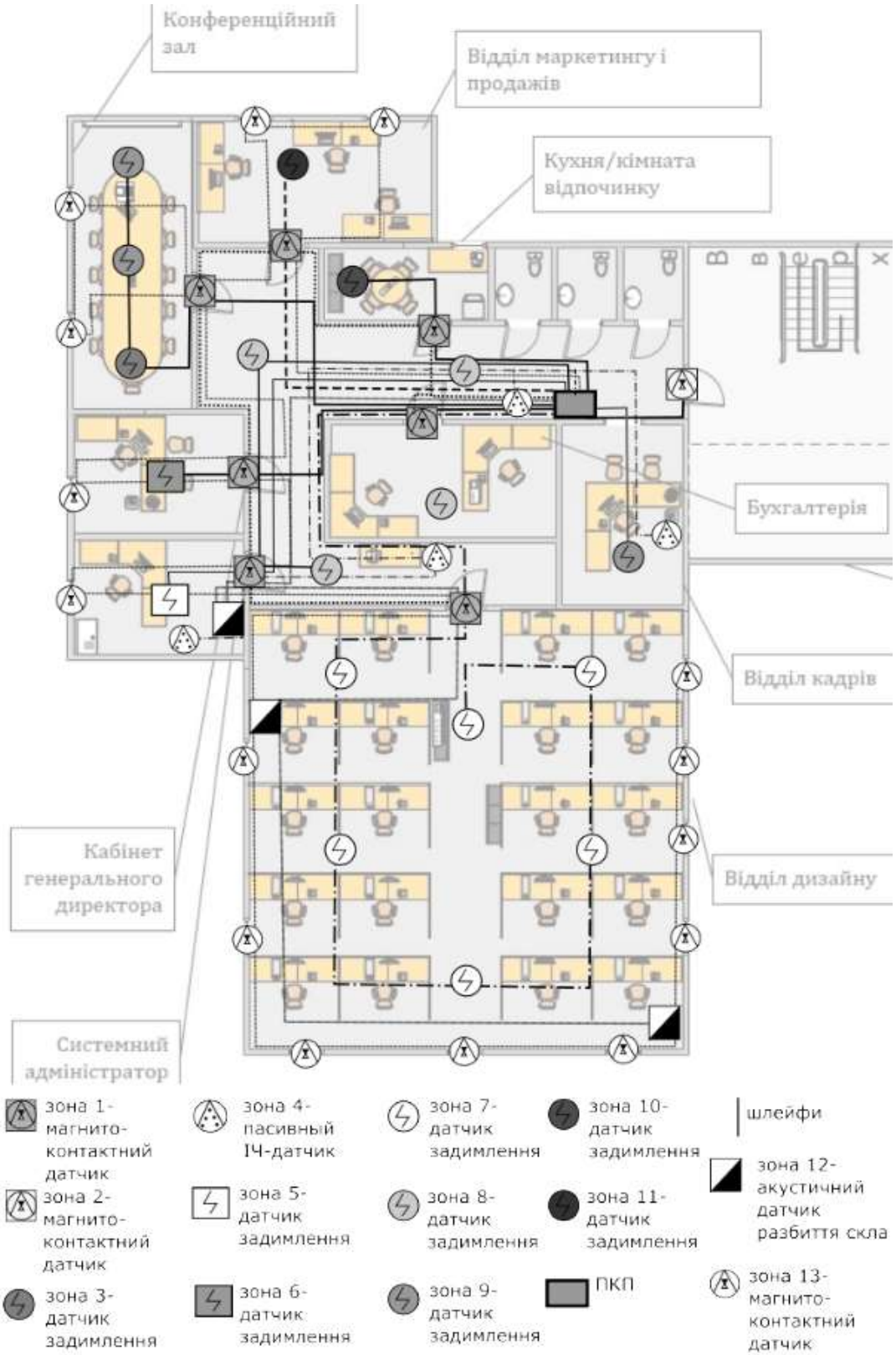

Рисунок 2.1 – Рекомендована схема сигналізації

2.2.6 Політика використання Інтернету на підприємстві

Метою цієї політики є:

Захист від неправомірної передачі документів компанії через незахищене середовище та захист від фішингу за допомогою створення правил щодо доступу працівників компанії до ресурсів в Інтернеті.

Область дії:

У цій політиці описуються права та обов’язки працівників при роботі з Інтернетом, методи контролю їх діяльності в Інтернеті. Ця політика стосується всіх робітників організації, які працюють з комп’ютерами або ноутбуками.

Політика безпеки:

Використання Інтернету робітниками дозволяється використовувати лише для:

– виконання своїх прямих обов’язків (наприклад, для відділу маркетингу і продажів – для зв’язку з клієнтами);

– пошуку довідкових матеріалів, матеріалів для покращення своєї професійної діяльності, навчальних матеріалів;

– збору необхідних для роботи відомостей;

– реклами та просування компанії.

Забороняється використовувати Інтернет для:

– передачі конфіденційних документів нерегламентованими каналами;

– особистих цілей.

Системний адміністратор повинен періодично контролювати відвідування користувачами інтернет-ресурсів, включати відповідну інформацію до свого звіту генеральному директору. Для цих цілей він може використовувати Wireshark (встановлюючи фільтри га відповідні протоколи і хости) або інший аналізатор трафіку. За рішенням директора може бути створено список заборонених ресурсів і видано відповідний наказ. В такому разі системний адміністратор повинен буде заблокувати ці ресурси для зазначених директором користувачів.

Відповідальність:

У разі явного порушення даної політики співробітником підприємства, йому повинно бути висунуто попередження. Наступного разу, його може

очікувати штраф або блок на використання Інтернету (за рішенням генерального директора).

Контролювати виконання даної політики має системний адміністратор.

2.3 Висновки

В другому розділі було проаналізовано наявні в ІТС критерії захищеності, виділено засоби забезпечення відповідних послуг. Було обрано нові додаткові критерії захищеності, що забезпечують належний рівень інформаційної безпеки. Було також зазначено рекомендовані засоби забезпечення доданих послуг.

Для забезпечення захисту від існуючих на ОІД загроз та для забезпечення належної роботи критеріїв захищеності було розроблено рекомендовані розділи політики безпеки щодо:

– доступу сторонніх осіб в приміщення в робочий час;

– передачі документів в електронному вигляді, тобто, регламентування каналів передачі інформації;

– резервного копіювання;

– обліку знімних носіїв, правил поводження з ними та збереження матеріальних носіїв.

Було також створено рекомендації щодо поліпшення системи сигналізації для того, щоб запобігти виникненню загрози проникнення порушників у неробочий час.

Додатково було розроблено розділ політики щодо використання Інтернету задля захисту від неправомірної передачі документів через незахищене середовище та захисту від фішингу.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

Метою виконання економічного розділу є визначення того, чи буде використання запропонованих засобів та заходів інформаційної безпеки на ТОВ «ArtCastle» вигідним для підприємства. Щоб з’ясувати це, необхідно визначити розмір капітальних та експлуатаційних витрат на заходи і засоби інформаційної безпеки, визначити величину відвернених втрат та, на основі цього, розрахувати коефіцієнт повернення інвестицій та термін окупності капітальних інвестицій. На основі розрахованих показників можна буде визначити, наскільки прибутковим або збитковим є запропонований проект.

3.1 Розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення

До фіксованих (капітальних) варто відносити наступні витрати на ТОВ “ArtCastle”:

– витрати на залучення зовнішніх консультантів (спеціаліста з розробки політики безпеки інформації);

– витрати на первісні закупівлі апаратного забезпечення (датчики розбиття вікон та датчики відкриття вікон, електронні замки та смарт-картки, сейфи для збереження носіїв інформації);

– витрати на інтеграцію системи інформативної безпеки у вже існуючу корпоративну систему (встановлення обладнання та налагодження системи інформаційної безпеки);

Для підрахунку заробітної платні залученого працівника, який створює або дороблює політику безпеки, необхідно розрахувати трудомісткість розробки політики безпеки інформації. Вона визначається тривалістю кожної робочої операції цього працівника:

$$t = t_o + t_a + t_{\text{в}} + t_{\text{д}} \quad , \text{ годин,} \tag{3.1}$$

де:

$t_o = 75$ – тривалість проведення обстеження ІТС підприємства

$t_а = 14$ – тривалість процесу аналізу можливих загроз та ризиків;

$t_в = 20$ –тривалість визначення вимог до заходів, методів та засобів захисту, вибору основних рішень з забезпечення безпеки інформації;

$t_д = 12$ – тривалість документального оформлення політики безпеки.

t = 75+14+20+12=121 година.

У даному випадку, витрати на розробку політики безпеки інформації включають в себе лише заробітну плату робітника, який залучається для створення політики безпеки. В його оплату вже включено всі витрати, яких він зазнає (витрати на електроенергію, тощо). Виконавець не використовує у своїй роботі ноутбуки чи комп'ютери компанії. Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) та визначається за формулою:

$$К_{пр} = t \cdot З_{іб}, \text{ грн,} \quad (3.2)$$

де:

t =121 – загальна тривалість розробки політики безпеки, годин;

$З_{іб} = 75$ – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

$$К_{пр} = 121 \cdot 75 = 9075 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = K_{пр} + K_{др} + K_{дв} + K_{ез} + K_{ск} + K_{с} + K_{вз}, \text{ грн,} \quad (3.3)$$

де:

$К_{пр}$ – вартість розробки політики безпеки інформації (9075 грн);

$К_{др}$ – вартість закупівлі датчиків розбиття скла (443 грн $\cdot 6$ шт $=$ 2658 грн);

$К_{дв}$ – вартість закупівлі датчиків відкриття вікон (56 грн $\cdot 13$ шт $=$ 728 грн);

$К_{ез}$ – вартість закупівлі електронних замків (675 грн $\cdot 2$ шт $= 1375$ грн);

$К_{ск}$ – вартість закупівлі смарт-карток (10 грн $\cdot 30$ шт $= 300$ грн);

$К_{с}$ – вартість закупівлі сейфів (3420 грн $\cdot 3$ шт $= 10260$ грн);

$К_{д}$ – витрати на встановлення датчиків (1000 грн);

$К_{вз}$–витрати на встановлення електронних замків (1500 грн);

$$К = 9075 + 2658 + 728 + 1375 + 300 + 10260 + 1000 + 1500 = $$
$$= 26896 \text{ , грн.}$$

3.2 Розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (рік), що виражені у грошовій формі.

Для компанії актуальними можуть бути експлуатаційні витрати на:

– заробітну плату системному адміністратору (оскільки коло його обов’язків було розширено в нових розділах політики безпеки);

– електроенергію, що споживається новим обладнанням (новими датчиками сигналізації та електронними замками);

– журнали обліку знімних носіїв.

Додаткова заробітна плата ($С_з$), що сплачується робітнику за виконання нових обов’язків складає 8-10% від основної заробітної плати.

Системному адміністратору необхідно доплачувати за такі види робіт:

– контроль виконання користувачами розділів політик безпеки;

– налаштування групових політик (створення правил щодо використання знімних носіїв);

– резервне копіювання;

Тому, пропонується доплачувати системному адміністратору 10% від основної заробітної плати.

Основна заробітна плата системного адміністратора складає 15000 грн з перерахуваннями. Отже, за виконання нових обов'язків, адміністратор отримуватиме додатково 1500 грн. Таким чином, окрім основної заробітної платні, адміністратор отримуватиме на рік:

$$С_з = 1500 \cdot 12 = 18000 \quad , \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_е = (Р_з + Р_д) \cdot F_р \cdot Ц_е \quad , \text{ грн,} \qquad (3.4)$$

де:

$Р_з$ = 0,0002– встановлена потужність електронних замків (апаратури інформаційної безпеки), кВт;

$Р_з$ = 0,004 – встановлена потужність датчиків (апаратури інформаційної безпеки), кВт;

$F_р$ =8760 год - річний фонд робочого часу системи інформаційної безпеки (за умови безперервного режиму роботи);

$Ц_е$ = 2,01 - тариф на електроенергію, грн/кВт·годин.

$$С_е = (0{,}0002 + 0{,}004) \cdot 8760 \cdot 2{,}01 = 73{,}95 \quad , \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки (Стос) у відсотках від вартості капітальних витрат (1-

3%). До таких витрат може бути віднесено обслуговування нових датчиків та електронного замка, отже, необхідно врахувати 1% від їх вартості.

$$C_{тос} = 0{,}01 \cdot (2658 + 728 + 1375) = 47{,}61 \quad , \text{ грн.}$$

Крім того, організації періодично необхідно купляти журнали обліку знімних носіїв. Такий журнал необхідний трьом відділам приблизно раз на 2 роки:

$C_{жо}$ – вартість закупівлі журналів обліку знімних носіїв$= 35 \text{ грн} \cdot 3 \cdot 0{,}5 = 52{,}5 \text{ грн}$;

Отже, річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$C = C_з + C_е + C_{тос} + C_{жо} = 18000 + 74 + 48 + 54 = 18176 \quad , \text{ грн.} \qquad (3.5)$$

3.3 Визначення річного економічного ефекту від впровадження об'єкта проектування

Необхідно визначити величину відвернених збитків, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього.

Далі буде визначено можливі збитки від таких загроз:

– проникнення у приміщення злочинців або конкурентів у неробочий час;

– проникнення у приміщення злочинців або конкурентів у робочий час через відсутність контролю за переміщенням відвідувачів у робочий час;

– фішинг та інші загрози, пов’язані з використанням електронної пошти та передачею внутрішніх документів через незахищене середовище. Можливість перехоплення інформації через відсутність регламенту щодо каналів передачі інформації між робітниками;

– можливість крадіжки паперових та електронних (знімних) носіїв інформації, несанкціонованого знищення, або несанкціонованого ознайомлення з відповідною інформацією;

– збій серверу та втрата інформації, що знаходиться на ньому, у результаті збою та відсутності належної системи резервного копіювання.

Внаслідок проникнення в офіс в неробочий час, може бути викрадено ноутбук або знімний носій. Внаслідок цього може бути зупинена діяльність системного адміністратора, порушено діяльність бухгалтерії або відділу маркетингу і продажів. Може бути втрачено проекти внаслідок порушення умов договору з клієнтом, через це ж компанія може зазнати репутаційних збитків.

Таким чином, упущена вигода від простою атакованого вузла (системного адміністратора) становить:

$$U_{\text{а}} = \text{П}_{\text{п}} + \text{П}_{\text{в}} + V \quad , \text{ грн,} \tag{3.6}$$

де:

Пп – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн;

Пв – вартість відновлення працездатності вузла (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності системного адміністратора являють собою втрату його заробітної плати (оплата непродуктивної праці) за час простою:

$$\text{П}_{\text{п}} = \frac{\Sigma\, 3_{\text{с}}}{F} \cdot t_{\text{п}} \quad , \text{ грн,} \tag{3.7}$$

де:

F =176 год – місячний фонд робочого часу (40-годинний робочий тиждень);

Зс = 16000 грн - розмір заробітної платні працівника;

tп = 24 год - час простою вузла внаслідок атаки. Простій займає приблизно 3 дні по 8 годин робочого часу.

$$П_п = \frac{16000}{176} \cdot 24 = 2181, \text{ грн.}$$

Витрати на відновлення працездатності вузла включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн,} \quad (3.8)$$

де:

$П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ =13049 грн– вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\Sigma З_с}{F} \cdot t_{ви} = \frac{16000}{176} \cdot 8 = 727 \text{ , грн.} \quad (3.9)$$

Витрати на відновлення вузла або сегмента корпоративної мережі можна не враховувати, оскільки існують шаблони для всіх необхідних налаштувань і, якщо відновлення й необхідне, його можливо виконати за дуже короткий проміжок часу. $П_{пв} = 0$.

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла також можна не враховувати, оскільки виконання проектів не залежить від системного адміністратора. V=0.

$$U_a = 2181 + 727 + 13049 = 15957, \text{ грн.}$$

Приблизно таку саму суму збитків зазнає компанія, якщо буде викрадено ноутбук бухгалтера або ноутбук працівника відділу маркетингу та продажів.

Крім того, у тому випадку, якщо буде вкрадено знімний носій з ескізами або готовими роботами, буде порушено договір з клієнтом – компанія втратить проект з ним і може зазнати репутаційного збитку.

Середня вартість розробки брендбуку -23400 грн.

Середня вартість розробки web-дизайну сайту або розробки інтерфейсу додатка -15000 грн.

Середня тривалість одного проекту – 3 тижні, паралельне виконання 3 проектів. Компанія виконує приблизно 40 замовлень на рік.

В разі втрати замовлення компанія втрачає до 38400 грн. Якщо страждає репутація компанії то передбачається, що вона може втратити до 10% проектів, тобто, приблизно 4 проекти. Збиток тоді становитиме до 153600 грн. на наступний рік.

Передбачається, що одна така загроза може реалізуватися приблизно раз на рік.

Таким чином, загальний збиток від цієї загрози організації складе:

$$B = 15957 + 38400 + 153600 = 207957 \text{ грн.}$$

Внаслідок проникнення в офіс в робочий час, може бути втрачено проекти внаслідок порушення умов договору з клієнтом, через це ж компанія може зазнати репутаційних збитків. Отже, B=38400+153600=192000 грн. Те ж саме стосується загроз перехоплення інформації через відсутність регламенту щодо

каналів передачі інформації між робітниками, крадіжки паперових та електронних (знімних) носіїв інформації. Збій серверу та втрата інформації, що знаходиться на ньому може спричинити затримку в роботі працівників та зменшення кількості проектів, що може виконуватись одночасно. Наприклад, в разі втрати ескізів, до проекту може бути залучено додаткових працівників для пришвидшення відновлення матеріалів. Тоді зазначені працівники не зможуть брати участь в нових проектах компанії. B = 38400 грн.

У таблиці 3.1 наведено актуальні загрози для підприємства та величини можливих збитків від реалізації цих загроз.

Таблиця 3.1 – Оцінка величини збитків

Загроза	Збиток B, грн	Ймовірність R	B · R, грн
Проникнення у приміщення злочинців або конкурентів у неробочий час	207957	0,17	35352
Проникнення у приміщення злочинців або конкурентів у робочий час через відсутність контролю за переміщенням відвідувачів у робочий час	192000	0,32	61440
Фішинг та інші загрози, пов'язані з використанням електронної пошти та передачею внутрішніх документів через незахищене середовище. Можливість перехоплення інформації через відсутність регламенту щодо каналів передачі інформації між робітниками	192000	0,14	26880
Можливість крадіжки паперових та електронних (знімних) носіїв інформації, несанкціонованого знищення, або несанкціонованого ознайомлення з відповідною інформацією	192000	0,38	72960
Збій серверу та втрата інформації, що знаходиться на ньому, у результаті збою та відсутності належної системи резервного копіювання	38400	0,12	4608
Всього:	201240 грн.		

3.4 Визначення та аналіз показників економічної ефективності запропонованого в дипломному проекті проектного рішення

Загальний ефект від впровадження системи інформаційної безпеки становить:

$$E = B \cdot R - C = 201240 - 18176 = 183064 \text{ грн.} \quad (3.10)$$

де:

B – загальний збиток від атаки на вузол корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, грн.

Оцінка економічної ефективності системи захисту інформації здійснюється на основі визначення та аналізу наступних показників:

– сукупна вартість володіння (TCO);

– коефіцієнт повернення інвестицій ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій T_o.

TCO у даному випадку не використовується, оскільки не порівнюються декілька варіантів проектів.

ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

$$ROSI = \frac{E}{K} = \frac{183064}{26896} = 6{,}8 \quad (3.11)$$

де:

E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Для остаточної оцінки варіантів і вибору найбільш ефективного з них необхідно порівняти значення ROSI з бажаним значенням показника ефективності $E_н$.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів, тому в якості $E_н$ приймається бажана норма прибутковості альтернативних варіантів вкладення коштів К (на депозитний рахунок у банку).

Проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > \frac{(N_{\text{деп}} - N_{\text{інф}})}{100} \quad (3.12)$$

де:

$N_{деп}$ =14,5 – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, %;

$N_{інф}$ = 9,2 – річний рівень інфляції, %.

6,8> 0,05, отже проект є економічно доцільним.

Термін окупності капітальних інвестицій $T_о$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_0 = \frac{K}{E} = \frac{1}{ROSI} = 0{,}147 \text{ року.} \quad (3.13)$$

3.5 Висновок про економічну доцільність проектного рішення

В цьому розділі було визначено розмір капітальних (26896 грн) та експлуатаційних (18176 грн) витрат на заходи і засоби інформаційної безпеки, величину відвернених втрат (201240 грн) та, на основі цього, розраховано коефіцієнт повернення інвестицій (6,8) та термін окупності капітальних інвестицій (0,147 року). На основі розрахованих показників можна зробити

висновок, що запропоновані заходи та засоби є вигідними для компанії, оскільки термін окупності капітальних інвестицій є досить малим (менше двох місяців) та розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта (річної депозитної ставки з врахуванням інфляції).

ВИСНОВКИ

Під час виконання кваліфікаційної роботи було обґрунтовано необхідність створення КСЗІ на підприємстві “ArtCastle”, виконано обстеження середовищ функціонування ІТС відповідно до НД ТЗІ 3.7-003-2005 «Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі». На основі отриманих даних було виділено актуальні вразливості та створено перелік актуальних джерел загроз. Було визначено актуальні загрози, виходячи зі списку вразливостей та джерел загроз. Проведено аналіз існуючих в ІТС критеріїв захищеності та обрано список рекомендованих додаткових критеріїв, зважаючи на актуальні загрози. Для визначення критеріїв захищеності АС було використано НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» та НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». З метою захисту від загроз інформаційній безпеці підприємства було розроблено розділи політики безпеки. Для їх створення було використано, в тому числі, рекомендації описані в НД ТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі». Після цього, було проведено аналіз економічної вигідності запропонованих в розділах політики безпеки заходів і засобів.

ПЕРЕЛІК ПОСИЛАНЬ

1 НД ТЗІ 3.7-003-05 "Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі" [Електронний ресурс]. – 2005. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074.

2 Закон України "Про захист персональних даних" [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

3 НД ТЗІ 2.5-004-99 "Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/doccatalog/.

4 НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/.

5 НД ТЗІ 1.1-002-99 "Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: www.dsszzi.gov.ua/dsszzi/.

6 Закон України "Про інформацію" [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2657-12.

7 Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

8 НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу" [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://tzi.com.ua/downloads/1.1-003-99.pdf.

9 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації. Технічний захист інформації. Терміни та визначення. ДСТУ 3396.2-97 [Електронний ресурс]. – 1998. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/.

10 НД ТЗІ 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі" [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/.

11 ЕКСПЛУАТАЦІЯ СИСТЕМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ [Електронний ресурс]. – 2013. – Режим доступу до ресурсу: https://lektsii.org/15-1903.html.

12 Віхорєв С. В. КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ [Електронний ресурс] / Сергій Вікторович Віхорєв. – 2001. – Режим доступу до ресурсу: https://elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf.

13 ІНСТРУКЦІЯ з порядку обліку і зберігання знімних носіїв конфіденційної інформації [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://www.mpsu-yar.ru/images/mpsu/docs/polozheniya/.

14 Рекомендації щодо захисту Active Directory: Частина 1. Бекап контролера домену [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.veeam.com/blog/ru/backing-up-domain-controller-best-practices-for-ad-protection.html.

15 Крижанівський В. Б. КОНСПЕКТ ЛЕКЦІЙ з курсу «Безпека інформаційних систем» [Електронний ресурс] / В'ячеслав Борисович Крижанівський. – 2012. – Режим доступу до ресурсу: https://learn.ztu.edu.ua/mod/resource/view.php?id=201.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	37	
6	А4	Спеціальна частина	19	
7	А4	Економічний розділ	12	
8	А4	Висновки	1	
9	А4	Список літератури	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

- Маркіна М.В._УБіт-15-1.docx
- Маркіна М.В._УБіт-15-1.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник економічного розділу к.е.н., доц. Пілова Д.П.

Дата: _____ Підпис: _____

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

«Розробка політики безпеки інформації інформаційно-комунікаційної системи ТОВ "АртКасл"»

студентки групи Убіт-15-1 Маркіної Марії Володимирівни

Кваліфікаційна робота за спеціальністю 6.170103 Управління інформаційною безпекою Маркіної М.В. представлена пояснювальною запискою на 85 с., 9 рис., 14 табл., 4 додатка, 15 джерел.

Мета кваліфікаційної роботи – підвищення рівня безпеки інформації в ІТС ТОВ «АртКасл», розробка рішень для захисту від загроз інформаційної безпеки. Тема і зміст дипломної роботи повністю відповідає технічному завданню на дипломну роботу.

У ході виконання дипломного проекту були вирішені наступні питання: аналіз існуючих загроз, обґрунтування необхідності створення комплексної системи захисту інформації для ОІД ТОВ "АртКасл", приведена модель загроз та порушника для підприємства, прийняті проектні рішення щодо захисту інформації.

У економічному розділі були розраховані витрати на впровадження політики безпеки.

До недоліків проекту слід віднести окремі незначні невідповідності вимогам оформлення.

В цілому дипломний проект виконано у відповідності до вимог, які пред'являються до кваліфікаційної роботи бакалавра і заслуговує оцінки "відмінно", а Маркіна Марія Володимирівна – присвоєння їй кваліфікації "фахівець з організації інформаційної безпеки" освітньо-кваліфікаційного рівня "бакалавр".

Керівник кваліфікаційної роботи к.т.н., доц. Флоров С.В.

Дата: _____ Підпис: _____