Хмельницький національний університет
Факультет програмування та комп'ютерних
і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем та мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС»
Назва теми

КвРКБ.170143.17.01.04 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *125 «Кібербезпека»*
Шифр, назва

Освітня програма *Кібербезпека*

Виконав студент IV курсу, група КБ-17-1 _____ І. М. Демидов
Підпис Ініціали, прізвище

Керівник _____ К. В. Молодецька
Підпис, дата Ініціали, прізвище

Нормоконтролер _____ І. В. Муляр
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки,
та комп'ютерних систем
і мереж _____ Ю. П. Кльоц
Підпис, дата Ініціали, прізвище

17 06 2021 р.

Хмельницький, 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ПРОГРАМУВАННЯ ТА КОМП'ЮТЕРНИХ І ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Кафедра КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Освітній рівень БАКАЛАВР

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 125 КІБЕРБЕЗПЕКА

Освітня програма ОСВІТНЬО-ПРОФЕСІЙНА ПРОГРАМА ПІДГОТОВКИ БАКАЛАВРІВ

ЗАТВЕРДЖУЮ

Завідувач кафедри _____

_____

5 • 02 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Демидову Ігорю Миколайовичу

Прізвище, ім'я, по батькові студента

1 Тема роботи Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС»

Керівник роботи Молодецька Катерина Валеріївна, д.т.н., проф.

_____

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 05 02 2021р. № 11 додаток 9

2 Строк подання студентом роботи на кафедру: _____

3 Вихідні дані до роботи апаратні, програмні та криптографічні засоби захисту інформації, їх різновиди та способи використовування

_____

4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) Аналіз об'єкта захисту, обґрунтування вибору засобів для побудови системи безпеки, проектування системи безпеки, реалізація роботи

_____

5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень) «План розташування камер на підприємстві», «Загальна схема системи відеоспостереження», «Схема використання ЗКЗІ», «Встановлення зони спостереження»

6 Консультанти розділів курсового проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Муляр І.В., доцент кафедри КбКСМ		
Антиплагіат	Муляр І.В., доцент кафедри КбКСМ		

7 Дата видачі завдання 5 02 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Примітка
1	Вибір та затвердження теми кваліфікаційної роботи.	Січень	–
2	Аналіз об'єкта захисту.	Січень–лютий	–
3	Проектування та розробка загальної архітектури і структури системи захисту.	Лютий–березень	–
4	Програмна реалізація запропонованого рішення та тестування системи; аналіз результатів і оцінювання прийнятих рішень.	Квітень	–
5	Написання тексту пояснювальної записки та розробка графічних матеріалів.	Травень	–
6	Остаточне коригування кваліфікаційної роботи з урахуванням зауважень керівника.		–
7	Оформлення кваліфікаційної роботи як документа відповідно до вимог.		–
8	Отримання супровідних документів. Нормоконтроль.	Червень	–
9	Підготовка до захисту та захист кваліфікаційної роботи.		–

Студент _____ І. М. Демидов
Підпис Ініціали, прізвище

Керівник проекту (роботи) _____ К.В. Молодецька
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС».

Автор роботи: Демидов Ігор Миколайович.

Керівник роботи: Молодецька Катерина Валеріївна.

Обсяг – 76 с., 21 рис., 4 додатки, 24 джерел.

Графічна частина: 11 презентаційних слайдів, 4 плакати.

ІНФОРМАЦІЙНА БЕЗПЕКА, ЗАГРОЗИ, РИЗИКИ, ЗАХИСТ ІНФОРМАЦІЇ

Метою роботи є реалізація та впровадження системи управління інформаційною безпекою, оцінка ризиків інформаційної безпеки, аналіз загроз, створення план-схеми підприємства та проведення розрахунків для встановлення камер відеоспотереження.

У роботі був здійснений аналіз наявних засобів захисту інформації, інформація про додаткові засоби захисту.

В ході кваліфікаційної роботи була розроблена комплексна система захисту інформації на підприємстві.

Підпис студента:_____ Дата: 03.06.21

Форм	Зона	Позиція	Позначення	Найменування	Кіл.	Прим.
А4		1		Завдання на дипломний проект	1	
А4		2		Анотація	1	
А4		3	КвРКБ.170143.17.01.04 ПЗ	Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС» Пояснювальна записка	1	
А2		4	КвРКБ.170143.17.01.04 Е8	План розташування камер на підприємстві Схема структурна	1	
А2		5	КвРКБ.170143.17.01.04 Е8	Загальна схема системи відеоспостереження Схема структурна	1	
А2		6	КвРКБ.170143.17.01.04 Е8	Схема використання ЗКЗІ Схема структурна	1	

КвРКБ.170143.17.01.04 ВП

Зм.	Арк.	№ Докум.	Підп.	Дата	Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС» Відомість проекту	Літера	Аркуш	Аркушів
Розробив		Демидов І. М.				н	1	2
Перев.		Молодецька К.В.						
Н. контр.		Муляр І.В.			ХНУ, КБ-17-1			
Затв.		Кльоц Ю.П.						

Зона	Позиц	Позначення	Найменування	Кільк.	Прим.
	7	КвРКБ.170143.17.01.04 Е8	Встановлення зони спостереження	1	
			Схема структурна		

Зм.	Арк.	№ Докум.	Підп.	Дата	КвРКБ.170143.17.01.04 ВП	Арк. 2

ЗМІСТ

ВСТУП

Інформація є одним з найважливіших активів організації. Для організації інформація цінна і її слід належним чином захищати. Безпека полягає у поєднанні систем, операцій та внутрішнього контролю для забезпечення цілісності та конфіденційності даних та процедур роботи в організації. Історія інформаційної безпеки починається з історії комп'ютерної безпеки. Він розпочався приблизно в 1980 році. У 1980 році використання комп'ютерів зосередилося на комп'ютерних центрах, де впровадження комп'ютерної безпеки зосереджується на забезпеченні фізичної обчислювальної інфраструктури, що є високоефективною організацією.

Незважаючи на те, що відкритість Інтернету дозволила бізнесу швидко прийняти свою технологічну екосистему, це також виявилося великою слабкістю з точки зору інформаційної безпеки. Початкове призначення системи як засобу співпраці між групами довірених колег більше не є практичним, оскільки використання поширилося на мільйони часто анонімних користувачів.

Численні інциденти з безпекою, пов’язані з вірусами, хробаками та іншим шкідливим програмним забезпеченням, сталися з часів «Черв’яка Моріса», який був першим і закрив 10% систем в Інтернеті в 1988 р. Ці інциденти ставали дедалі складнішими та дорожчими. Однак рівень обізнаності щодо інформаційної безпеки зростає. Багато організацій запровадили інформаційну безпеку для захисту своїх даних.

Загалом, інформаційну безпеку можна визначити як захист даних, якими володіє організація чи особа від загроз чи ризиків. Згідно зі словником Merriam-Webster, безпека взагалі - це якість або стан безпеки, тобто відсутність пошкоджень.

Згідно з Oxford Students Dictionary Advanced, у більш оперативному сенсі також вживаються заходи безпеки для забезпечення безпеки країни, людей,

цінних речей тощо. Шнайєр (2003) вважає, що безпека полягає у запобіганні несприятливих наслідків навмисних та невиправданих дій інших людей.

Тому метою безпеки є побудова захисту від ворогів тих, хто завдав би шкоди, навмисно чи ні. Відповідно до Whitman and Mattord (2005), інформаційна безпека - це захист інформації та її найважливіших елементів, включаючи системи та обладнання, які використовують, зберігають та передають цю інформацію.

Інформаційна безпека - це сукупність технологій, стандартів, політик та практик управління, які застосовуються до інформації для її захисту. Інформаційна безпека виконує чотири важливі функції для організації, що забезпечує безпечну роботу програми, реалізованої в системах інформаційних технологій (IT) організації, захищає дані, які організації збирають і використовує, захищає технологічні активи, що використовуються в організації, і, нарешті, є для захисту здатності організації функціонувати. Інформаційна безпека також забезпечує безпечну роботу програми, реалізованої в системах інформаційних технологій (IT) організації.

Це пов’язано з тим, що для захисту даних організація застосує або встановить відповідне програмне забезпечення, яке захищатиме дані, наприклад антивірус та інші захищені програми.

Отже, інформаційна безпека дуже важлива в організації для захисту програм, що реалізуються в організаціях, а також для захисту сховища даних на комп'ютері. Окрім захисту даних, встановлений додаток також повинен бути захищений, оскільки він може сприяти втраті чи пошкодженню інформації. Інформаційна безпека захистить дані, які організація збирає та використовує. Якщо інформація залишається незахищеною, кожен може отримати до неї доступ. Якщо інформація потрапляє в чужі руки, це може знищити життя людей, залишити бізнес, а також може бути використано для заподіяння шкоди.

Програми інформаційної безпеки забезпечуватимуть захист відповідної інформації як діловими, так і юридичними вимогами через заходи, вжиті для

захисту даних організації. Крім того, заходи, вжиті для захисту інформації організацій, є питанням збереження конфіденційності та допоможуть запобігти крадіжці особистих даних. В організації інформація є важливим і важливим діловим активом для бізнесу, і тому потребує належного захисту. Це особливо важливо в умовах дедалі більш взаємопов'язаного ділового середовища, в якому інформація зараз стикається зі зростаючим числом і широким розмаїттям загроз та вразливостей. Нанесення таких збитків, як зловмисний код, хакерські атаки та атаки на відмову в сервісі, стали більш поширеними, більш амбіційними та більш складними.

Отже, впроваджуючи інформаційну безпеку в організації, ви можете захистити технологічні активи, що використовуються в організації. З точки зору захисту функціональних можливостей організації як загальне керівництво, так і управління IT відповідають за впровадження інформаційної безпеки, яка захищає здатність організації функціонувати. Інформація є найважливішим елементом організації для ведення бізнесу. Окрім організації, яка зберігає інформацію своїх клієнтів, для них надзвичайно важливо захищати інформацію. Без інформації бізнес не може функціонувати. Захист сховища інформації; Це також може дозволити організації вести свій бізнес. Ось чому інформаційна безпека важлива в організаціях.

1 ІНФОРМАЦІЙНА БЕЗПЕКА НА ПІДПРИЄМСТВІ «ІНФОСЕРВІС»

1.1 Джерела вразливостей інформаційної безпеки на підприємстві

Будь-яка робота щодо кібер-ризиків в організації повинна починатися з розуміння більш широкого погляду організації на бізнес-ризик, який повинні обов'язково вивчити наслідки або наслідки несподіваних подій. Це може призвести до будь-чого з наступного:

- Фінансові збитки, які можуть включати втрату бізнесу чи інтелектуальної власності.
- Юридичні та нормативні санкції, які можуть виникнути як через порушення регуляторної практики, так і через недотримання нормативних термінів.
- Репутаційний збиток, який, як правило, починається з негативних повідомлень у ЗМІ.
- Пошкодження діяльності організації, що може призвести до подальшої шкоди репутації.
- Шкода персоналу організації або загальній громадськості, що знову може спричинити шкоду діяльності та репутації організації.

Хоча багато з них не засновані на чистих фінансах, суть полягає в тому, що в основному йдеться про гроші, оскільки багато інших видів впливу в кінцевому підсумку призведуть до певної форми фінансових втрат, прямо чи опосередковано.

Сьогодні, оскільки ризики та загрози стали більш досконалими, тепер є два додаткові основоположні завдання:

- Визначте екосистему організації
- Впровадити тренінг з підвищення обізнаності щодо безпеки для працівника

Комплексна оцінка вразливості до компрометації інформації вимагає ознайомлення з основними причинами ризику інформаційної безпеки. З цією метою більшість текстів про інформаційну безпеку зосереджуються на технологіях під час виявлення проблем, що потребують виправлення.

Виняткова увага до технологій ігнорує організаційні проблеми, що спричиняють ризик інформаційної безпеки, але проявляються як технологічні проблеми. Фактично віртуальна лавина інформації генерується засобами управління технологіями безпеки. Ці засоби контролю можуть бути ефективними для виявлення тактичних проблем, але може бути більш широкий ризик, пов'язаний із отриманими таким чином даними безпеки важко інтерпретувати відповідно до виявлення системних проблем безпеки.

Як зазначалося раніше, основними джерелами вразливостей інформаційної безпеки в організаціях є наступні:

- ділова практика
- відсутність управління безпекою
- Впровадження IT
- фізична безпека інформаційних активів
- поведінка користувача

Ділова практика невблаганно пов’язана з організаційною культурою, де перша є побічним продуктом другої. Насправді, не буде перебільшенням сказати, що культура формує позицію безпеки в будь-якій організації і відображає результат діалектики безпеки та зручності, що розгортається щодня.

Недолік управління безпекою, можливо, обумовлений також організаційною культурою. Розхлиблений підхід до розробки та впровадження політики інформаційної безпеки випливає з культури вседозволеності або де творчість заохочується на всіх рівнях. Зокрема, відсутність чітко розроблених політик та стандартів безпеки корелює із поширенням уразливих місць інформаційної безпеки.

Впровадження IT явно є джерелом факторів ризику для компрометації інформації.

Погана реалізація технологій, що використовуються для зберігання, обробки та / або передачі конфіденційної інформації, сприяє загальному профілю ризику організації, і на неї слід звертати увагу як на тактичному, так і на стратегічному рівні, але не за винятком інших джерел ризику.

Поведінка користувача заслуговує на пильну увагу при виявленні першопричин ризику інформаційної безпеки. Поведінка користувачів у цьому контексті включає історію відвідуваних веб-сайтів, привілеї електронного доступу (наприклад, користувача Windows, локального адміністратора, адміністратора домену), фізичний доступ системні привілеї, історія доступу до внутрішніх ресурсів та складність паролів.

1.2 Управління ризиками на підприємстві «Інфосервіс»

Управління ризиками є ключовим для управління організацією та захисту її інформаційних активів. Якщо організація не знає ризиків, з якими стикається, вона не зможе здійснити належне та ефективний захист.

Загалом, необхідні комплексні оцінки ризиків інформаційної безпеки, щоб встановити глибоке розуміння факторів ризику, що впливають на організацію. Крім того, такі оцінки повинні проводитися стосовно політики та стандартів, заснованих на ризику, за відсутності корисної статистики щодо інцидентів. Прийняття процесу суворої оцінки ризиків, пов'язаних із загрозами інформаційної безпеки, має важливе значення для розвитку узгодженого ризику інформаційної безпеки стратегія управління

Чотири основні компоненти управління ризиками, зазначені в літературі, це:

виявлення ризику,

аналіз ризиків,

заходи щодо зменшення ризику,

моніторинг ризику.

Управління ризиками для ІТ починається з процесу ідентифікації ризиків, який дозволяє підприємствам на ранній стадії визначити потенційний вплив реалізації внутрішніх та зовнішніх загроз на все ІТ-середовище. Ідентифікація ризиків - це процес виявлення, опису, документування та передачі ризиків до того, як вони стануть проблемами та негативно вплинуть на організацію

Аналіз ІТ-ризику, безсумнівно, є ключовим елементом процесу управління безпекою інформаційних систем, а отже, і управління ризиками. Публікації, пов’язані з цими проблемами - як внутрішніми, так і міжнародними, - схоже, трактують це довільно.

Це проявляється у безлічі визначень аналізу ризиків, а також у тому, що аналіз ризику часто ототожнюється з його управлінням. Аналіз ризиків є основним і найважливішим процесом управління ризиками, визначає та оцінює ризик, який необхідно контролювати, мінімізувати або приймати. Аналіз ризиків - це всебічне виявлення загроз та сприйнятливості активів ІТ-системи та визначення необхідності її контролю або прийняття визначених заходів на раніше заявленому рівні. Метою аналізу ризиків є надання інформації, яка є необхідною для прийняття рішення про застосування зазначених методів, ресурсів безпеки на підприємстві. Аналіз ризику схильний виконувати роботи в таких областях:

- Оцінка ресурсів (інформація, програмне, апаратне забезпечення та фізичні ресурси) - вартість ресурсу - це не тільки вартість його придбання, але також короткочасні наслідки та довгострокові наслідки від його знищення,
- Оцінка наслідків - визначення ступеня руйнування або втрат, які можуть нібито статися,
- Ідентифікація загроз - аналіз загроз повинен визначити ймовірність їх виникнення та можливість знищення ресурсів,

- Аналіз засобів захисту з точки зору ефективності існуючих засобів захисту,
- Аналіз сприйнятливості певних ресурсів ІС,
- Оцінка ймовірності - це частота виникнення загрози - цей знак повинен охоплювати наявність, тривалість та силу загрози, а також ефективність захисту.

Кількісні та якісні методи - це дві основні групи методів, що застосовуються для аналізу ризику, якому піддаються активи на підприємствах.

Групи методів аналізу ІТ-ризиків:

Кількісна, коли оцінка значення ризику пов'язана із застосуванням чисельних показників - вартість ресурсів визначається у величинах, частоті виникнення загрози у кількості випадків та сприйнятливості за величиною ймовірності її втрати, ці методи представляють результати форма показників. Приклади кількісних методів: очікувана річна втрата, методи Кортні та Фішера, модель ISRAM тощо.

Якісні, які не оперують числовими даними, представляючи результати у вигляді описів, рекомендацій, де ризик оцінки ризику пов'язаний з: якісним описом вартості активів, визначенням якісних шкал щодо частоти виникнення загрози та сприйнятливості для даного загроза або опис так званих сценаріїв загрози шляхом прогнозування основних факторів ризику.

Приклади якісних методів: FMEA / FMECA, Microsoft Corporate Security Group Risk Management Framework, NIST SP 800-30, CRAMM. Залежно від серйозності даної загрози можуть застосовуватися різні міри ризику від дуже простих оцінок, що визначають ризик як високий, середній та низький, до дуже точних показників, представлених як ймовірність настання даної події. У разі оцінки ризику інформаційної безпеки в Інформаційній системі зазвичай проводиться якісний аналіз ризику. Цей метод найчастіше базується на таких критеріях інформаційної безпеки, як: конфіденційність, цілісність та доступність.

Повний аналіз ризику може бути проведений окремо для кожного із згаданих критеріїв. Правильна оцінка ризику та оцінка ймовірності його виникнення дає чітке уявлення про його вплив на функціональність всієї Інформаційної системи.

1.3 Постановка задачі

Після дослідження усіх аспектів захисту інформації стало зрозуміло, що через збільшення ролі інформаційних технологій в житті людини, збільшуються і вимоги до забезпечення безпеки. Не існує єдиновірного рішення щодо забезпечення якісного захисту підприємств, кожний випадок потребує окремого аналізу.

Аналіз об’єкта захисту дав змогу виявити напрямки модифікацій системи захисту інформації. Для вирішення задачі було обрано побудова комплексної системи захисту інформації.

Сформульовано практичне завдання проекту:

— модифікація існуючої системи захисту об’єкту;

— створення моделей загроз та порушника;

— моделювання можливих каналів витоку інформації;

2 ДОСЛІДЖЕННЯ ТА АНАЛІЗ ІНФОРМАЦІЙНИХ ПОТОКІВ НА ПІДПРИЄМСТВІ «ІНФОСЕРВІС» ЯК ОБ'ЄКТА ЗАХИСТУ

2.1 Інформаційні потоки на підприємстві «Інфосервіс»

Структурна схема потоків інформації підприємства «Інфосервіс» представлена на рис. 2.1.

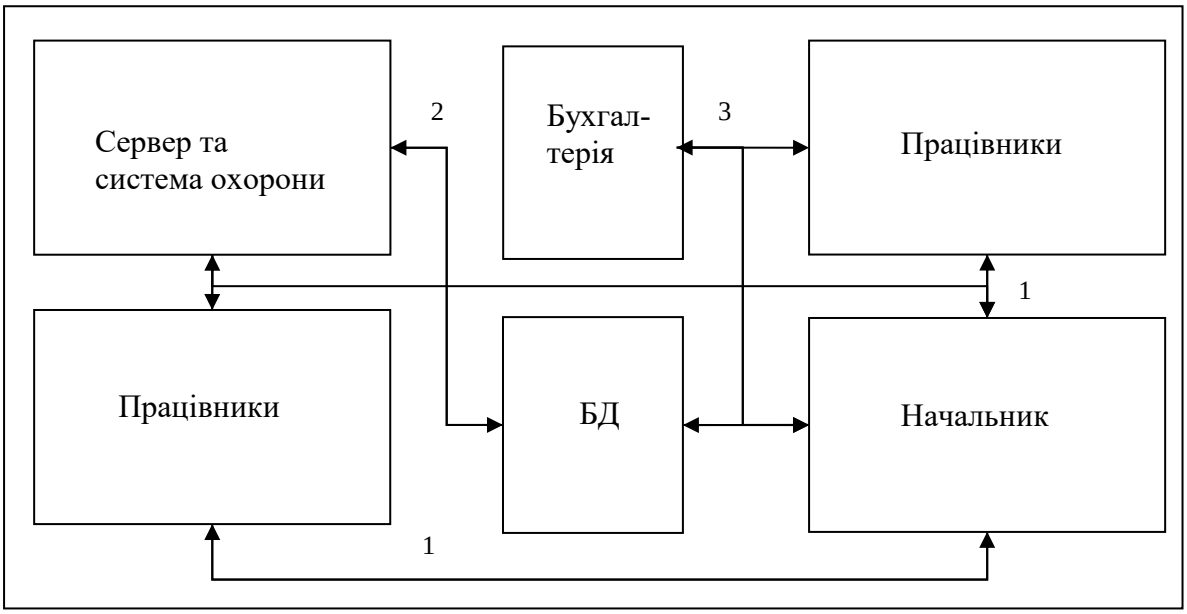


Рисунок 2.1 - Структурна схема потоків інформації підприємства

На рисунку 2.1 у вигляді блоків схематично представлені наступні елементи:

— Начальник – керівник фірми, виконує організаційні функції та керує процесом роботи;

— Працівники – група співробітників, яка складає основну частину персоналу, виконують задачі згідно наказів начальника.

— Сервер та система охорони – група обладнання та програмний комплекс пов’язаних із обробкою, збереженням, аналізом та захистом інформації, яка використовується всередині підприємства;

Серед розглянутих інформаційних потоків є:

1) Зв’язок начальника та персоналу, видача завдань кожній групі працівників

2) Бази даних – доступ до баз даних для працівників та начальника, згідно з рівнем доступу.

3) Бухгалтерія –розпорядження та накази, видача заробітної плати та різні організаційні питання.

Джерелами інформації можуть бути суб’єкти та об’єкти, від яких інформація може потрапити до зловмисника або людини, яка не повинна була отримати доступ.

Основними джерелами інформації є: люди; документи; датчики вимірювання; засоби обробки інформації; матеріал і технічне обладнання.

Кожна людина володіє різною кількістю інформації, начальник чи його заступник знають набагато більше конфіденційної інформації чін рядовий працівник, проте все-одно, навіть рядовий співробітник знає набагато більше, ніж йому потрібно для роботи. Виток інформації може статись внаслідок неформального спілкування з друзями та знайомими.

Пункт документи означає усю інформацію, яка десь записана, до неї відносяться як паперові носії інформації, так і електронні, наприклад звіти співробітників, різні публікації, службову інформацію тощо.

Класифікація інформації у відповідності до Закону України «Про інформацію» предсталена на рис. 2.2.

Рисунок 2.2 - Класифікація інформації у відповідності до Закону України «Про інформацію»

Для об’єкту захисту, що розглядається в рамках даного курсового проекту, актуальними класами інформації є:

— Відкрита інформація;

— Конфіденційна інформація;

— Банківська таємниця

— Службова таємниця;

— Таємниця нарадчої кімнати;

— Таємниця листування, телефоних розмов та телеграфних відправлень.

Наведені категорії є необхідними для роботи інформаційно-телекомунікаційної системи об’єкту захисту.

В ході аналізу структури роботи ІТС об’єкту захисту найбільш використованими носіями інформації виявились носії вказані в табл. 2.1.

Таблиця 2.1 - Носії інформації, методи та засоби захисту

№ з/п	Перелік носіїв для нформаційних ресурсів	Засоби захисту
1	Документи	Організаційні
2	Люди	Організаційні
3	Жорсткі диски	Шифрування
4	Флеш-накопичувачі	Шифрування
5	Телефони	Організаційні

Протягом майже двох десятиліть після створення першого у світі цифрового комп’ютера в 1943 році здійснення кібератак було складним завданням. Доступ до гігантських електронних машин був обмежений невеликою кількістю людей, і вони не були пов’язані з мережею - лише декілька людей знали, як ними працювати, тому загроза майже не існувала.

Цікаво, що теорія, що лежить в основі комп'ютерних вірусів, була вперше оприлюднена в 1949 році, коли піонер комп'ютера Джон фон Нойман припустив, що комп'ютерні програми можуть відтворюватися.

1950-ті: телефонний фрік

Наприкінці 1950-х років з’явився «фрік телефон». Цей термін охоплює декілька методів, які "виродки" - люди, які особливо цікавляться роботою

телефонів - використовували для викрадення протоколів, які дозволяли інженерам телекомунікацій працювати в мережі віддалено, щоб здійснювати безкоштовні дзвінки та уникати плати за далекі відстані. На жаль, для телефонних компаній не було способу зупинити фреки, хоча ця практика врешті-решт вимерла у 1980-х.

1960-ті:

Навіть до середини 1960-х років більшість комп'ютерів були величезними мейнфреймами, зачиненими в захищених приміщеннях з регульованою температурою. Ці машини були дуже дорогими, тому доступ - навіть для програмістів - залишався обмеженим.

Однак деякі з тих, хто мав доступ, часто студенти, мали випадки хакерської атаки. На цьому етапі напади не мали комерційних або геополітичних переваг. Більшість хакерів були цікавими зловмисниками або тими, хто прагнув вдосконалити існуючі системи, змусивши їх працювати швидше або ефективніше.

У 1967 році IBM запросила школярів спробувати свій новий комп'ютер. Після вивчення доступних частин системи студенти працювали над глибшим дослідженням, вивчаючи мову системи та отримуючи доступ до інших частин системи.

Це було цінним уроком для компанії, і вони визнали свою вдячність "ряду старшокласників за їх примус бомбити систему", що призвело до розробки захисних заходів - і, можливо, оборонного мислення, яке виявилося б важливим для розробників з тих пір. Етичний злом практикується і сьогодні.

1970-ті: народжується комп'ютерна безпека

Власна кібербезпека розпочалась у 1972 році з дослідницького проекту на ARPANET (Мережа Агентства перспективних дослідницьких проектів), попередника Інтернету.

ARPANET розробив протоколи для віддалених комп'ютерних мереж.

Дослідник Боб Томас створив комп’ютерну програму під назвою Creeper, яка може рухатись по мережі ARPANET, залишаючи слід, де б не було. У ньому було написано: «Я повзучий, злови мене, якщо зможеш». Рей Томлінсон - винахідник електронної пошти - написав програму Reaper, яка переслідувала і видаляла Creeper. Reaper був не лише першим прикладом антивірусного програмного забезпечення, але і першою програмою, що самовідтворюється, що робить його першим у світі комп’ютерним хробаком.

У міру зростання залежності від комп’ютерів та зростання мереж, урядам стало зрозуміло, що безпека є надзвичайно важливою, а несанкціонований доступ до даних та систем може бути катастрофічним. У 1972-1974 рр. Спостерігалося помітне посилення дискусій навколо комп'ютерної безпеки, головним чином в наукових роботах.

До середини 70-х років концепція кібербезпеки визрівала. У 1976 році Структури операційних систем для підтримки безпеки та надійного програмного забезпечення заявили: "Безпека стала важливою та складною метою при розробці комп'ютерних систем".

1987: Народження кібербезпеки

1987 рік був родом комерційного антивірусу, хоча є конкуруючі претензії щодо новатора першого антивірусного продукту.

Андреас Люнінг та Кай Фігге випустили свій перший антивірусний продукт для Atari ST, який також випустив Ultimate Virus Killer (UVK)

Троє чехословацьких громадян створили першу версію антивірусу NOD

У США Джон Макафі заснував McAfee (на той час входив до складу Intel Security) і випустив VirusScan.

Також у 1987 році:

Одне з найбільш ранніх задокументованих вилучень вірусів було здійснено німецьким Берндом Фіксом, коли він знешкодив сумнозвісний віденський вірус - ранній приклад зловмисного програмного забезпечення, яке поширювало та пошкоджувало файли.

1990-ті: Підйом брандмауерів

Коли Інтернет стає доступним для громадськості, все більше людей починають розміщувати свою особисту інформацію в Інтернеті. Через це суб'єкти організованої злочинності розглядали це як потенційне джерело доходу і почали красти дані у людей та урядів через Інтернет.

До середини 90-х років загрози безпеці мережі зросли в геометричній прогресії, і як такі, брандмауери та антивірусні програми повинні були масово створюватися для захисту громадськості. Саме дослідник NASA створив першу розробку програми брандмауера після атаки комп'ютерного вірусу на їх базі в Каліфорнії. Дослідники та їх команда створили віртуальний "брандмауер", який вони змоделювали на фізичних спорудах, що запобігають поширенню фактичних пожеж всередині будівель чи споруд.

Однак, хоча ці брандмауери та антивірусні програми мали певний шлях до мінімізації ризику атак, комп'ютерні віруси та хробаки постійно надходили рясно і швидко, тому хакери, безумовно, мали перевагу на той момент.

2000-ті: належне покарання

На початку 2000-х уряди почали припиняти злочинність хакерства, даючи винним набагато серйозніші покарання - включаючи великий тюремний термін і великі штрафи. Це було далеко від 1980-х років, коли хакерам давали набагато легші покарання - від суворих попереджень до умовного терміну.

Інформаційна безпека продовжувала прогресувати в міру зростання Інтернету, але, на жаль, зростали і віруси. Хакери швидко змогли створити віруси, які можуть бути націлені не тільки на певні організації, а й на цілі міста, штати і навіть континенти.

2010-ті: Ера великих порушень

Завдяки послідовному піднесенню технологій, злом ускладнювався протягом наступних років, і низка основних порушень даних зараз багато в чому визначає епоху. До них належать:

Сноуден і АНБ, 2013. Едвард Сноуден - колишній співробітник ЦРУ та підрядник уряду США - копіював та витікав секретну інформацію з Агентства національної безпеки (АНБ), підкреслюючи той факт, що уряд фактично "шпигував" за громадськістю. Його суперечливо вважають героєм, а когось зрадником.

Yahoo, 2013 - 2014 рр. Хакери увірвались у Yahoo, поставивши під загрозу облікові записи та особисту інформацію всіх своїх трьох мільярдів користувачів. Їх оштрафували на 35 мільйонів доларів за невчасне розголошення новин про порушення, а в результаті ціна продажу Yahoo зменшилася на 350 мільйонів доларів.

WannaCry, 2017. Більш відомий як перший «викупник», WannaCry націлював комп'ютери під управлінням операційної системи Microsoft Windows і вимагав викупних платежів у криптовалюті Bitcoin. Лише за один день черв'як заразив понад 230 000 комп'ютерів у 150 країнах.

Незважаючи на те, що кожне з цих порушень даних було неймовірно серйозним, на щастя, існує низка компаній, які пропонують рішення щодо цих потенційних трагедій - тож це не все погано.

Інформаційна безпека постійно покращується, і багато компаній розробляють широкий спектр варіантів пом'якшення атак для початківців, які використовують такі речі, як аналіз поведінки мережі (NBA), брандмауери веб-додатків (WAF) та захист від відмови в обслуговуванні (DoS).

Однак на більш особистому рівні людям і компаніям життєво важливо стежити за своєю інформаційною безпекою та впроваджувати методи, що забезпечують захист їхніх даних. Наприклад, якщо ви займаєтеся бізнесом, використання експертної служби сканування, зберігання та управління документами може надати вам спокій, за яким ви перебуваєте, знаючи, що ваші документи в безпеці. Подібним чином використання хмарної платформи для зберігання ваших особистих файлів може бути абсолютно знахідкою, якщо ви коли-небудь втратите або пошкодите свої фізичні файли.

2.2 Аналіз та дослідження рівнів захисту(LOFA) на підприємстві «Інфосервіс»

Використовуючи аналіз ризику, LOPA також може бути включений для вдосконалення впровадження інструментів оцінки наслідків (Summers, 2010). На додаток до інструменту оцінки наслідків, аналіз ризику також залежить від передбачуваної частоти небезпечної події. Крім того, будь-яка помилка, пов'язана з оцінкою тяжкості наслідків, безпосередньо впливає на заходи щодо зменшення ризику. Більшість фахівців із безпеки виявлять, що використання LOPA є простим та гнучким. Намагаючись визначити пріоритети на основі оцінки частоти небезпечних подій, уважно подивіться на ті основні причини подій, які призводять до небезпечної події, і на можливість того, що заходи безпеки та безпеки можуть провалитися. Професіонали охорони будуть використовувати досвід для визначення правильних типів захисних шарів для використання та використовувати найкращі практики, щоб продемонструвати методи зменшення або зменшення ризику, які працювали під час попереднього аналізу ризику. Спеціалістам з безпеки потрібно буде визначити основні причини (або ініціюючі причини) та проаналізувати ті умови, що сприяють відхиленню процесу (або ініціюванню подій). Це є критично важливою частиною аналізу ризику, оскільки розуміючи ймовірність видів небезпек, які можуть виникнути, та умов, що дозволяють це зробити, фахівці з безпеки можуть оцінити частоту початкової події.

У LOPA фахівець з безпеки може рекомендувати IPL на основі небезпеки чи загрози. Крім того, IPL може бути найкращою практикою, яка, як відомо, забезпечує зниження ризику (тобто огорожі, ворота, охорона, поліція, відеоспостереження, сигналізація тощо ...). Як правило, використовуються всі вищезазначені найкращі практики, однак сигнали тривоги, як правило, ідентифікуються як засоби безпеки та охорони, які використовуються як вхідні дані в системи ідентифікації та сповіщення. В основному такі типи сигналів

тривоги визначаються як «звуковий та / або видимий засіб індикації оператору несправності обладнання, відхилення процесу або ненормального стану, що вимагає реакції», який відрізняється від сигналізації безпеки, «сигналізації, яка є класифікується як критично важливий для безпеки процесів або захисту людського життя ».

Використання методу зниження ризику IPL також дозволяє фахівцеві з безпеки оцінити частоту небезпечних подій на основі інформації та даних про події, що відповідають ключовим показникам ефективності (тобто це можуть бути журнали тривог, використання системи відеоспостереження для перегляду інцидентів, звітів поліції, персоналу або інформація про відвідувачів тощо ...). Ще раз фахівці з безпеки виявлять, що LOPA - це чудовий інструмент для оцінки широкого спектру критичних сценаріїв загрози, а також здатності застосовувати відповідні шари захисту та проектні заходи. Крім того, LOPA може бути використаний як напівкількісний аналіз, як уже згадувалося раніше, з ключовими характеристиками, що також дозволить ефективно оцінити загрозу або вразливість. Реально, чим більше організацій прогресує у використанні та впровадженні LOPA в різних школах, це незмінно призведе до подібного використання, порівняння та запитань щодо впровадження. Коли подібні загрози або вразливості порівнюватимуться від школи до школи, LOPA стане більш постійним, а співробітники побачать зміни в оцінці ризику для подібних загроз. На щастя, процедури LOPA мають чітко визначені методи, які можуть застосовувати фахівці з безпеки при оцінці будь-якого типу частоти небезпечних подій. Крім того, це допоможе зрозуміти невідповідність оцінки ризику, яка, як правило, зумовлена різницею в оцінюваній тяжкості наслідків.

Використовуючи аналіз ризику, LOPA також може бути включений для вдосконалення впровадження інструментів оцінки наслідків. На додаток до інструменту оцінки наслідків, аналіз ризику також залежить від передбачуваної частоти небезпечної події. Крім того, будь-яка помилка, пов'язана з оцінкою тяжкості наслідків, безпосередньо впливає на заходи щодо зменшення ризику.

Більшість фахівців із безпеки виявлять, що використання LOPA є простим та гнучким. Намагаючись визначити пріоритети на основі оцінки частоти небезпечних подій, уважно подивіться на ті основні причини подій, які призводять до небезпечної події, і на можливість того, що заходи безпеки та безпеки можуть провалитися. Професіонали охорони будуть використовувати досвід для визначення правильних типів захисних шарів для використання та використовувати найкращі практики, щоб продемонструвати методи зменшення або зменшення ризику, які працювали під час попереднього аналізу ризику.

Спеціалістам з безпеки потрібно буде визначити основні причини (або ініціюючі причини) та проаналізувати ті умови, що сприяють відхиленню процесу (або ініціюванню подій). Це є критично важливою частиною аналізу ризику, оскільки, розуміючи ймовірність видів небезпек, які можуть виникнути, та умов, що дозволяють це зробити, фахівці з безпеки можуть оцінити частоту початкової події

2.3 Дослідження режимів відмов та ефектів на підприємстві «Інфосервіс»

Аналіз режимів відмов та ефектів (FMEA) та FailureModes, Effects and Critical Analysis (FMECA) - це методології, призначені для виявлення потенційних режимів відмов для продукту або процесу до виникнення проблем, для оцінки ризику. В ідеалі, FMEA проводиться на стадіях розробки продукту або процесу, хоча проведення FMEA на існуючих продуктах або процесах також може принести користь.

Команда FMEA визначає, аналізуючи режим відмов, ефект кожного збою та визначає окремі точки відмови, які є вирішальними. Він також може класифікувати кожну несправність відповідно до критичності ефекту несправності та ймовірності її виникнення.

FMECA є результатом двох кроків:

- Режим відмов та аналіз ефектів (FMEA)

- Аналіз критичності (CA).

Аналіз краватки-метелика зосереджений на бар'єрах або елементах управління, зображених на лівій стороні вузла, які можуть змінити ймовірність події чи обставини, або на правому боці, які можуть змінити її наслідки. Він використовується при оцінці повноти засобів контролю, щоб перевірити, чи кожен шлях від причини до події та події до наслідку має ефективні засоби контролю та чи визнаються фактори, які можуть спричинити збій у керуванні (включаючи збої в системах управління).

Основним використанням аналізу краватки є виявлення прогалин у контролі, де можуть бути необхідними додаткові засоби контролю. Вивчення причин, наслідків та існуючих засобів контролю, що стосуються їх, допомагає виявити прогалини в поточному контролі.

Найефективніші засоби контролю зазвичай стосуються причин, як правило, щоб зупинити їх виникнення або приведення до ризику (превентивний контроль). Вони повинні відповідати причинам, за ступенем та характером. Це вимагає чіткого розуміння причин та їх наслідків для бізнес-цілей, часто з деякими деталями. Наприклад, системи технічного обслуговування є превентивним контролем щодо ризиків, пов’язаних із цілісністю активів.

Праворуч від краватки-метелика органи управління повинні забезпечувати відповідні реакції на наслідки, що відчуваються, або створювати перешкоди для наслідків, що розвиваються. Вони можуть або впливати безпосередньо на наслідки для бізнес-цілей (коригуючий чи реактивний контроль), або швидко виявляти зміни та створювати активатори для планів дій на випадок надзвичайних ситуацій (детективні засоби контролю). Наприклад, скупчення навколо ємності для зберігання може не перешкоджати випуску продукту, але це обмежує розповсюдження випуску і, отже, несприятливі наслідки; димова сигналізація - це детектив, що дозволяє швидко реагувати на пожежу.

Аналіз краватки-метелика є важливим фактором, що сприяє етапу лікування ризиків при управлінні ризиками; лікування ризику - це стадія, яка дозволяє

отримати користь від аналізу, проведеного раніше в процесі. Без лікування ризику ми лише описуємо ситуацію, в якій ми працюємо. Приклад діаграми “краватка-метелик” преставлений на рис. 2.3.

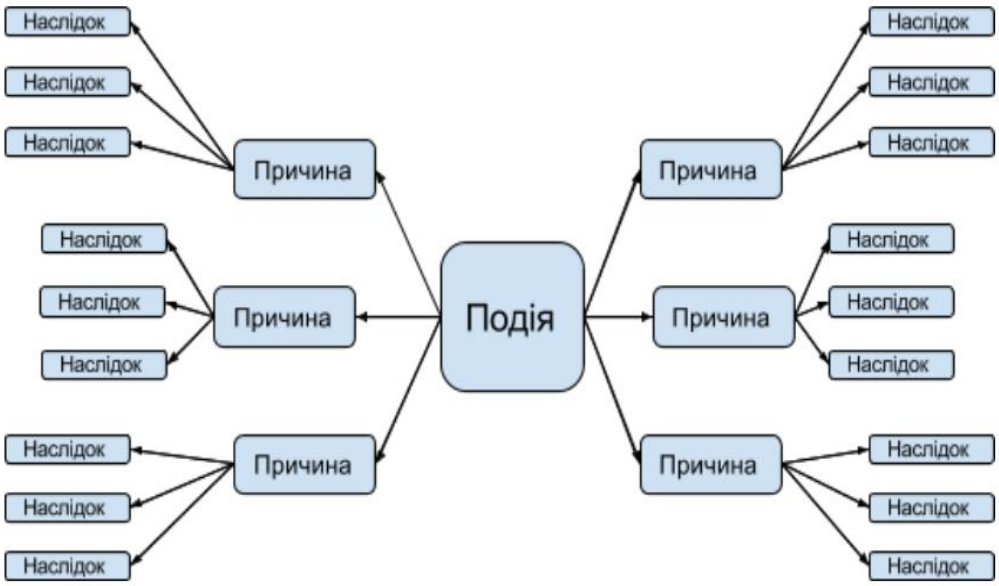


Рисунок 2.3 - Приклад діаграми “краватка-метелик”

Аналіз краватки-метелика є найбільш корисним у таких ситуаціях:

- Потрібна проста діаграма, щоб повідомити про коло причин та наслідків та відповідні засоби контролю
- Потрібна більш детальна інформація про причини та наслідки ризику, ніж міститься у реєстрі ризиків
- Де графічне зображення може бути набагато чіткішим, ніж текст
- Існують чіткі шляхи від причин до ризику та від ризику до наслідків
- Загальний рівень ефективності контролю вважається низьким
- Основна увага приділяється виявленню засобів контролю, ефективності контролю та прогалин у контролі та забезпеченню того, щоб кожен шлях мав контроль (бар’єр)

- Ситуація є більш складною, ніж один шлях "причина-подія-наслідок", але не настільки складна, що є повним аналіз дерева помилок та аналіз дерева подій.
- Аналіз краватки-метелика можна використовувати як для бажаних впливів, так і для тих, яких ми прагнемо уникати. У цьому випадку засоби контролю є не бар’єрами, а скоріше факторами, які підтримують або покращують шляхи.

Аналіз краватки-метелика не корисний, коли:

- Існує безліч причин, які пов'язані складними способами, наприклад, коли можуть бути ворота І та АБО в дереві несправностей, що зображають ліву сторону метелика
- Де потрібна детальна кількісна оцінка.

Рисунок 2.4 Поширені методи атак на підприємство

2.4 Висновки

В ході аналізу структури роботи ІТС об’єкту захисту було визначенно, інформаційні потоки підприємства, що дало нам змогу прогнозувати звідки та які дані можуть “витікати” за межі підприємства. Знайденно основні носії інформації та спосіб як запобігти витоку інформації з них.

За допомогою методів LOPA та “краватка-метелик”, було проаналізовано основні ризики для інформації на підприємстві та запропоновані рекомендації, як цьому запобігти.

Основні ризики та спосіб захисту:

Віруси та шкідливе ПЗ, незаконне проникнення, цільові атаки, несправність обладнання, помилки персоналу, помилки ПЗ, спосіб захисту – використання антивірусів, брандмауерів, створення резервних копій інформації та доступ до інформації лише особам з правами доступу до неї.

Пожежі, коротке замикання, доступ до інформації з проникненням – встановлення пожежних датчиків, камер відеонагляду та датчиків руху.

3 АПАРАТНЕ І ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ ПІДПРИЄМСТВА «ІНФОСЕРВІС»

3.1 Апаратне забезпечення підприємства «Інфосервіс»

Апаратне забезпечення інформаційної безпеки використовується для вирішення таких завдань:

- Проведення спеціальних досліджень технічних засобів для забезпечення виробничої діяльності та пошуку потенційних каналів виходу інформації.
- Виявлення каналів витоку інформації на різних об'єктах та кімнатах.
- Локалізація каналів витоку інформації.
- Шукати та виявляти засоби промислового шпигунства.
- Протидіяти несанкціонованому доступу до джерел конфіденційної інформації та іншим діям.

Апаратне обладнання класифікується наступним чином відповідно до його функціонального призначення:

- Засоби виявлення;
- Засоби пошуку та вимірювання.
- Засоби активних та пасивних контрзаходів.

У той же час засоби захисту інформації можуть бути загального призначення, часто використовуються непрофесіоналами для отримання попередніх (загальних) оцінок, залежно від їх технічних можливостей, а також професійні, для ретельного пошуку, виявлення та точних вимірювань всіх характеристик промислового шпигунства.

Перший приклад - це група показників електромагнітного випромінювання, наприклад, «індикатори поля», які мають широкий діапазон прийнятих сигналів і досить низьку чутливість.

Другий – Дельта комплекс, призначений для автоматичного виявлення та ідентифікації мережевих бездротових передавачів, бездротових мікрофонів, телефонних закладок та радіопередавачів. Це складний та сучасний експертно-розвідувальний комплекс.

Пошукові пристрої поділяються на пошукові пристрої для знімання інформації та дослідження каналів для цього джерела.

Перший тип пристроїв спрямований на пошук і локалізацію методів несанкціонованого доступу, вже реалізованих зловмисниками. Другий тип обладнання призначений для виявлення каналів витоку інформації.

Дослідження в таких системах дуже оперативні та отримують точні результати.

Лише висококваліфікований оператор повинен використовувати спеціалізоване пошукове обладнання.

Як і в інших технічних областях, різноманітність обладнання знижує параметри індивідуальних характеристик. З іншого боку, існує безліч фізичних каналів для витоку інформації, а також існує фізичний принцип роботи систем несанкціонованого доступу. Ці фактори визначають різноманітність пошукового обладнання, а його складність визначає високу вартість кожного пристрою. У зв'язку з цим достатній набір пошукового обладнання може мати структуру, яка завжди проводить відповідні дослідження. Це або служби безпеки, або компанії, що спеціалізовані в цьому напрямку, які обслуговують сторонніх замовників.

У більшості випадків для незалежних пошуків використовують прості засоби для профілактики перед серйозними пошуковими тестами.

До спеціальних груп належать апаратні засоби захисту комп’ютерів та системи зв'язку на їх основі.

Апаратний захист використовується як для окремих комп’ютерів, так і для різних рівнів та областей мережі.

Кодовий захист процесора використовується для захисту процесора. Тобто він створює додаткові біти у вигляді машинних інструкцій (секретів) та регістрів

резервного копіювання. Одночасно існує два можливі режими роботи процесора, відокремлюючи допоміжні операції від операцій, які безпосередньо вирішують проблему користувача. Це спеціальна система переривань, реалізована апаратним забезпеченням. Щоб вказати ступінь конфіденційності програми та даних, у категоріях користувачів використовуються біти, які називаються бітами конфіденційності (це два-три додаткові біти, які кодують категорії конфіденційності користувачів, програм та даних).

Програми та дані, завантажені в оперативну пам’ять, повинні бути захищені, щоб недопустити несанкціонованого доступудо них. Часто використовуються парні біти, ключі та стійка спеціальна пам'ять. Під час читання з оперативної пам’яті важливо переконатися, що програма не пошкоджена шкідливими діями користувача або збоями обладнання. Спеціальна схема стирання використовується для запобігання зчитуванню даних, що залишаються після обробки в оперативній пам'яті.

Для захисту засобів масової інформації рекомендуються такі заходи:

- Управління носіями інформації та перевірка реєстрації.
- Навчання користувачів правильному способу чистки та знищення носіїв інформації.
- Позначення носіїв інформації, залежно від рівня важливості інформації, яка там міститься
- Знищення носіїв інформації відповідно до планів організації.
- Дозволити лише уповноваженим особам доступ до носіїв інформації для зберігання, передачі, маркування та знищення.
- Зберігання носіїв інформації у важкодоступних місцях.
- Надання усіх необхідних документів працівникам.

Усі користувачі повинні бути авторизовані на персональних комп'ютерах, до яких вони закріплені, при змані робочого місця необхідно знову авторизуватись. Доступ до інформації обмежений правами доступу.

Для автентифікації користувача використовуються такі апаратні засоби:

- Ключі
- Кодові карти(ключ карти)
- Детектори відбитків, чи розпізнавання обличчя
- Персональні коди

3.2 Програмне забезпечення та пристрої безпеки підприємства «Інфосервіс»

Організації можуть використовувати як захисні пристрої, так і програмне забезпечення та програми захисту для захисту свого мережевого середовища.

Засоби безпеки

Пристрій безпеки - це пристрій або сервер, які можуть блокувати небажаний трафік від проникнення в мережу. Типи охоронних приладів включають:

- Пристрої виявлення вторгнень, які можуть попереджати команди безпеки про загрози, що потрапили в мережу.
- Пристрої захисту електронної пошти, які можуть блокувати та виявляти такі загрози, як електронна пошта та шкідливе програмне забезпечення.
- Пристрої уніфікованого управління загрозами (UTM), які можуть працювати з різними функціями, включаючи антивірус, виявлення та запобігання вторгненню, фільтрацію вмісту тощо. За допомогою пристроїв UTM організації можуть поєднувати кілька можливостей захисту від одного постачальника та керувати ними за допомогою однієї консолі.

Програмне забезпечення

Програмне забезпечення та програми захисту, такі як розширене програмне забезпечення для захисту від шкідливого програмного забезпечення або програми захисту електронної пошти, можна встановлювати на пристрої та вузли в мережі. На додаток до захисту мереж, програмне забезпечення та програми безпеки можуть допомогти організаціям захистити сервери, ноутбуки та мобільні пристрої від несанкціонованого доступу та інших загроз.

Традиційні програми, що проводять пошук, виявлення та видалення вірусів та шкідливого програмного забезпечення, таких як хробаки та троянські програми, стали неефективними. Прогресивне програмне забезпечення для захисту від шкідливих програм стало новим стандартом.

Розширений захист від шкідливих програм - це рішення безпеки, яке вирішує весь життєвий цикл розширеної проблеми зловмисного програмного забезпечення. Він запобігає порушенням і забезпечує видимість, контекст і контроль, необхідні для швидкого виявлення, утримання та усунення загроз, якщо вони ухиляються від фронтової оборони.

Програмне забезпечення мережевої безпеки допомагає компаніям виявляти та зупиняти несанкціонований доступ до мережі через фішинг, шпигунське програмне забезпечення тощо. Це також може допомогти захистити дані під час транспортування та відпочинку. Рішення мережевої безпеки включають:

Управління ідентифікацією та доступом (УІД). IT-адміністратори використовують рішення УІД для безпечного та ефективного управління цифровими посвідченнями користувачів та відповідними привілеями доступу. Вони можуть встановлювати та змінювати ролі користувачів, відстежувати та звітувати про діяльність користувачів тощо, щоб захистити безпеку даних та конфіденційність.

IPS наступного покоління (NGIPS). Пристрої загроз NGIPS забезпечують видимість мережі, інформацію про безпеку, автоматизацію та вдосконалений захист від загроз. Вони можуть перевіряти периметр мережі та відстежувати розвиток підозрілих файлів та шкідливих програм у мережі, щоб запобігти поширенню спалахів та повторному зараженню.

Інформація про безпеку та управління подіями (SIEM). Багато організацій використовують продукти SIEM для звітності в реальному часі та довгострокового аналізу подій безпеки. Ці продукти включають фізичні та віртуальні прилади та серверне програмне забезпечення. Вони полегшують

завдання збору, співвіднесення та дії з інформацією про загрози для команд безпеки.

Аналітика мережевої безпеки. Розширені рішення аналітики мережевої безпеки пропонують організаціям всебічну видимість загроз у розширеній мережі. Вони можуть спростити сегментацію мережі за допомогою поведінкового моделювання, машинного навчання та глобальної інформації про загрози.

3.2.1 Засоби криптографії

Засоби криптографічного захисту інформації (ЗКЗІ) - спеціальні пристрої, служби або програми, що забезпечують шифрування (кодування) і розшифрування (декодування) інформації з метою її захисту від несанкціонованого обробки, доступу і зберігання при обміні нею по каналах зв'язку, а також відповідають за генерацію електронного підпису (ЕП)(Рис 3.1).

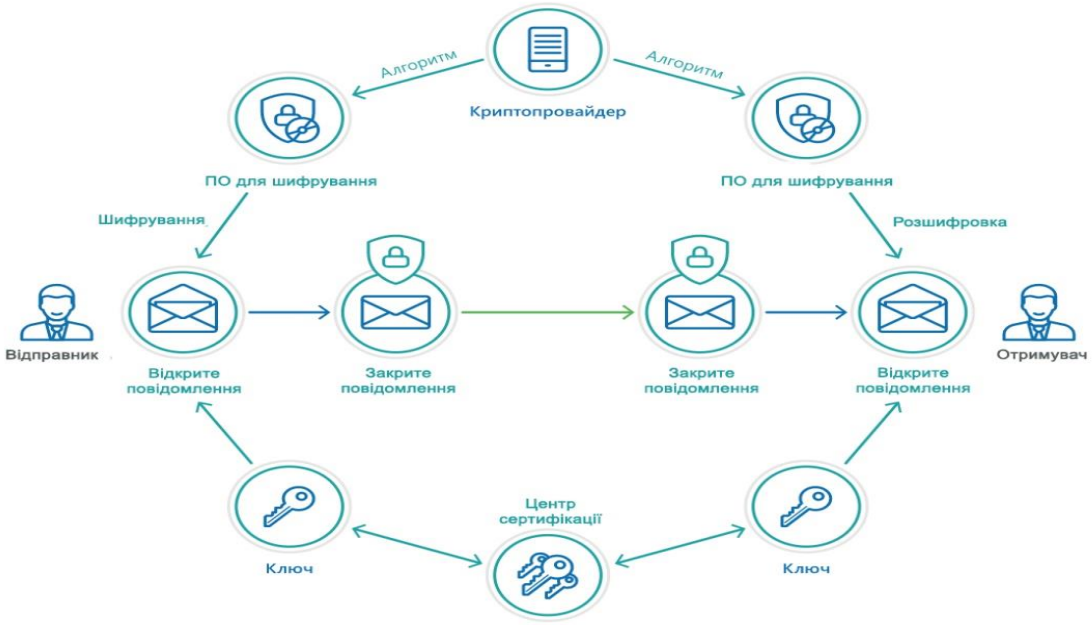


Рис. 3.1 - Схема використання ЗКЗІ

При шифруванні кожен символ документа, переданого по каналу зв'язку, підлягає кодуванню, а сама інформація, яку необхідно захистити, підрозділяється на окремі блоки, кожен з яких замінюється кодом: буквеним, цифровим або комбінованим. Також широко використовуються такі методи шифрування, як перестановка, заміна, аналітичне перетворення і гамування. Суть роботи ЗКЗІ полягає в тому, що створений користувачем інформаційний документ з'єднується з файлом електронного підпису, для чого застосовується власний закритий ключ цифрового підпису. Одержувач розшифровує отриманий файл за допомогою СКЗИ і власного ключа цифрового підпису. Далі одержувач переконується в тому, що в отриманий файл не вносилися правки і що електронний підпис ціла.

Існує два види ЗКЗІ. Одні вбудовуються в носій, інші встановлюються окремо. Засоби криптографічного захисту інформації, які вбудовуються в носій, являють собою засоби кодування, «вшиті» в систему і запрограмовані на самостійну роботу.

До таких ЗКЗІ відносяться «КріптоПро CSP» (Cryptographic Service Provider), «КріптоПро JCP» (Java Cryptography Architecture), LISSI-CSP (Лисси-CSP), VipNet CSP.

Методи, що застосовуються в ЗКЗІ:

1) Авторизація даних і безпечне збереження, їх юридична значимость при передачі або зберіганні. Для цього застосовують алгоритми створення електронного підпису і її перевірки відповідно до встановленого регламентом RFC 4357, що використовує сертифікати за стандартом X.509.

2) Захист конфіденційності даних і контроль їх цілісності. Використовується асиметричне шифрування та імітозахист, тобто протидія підміні даних. Дотримується ГОСТ Р 34.12-2015.

3) Захист системного і прикладного програмного забезпечення. Відстеження несанкціонованих змін або невірного функціонування.

4) Управління найбільш важливими елементами системи в суворій відповідності з прийнятим регламентом.

5) Аутентифікація сторін, що обмінюються даними.

6) Захист з'єднання з використанням протоколу TLS.

7) Захист IP-з'єднань за допомогою протоколів IKE, ESP, AH.

Засоби, що використовуються для криптографічного захисту інформації, класифікуються в залежності від можливої небезпеки, оцінки ймовірного способу злому системи. Вони залежать від наявності недокументованих можливостей або невідповідності заявленим характеристикам, які можуть містити:

- системне ПО;
- прикладне ПО;
- інші недоліки носія інформації.

Фактично криптохист систем також поділяють на:

1) Апаратний криптозахист

Засоби апаратного криптографічного захисту - фізичні прилади, пов'язані з системою передачі даних, що забезпечують шифрування, запис, передачу відомостей. Вони можуть являти собою персональні пристрої або виглядати як:

- смарт-карт;
- зчитувачів для ПК;
- USB-шифраторів, флеш-дисків.

Використовуючи ці пристрої можна побудувати ідеально захищені комп'ютерні мережі.

Засоби апаратної криптозахисту легко встановлюються і мають високу швидкість відгуку. Інформація, необхідна для забезпечення високого рівня криптографічного захисту, розміщується в пам'яті пристрою. Вона може бути зчитана контактним або безконтактним способом.

2) Програмний криптозахист

Система програмного криптозахисту представлена комплексом рішень, призначених для шифрування повідомлень, розміщених на різних носіях інформації. Такими носіями інформації можуть бути карти пам'яті, флешки або жорсткі диски. Найпростіші з них можна знайти у відкритому доступі.

До програмного криптозахисту можна віднести віртуальні мережі, призначені для обміну повідомленнями, які працюють «поверх Інтернету», наприклад, VPN, розширення, мають протокол HTTP, що підтримують розширення для шифрування HTTPS, SSL.

3.2.2 Засоби ідентифікації і автентифікації

Автентифікація - це процес, в ході якого на підставі пароля, ключа або будь-якої іншої інформації, користувач підтверджує, що є саме тим, за кого себе видає.

Ідентифікація - це процес, в ході якого з'ясовуються права доступу, привілеї, властивості і характеристики користувача на підставі його імені, логіна або будь-якої іншої інформації про нього.

Як синонім слова "автентифікація" іноді використовують словосполучення "перевірка справжності".

Існує три основних види автентифікації - статична, стала і постійна.

Статична автентифікація використовує паролі і інші технології, які можуть бути скомпрометовані за допомогою повтору цієї інформації атакуючим фактором. Часто ці паролі називаються повторно використовуваними паролями. Стійка автентифікація використовує криптографію або інші способи для створення одноразових паролів, які використовуються при проведенні сеансів роботи. Цей спосіб може бути скомпрометований за допомогою вставки повідомлень атакуючим в конкретне з'єднання. Постійна автентифікація оберігає від вставки повідомлень атакуючим.

Функція ідентифікації полягає у нанесенні відомої величини на невідому сутність, щоб зробити її відомою. Відома величина називається ідентифікатором або ідентифікатором, а невідома сутність - це те, що потребує ідентифікації. Основною вимогою до ідентифікації є унікальний ідентифікатор; Ідентифікатори унікальні лише в певному обсязі. Після ідентифікації особи за допомогою ідентифікатора користувача або подібного значення вона повинна бути автентифікована, це означає, що вона або вона повинна підтвердити свою особу.

Існує три загальних фактори, які можуть бути використані для автентифікації, які спостерігаються нижче:

1. Щось, що людина знає: Щось, що людина знає, може бути паролем, PIN-кодом, дівочим прізвищем матері або поєднанням із замком. Автентифікація людини за допомогою чогось, що, як вона знає, зазвичай є найменш витратним для реалізації. Недоліком цього методу є те, що інша особа може отримати ці знання та отримати несанкціонований доступ до системи чи об'єкта.

2. Щось, чим вона володіє: Те, що у людини може бути ключем, карткою, що проводить пальцем, карткою доступу чи значком. Цей метод є загальним для доступу до об'єктів, але його також можна використовувати для доступу до чутливих областей або для автентифікації систем. Недоліком цього методу є те, що предмет можна загубити або викрасти, що може призвести до несанкціонованого доступу.

3. Те, ким є людина: Щось специфічне для людини ґрунтується на фізичному атрибуті. Автентифікація особи на основі унікального фізичного атрибута називається біометрією.

Двох факторна автентифікація та біометрія - це одні з найкращих методів автентифікації. На відміну від імені користувача та ідентифікатора, якими можна зловживати, ці типи надійної автентифікації корисні для високого рівня безпеки. Двох факторна автентифікація передбачає використання відомостей, відомих

користувачеві, таких як ідентифікатор користувача та пароль, а також щодо того, що є у користувача, наприклад, смарт-картки або маркера. Біометрія перевіряє особистість особи, аналізуючи унікальний особистий атрибут чи поведінку, що є одним з найбільш ефективних та точних методів перевірки ідентифікації.

3.2.3 Засоби управління доступом

Система контролю доступу - це комплекс, що складається з ПО і ряду технічних засобів: контролерів, замків, зчитувачів, кнопок виходу, іноді - турнікетів і шлагбаумів, фіксаторів двері, гнучких проводів. Для ідентифікації відвідувачів використовуються індивідуальні картки, браслети або брелоки.

Ефективність СКУД повною мірою може проявлятися при інтеграції цієї системи з іншими засобами захисту від несанкціонованого проникнення. Інтегровані системи безпеки (ІСБ) в даний час широко впроваджуються і визнані найбільш перспективним напрямком забезпечення безпеки об'єктів.

Ідентифікація та автентифікація в СКУД можуть проводитися за такими основними принципами.

Ідентифікація по коду - здійснюється за кодом (паролем), який повинен запам'ятати людина (користувач) і який вводиться вручну за допомогою клавіатури, кодових перемикачів або інших подібних пристроїв.

В даний час ідентифікація по запам’ятовуваному коду застосовується в простих автономних пристроях доступу або в якості додаткового рівня в СКУД з багаторівневою ідентифікацією. код може встановлюватися самим користувачем і довільно їм змінюватися і бути невідомим оператору системи (при відповідному побудові програмного забезпечення СКУД).

Ідентифікація по матеріальному коду виконується по коду, записаного на фізичному носії (ідентифікатор), в якості якого застосовуються різні електронні ключі, пластикові карти, брелоки і т.д. Даний принцип отримав в даний час найбільшого поширення.

Правильна організаційна побудова структури СКУД, облік взаємодії технічних засобів у складі ІСБ, а також їх раціональне використання може забезпечити високу ефективність і надійність захисту об'єкта від несанкціонованих проникнень. При цьому треба мати на увазі, що вибір складних (а найчастіше "модних", широко рекламованих і відповідно дорогих) рішень може виявитися неефективним.

3.2.4 Протоколювання і аудит

Протоколювання - це фіксування інформації про події, що відбуваються в інформаційній системі, а аудит - це подальший аналіз зафіксованої інформації з метою розслідування інцидентів інформаційної безпеки та підвищення захищеності інформаційної системи. Саме на цих двох діях і засновано дія сервісів безпеки, протоколювання і аудиту. При протоколюванні, в інтересах забезпечення безпеки інформації фіксується інформація не про всі події, а тільки про події, що стосуються безпеки інформації.

Це мінімальний набір подій, що відносяться до питань безпеки:

- вхід і вихід суб'єктів доступу, тобто початок і завершення сеансів роботи і доступу;
- запуск і завершення програм;
- друк документів;
- спроба доступу до ресурсів, що знаходяться під захистом;
- зміна повноважень суб'єктів доступу.

Більшість з цих подій пов'язані з діями суб'єктів в системі і до їх можливого доступу до конфіденційної інформації, а друк документів є одним із способів реалізації витоку інформації. Якщо документ не можна жодним чином скопіювати на носій, відправити електронною поштою, зробити скріншот, то існує ще одна можливість його надрукувати. Тому при роботі з конфіденційною інформацією, тим більше з інформацією, що становить якусь територію, що

охороняється законом таємницю, вкрай рекомендується всі дії, пов'язані з друком документів, як мінімум протоколювати, а ще краще вести спеціальні журнали реєстрації, в яких відзначати факти друку документів, вказуючи, хто надрукував, навіщо і в скількох примірниках.

При протоколюванні подій рекомендується записувати такі їх параметри в журнали реєстрації:

1) дату і час події – це дозволяє в подальшому відновити хронологію подій;

2) ідентифікатор суб'єкта, що ініціював подію, для того щоб в подальшому визначати, хто із суб'єктів відповідальний за ту чи іншу подію;

3) тип події, а також його результат - успіх або невдача, тобто те, що дозволить визначити, здійснилося чи щось в системі щось неприпустиме, і якщо так, то що конкретно;

4) джерело запиту, тобто, наприклад, який конкретний вузол мережі з'явився джерелом запиту;

5) імена порушених об'єктів та опис змін, внесених до баз даних засобів захисту інформації.

Це, власне, те, що дозволяє визначати, які саме зміни були проведені внаслідок тієї чи іншої події в інформаційній системі, і таким чином оцінити, чи несуть вони ту чи іншу загрозу для інформаційної системи, чи є вони частиною реалізації якогось шкідливого впливу.

3.2.5 Хмарні сховища

Настав час цифровізації і віртуалізації. Це означає, що від устаткування відбувається перехід до функцій. Коли ми використовуємо послугу каршерінга, це означає, що замість власної «апаратної» машини ми, фактично, використовуємо її функцію - «їхати». При цьому, звичайно, ми сідаємо в реальну

машину з брендом компанії каршерінга на кузові, але після використання ми відправляємо її назад в «хмару»(рис 3.2).

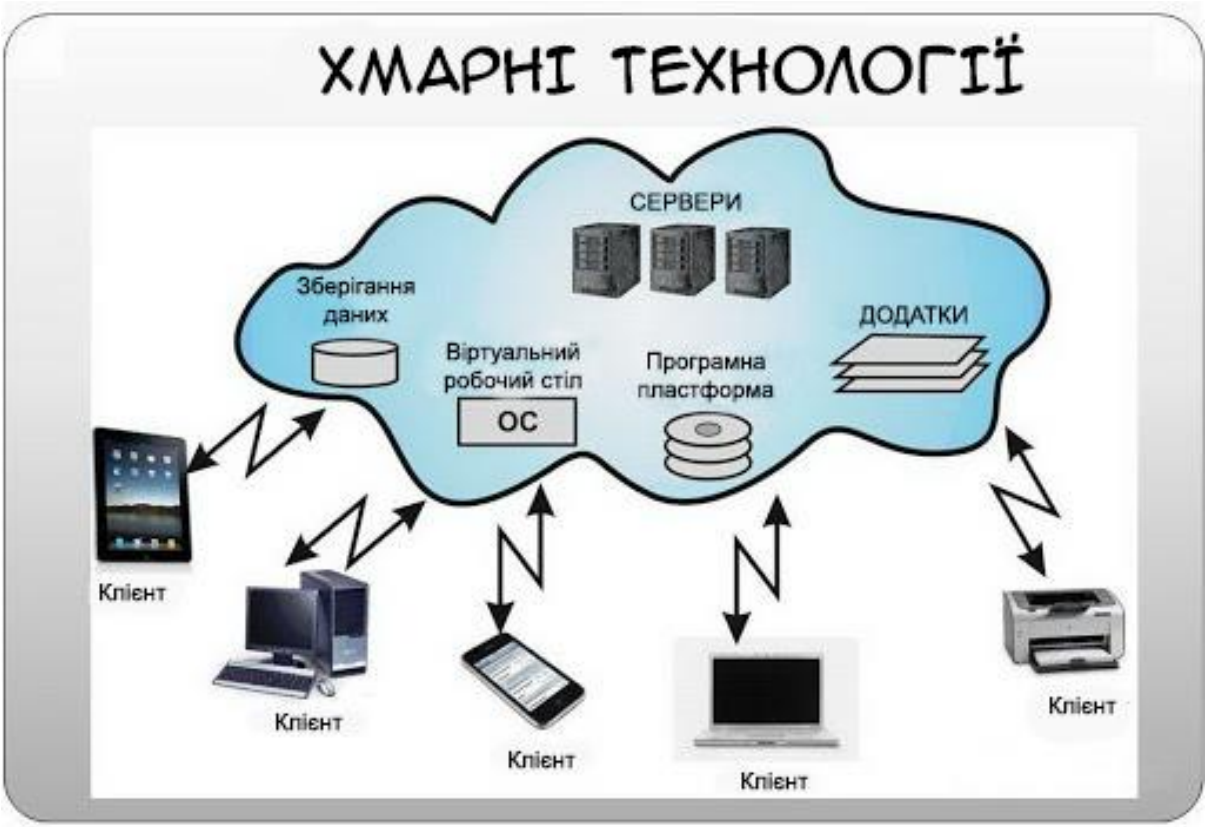


Рисунок 3.2 - Структура хмарних сервісів крупним планом

Досить цікава аналогія з хмарним сховищем - це віртуалізація вашої власної системи зберігання . В хмарі ваші дані також зберігаються на якомусь обладнанні.

Незалежно від типу хмарної системи зберігання: внутрішньої (приватної, private) або зовнішньої (public, публічної) - принцип їх роботи наступний. Провайдер хмарних послуг, або просто «хмари», надає свою IT-інфраструктуру, яка забезпечує надійне і безпечне управління потрібними серверами для зберігання даних [13].

Розрізняють публічнну та приватну хмару.

Публічне хмара - це віртуалізована система зберігання, послуги якої надає зовнішній провайдер. У його дата-центрі зберігаються дані багатьох клієнтів, на

умовах «Багатоарендності» (multi-tenancy), без взаємного впливу один на одного. За рахунок оптимального і централізованого використання ресурсів вдається досягти цінової ефективності.

Приватна хмара: віртуалізована система зберігання, організована в масштабах підприємства. У ній є виділений дата-центр (ЦОД), в віртуалізованій інфраструктурі якого зберігаються дані і працюють додатки підприємства. У цьому випадку, роль провайдера хмарних послуг найчастіше виконує IT-служба підприємства.

Сервери приватного або публічного хмари працюють не як незалежні системи всередині структури хмарного сховища, а як єдина група серверів. Для цієї мети дисковий простір разом з іншими компонентами сервера (наприклад, CPU або оперативною пам'яттю) віртуалізується з використанням гіпервізора. Поверх гіпервизора працюють вже не фізичні сервери, CPU і накопичувачі даних, а віртуальні сервери. А в них - віртуальні машини VM (Virtual Machine), які з точки зору функціоналу аналогічні фізичним пристроям. Можна сказати, що вони мають дивовижну властивість - адаптуватися під конкретні вимоги, можуть швидко мігрувати між фізичними серверами і навіть дата-центрами.

При цьому між реальним обладнанням і віртуальними функціями зберігання (Virtual Storage) виникає якийсь рівень абстрагування, на якому працює монітор віртуальних машин VMM (Virtual Machine Monitor), який ще називають гіпервізором (Hypervisor).

Для доступу до віртуального сховища в хмарі зазвичай потрібне відповідне програмне забезпечення. Послуги публічної хмари зазвичай містять не тільки НА веб-додатоках, яким можна користуватися через звичайний браузер, але також через драйвери доступу від різних пристроїв. З їх допомогою можна залогуватися і отримати доступ до свого диску в хмарі. Збережені там файли можна витягти через різні пристрої (комп’ютер, планшет, смартфон та ін.).

Для приватного хмарного сховища зазвичай потрібно з’єднання з сервером VPN через відповідну корпоративну мережу (інтернет), або за допомогою

послуги віртуальної приватної мережі VPN (Virtual Private Network) через публічний Інтернет. Останнім часом зявилася можливість використання для цієї мети технології SD-WAN (що програмно-конфігурується для глобальної мережі), але поки ця технологія ще не досягла стадії зрілості.

Хмарні провайдери, у своїй внутрішній інфраструктурі зберігання, крім звичайного файлового сховища (File Storage), можуть використовувати альтернативні види форматів: блочне сховище (Block Storage) і об'єктне сховище (Object Storage).

Переваги хмарного сховища

А) Перш за все, це економія коштів на придбання і обслуговування власного серверного обладнання для зберігання. Існує поширена думка, що хмарні послуги нітрохи не дешевше - або навіть дорожче, ніж власні системи зберігання.

Б) Гнучкість . Це можливість споживати рівно такий обсяг сховища, яке необхідне в даний момент. Якщо потрібно більше, провайдер надає більше - і плата зростає. Якщо потрібно менше, провайдер надає менше, а плата знижується. У своїй же системі необхідно завжди мати максимальну місткість на випадок сплесків трафіку. У звичайному режимі надлишкова ємність простоює. Якщо ємність знаходиться у стадіїї «під зав'язку», це негативно позначається на швидкодії роботи і системи. В хмарі цих проблем немає.

В) Масштабування. Віртуалізація сховища дозволяє вибирати необхідний обсяг сховища за контрактом. У будь-який час можна збільшити або зменшити обсяг сховища без закупівлі обладнання, його встановлення та налагодження.

Г) Доступність: хмарне сховище доступно в будь-який час і з будь-якого пристрою (при наявності нормального Інтернету). Тому отримувати дані можна де завгодно.

Недоліки хмарного сховища

Хмарне сховище в багатьох випадках може стати хорошою альтернативою традиційним рішенням по зберіганню в корпоративній системі (рис. 3.3).

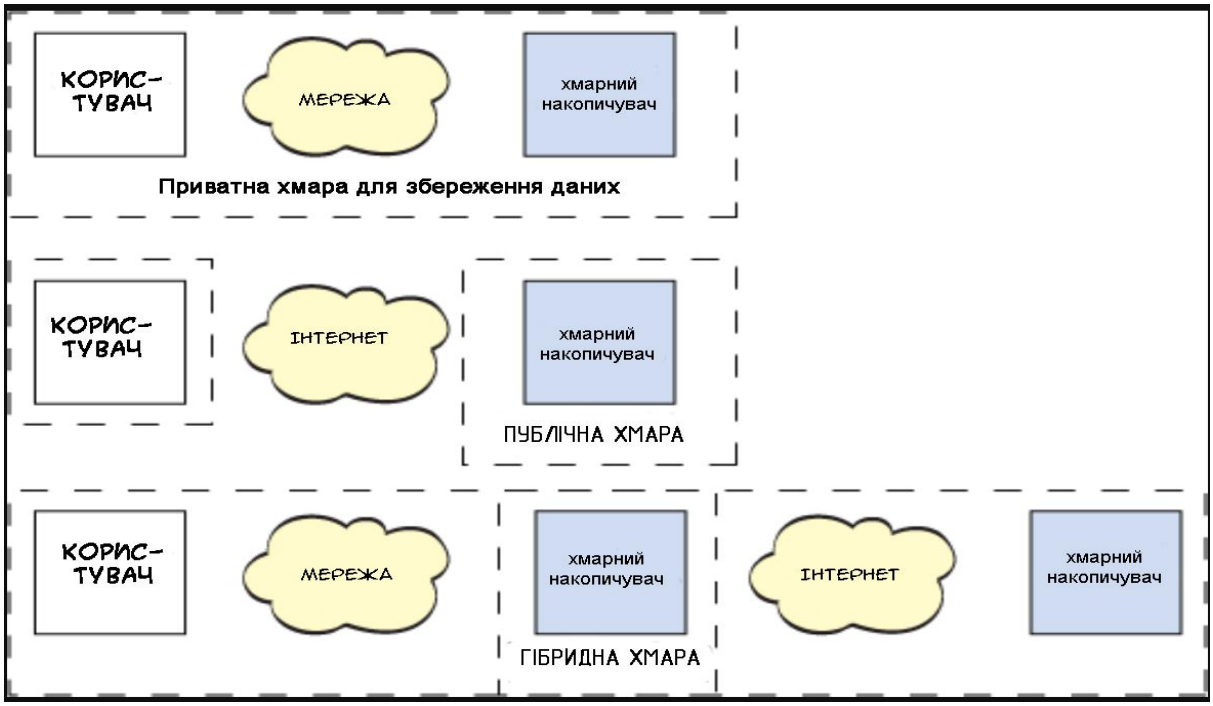


Рисунок 3.3 - Анатомія хмарної структури зберігання даних

Однак, у багатьох випадках резервування файлів в хмарі має деякі мінуси.

Перш за все, це залежність від Інтернет-з'єднання. Якщо воно порушується, файли в хмарі стають недоступними. Важливим фактором залишається доступна смуга пропускання: навіть при самому швидкодіючому сховище доступ до даних буде повільним через низьку швидкості з'єднання. Особливо це стосується мобільних мереж.

Залежність від провайдера . Якщо у провайдера відбуваються якісь проблеми, або він «по-свинськи» змінює умови контракту, замовник може поміняти провайдера, але це процес не швидкий.

Безпека . Пересилання даних за брандмауер корпоративної мережі - це завжди ризик. Не всі провайдери надають послугу шифрування даних, що зберігаються. Незважаючи на те, що хороші провайдери завжди намагаються забезпечити вищий рівень безпеки своїх систем, інфраструктура провайдера - бажана мета для атак хакерів.

Захист даних . Як дані будуть захищені в інфраструктурі провайдера - основне питання, яке необхідно з'ясувати при укладенні контракту на хмарне

зберігання даних. Це можна назвати «палицею з двома кінцями», схожа на вічний спір про те, де краще зберігати гроші - в банку або будинку у сейфі. І там, і там їх можуть вкрасти. Однак не підлягає сумніву, що, в цілому, банк може забезпечити більш високий ступінь захисту коштів своїх вкладників. Однак, на відміну від грошової аналогії, компрометація інформації, що зберігається у провайдера може створити непоправної шкоди для клієнта хмарної послуги.

Компромісом можна вважати гібридну хмару

При виборі між приватною і публічною хмарою, завжди потрібно робити ретельний аналіз ТСО. Витрати обладнання, ліцензії на ПЗ, на оплату праці IT-фахівців та ін. - це т. Зв. «Прямі» або «бюджетні» витрати.

Гібридна хмара, як це видно із самої назви, об'єднує в собі плюси публічного хмари (Public Cloud) і приватного хмари (Private Cloud).

Таким чином, рішення гібридного хмари поєднує в собі переваги як приватного, так і публічного хмари, і може забезпечити такі переваги, як:

більш високу ступінь керованості;

хорошу «пристосованість до змін», тобто можливість конфігурувати оптимальне рішення;

економічну ефективність.

3.3 Рекомендації для встановлення камер відеоспостереження

Система відеоспостереження - це комплекс обладнання та програмного забезпечення, призначений для спостереження за територією, діями і ситуацією, тощо.

Для цього використовують відеокамери – пристрій який записує відеоінформацію.

Для задачі відеоспостереження найчастіше використовують декілька видів камер:

1) Аналогові камери безпеки

Переваги:

Вартість: Аналогові камери, як правило, коштують дешевше, іноді навіть набагато дешевше, ніж їх цифрові аналоги для кожної камери.

Простота: відеореєстратор для більшості легше налаштувати та зрозуміти. Це одна одиниця з однією вартістю, а установка дещо простіша.

Нижчі вимоги до пропускної здатності: Відеофайли, записані в аналоговому режимі, як правило, менші, і вони передаються на відеореєстратор через коаксиальну замість локальної мережі, тому їх передача не займає стільки пропускної здатності. Крім того, відеореєстратори також зазвичай передають інформацію та використовують пропускну здатність лише тоді, коли хтось переглядає відео, а не постійно.

Більше варіантів дизайну: Завдяки широкому розмаїттю конструкцій аналогових камер вам може бути легше знайти модель камери з усіма необхідними функціями за нижчою вартістю.

Недоліки:

Підключення кабелів: Оскільки камери потрібно підключати як до джерела живлення, так і до відеореєстратора за допомогою кабелів, у вас, як правило, багато проводки, навіть якщо ви використовуєте кабелі, що поєднують відео та живлення. Крім того, коаксіальні кабелі зазвичай дорожчі самі по собі, ніж аналоги Cat 5 або 6, що використовуються для цифрових систем.

Якість зображення: Якість зображення на аналогових камерах досить низька. Більшість смартфонів сьогодні мають більш високу роздільну здатність. Як результат, деталі на відстані можуть бути зернистими, що ускладнює ідентифікацію потенційних підозрюваних у інциденті з високим ступенем впевненості. Більше того, немає цифрового масштабування. Якщо ви спробуєте збільшити щось на аналоговому відео, швидше за все, ви отримаєте ще більш розмите та зернисте зображення.

Площа покриття: Як правило, аналогові камери спостереження мають значно вужче поле зору, ніж їх цифрові аналоги, тому вам може знадобитися більше з них, щоб покрити потрібну вам область.

Обмеження розташування: Оскільки аналогові камери потрібно підключати до відеореєстратора, ви повинні тримати ці камери в межах розумного діапазону пристрою, інакше ви ризикуєте зменшити надійність з'єднання. Як результат, ви стаєте більш обмеженими, де можна розмістити свої камери.

Обмеження портів: У відеореєстраторів обмежена кількість портів, тому до них можна підключити лише обмежену кількість камер. Якщо ви хочете перевищити це число, вам, мабуть, доведеться придбати другий відеореєстратор.

Можливість бездротового зв'язку (або його відсутність): Реальність така, що аналогові бездротові системи працюють не дуже добре через державні норми щодо аналогових частот та потужності сигналу. Як результат, інші бездротові пристрої і навіть флуоресцентне освітлення можуть перешкоджати і спотворювати відеосигнал.

Шифрування: Аналогові сигнали не можуть бути зашифровані, як правило, кажучи, що означає, що небажаним очам може бути простіше переглянути сигнал.

2) Системи цифрових камер безпеки

Переваги:

Якість зображення: Якість зображення від цифрових камер безпеки значно вища, ніж аналогових, оскільки багато камер здатні записувати та передавати відео високої чіткості. Крім того, цифрові камери, швидше за все, мають функції цифрового масштабування, які можуть мати відстань масштабування більше 100 футів.

Область покриття: Одна цифрова камера може охоплювати область, яка потребує трьох або навіть чотирьох аналогових аналогів. Як результат, вам може знадобитися менше камер і ви зможете підтримувати нагляд за безпекою на більш широкій території.

Менше кабелів потрібно: Замість того, щоб окремо підключати кожну камеру живленням, а потім підключати кожну камеру до відеореєстратора, цифрові системи можуть мати кілька камер, підключених до комутатора, і тоді всі ці камери на комутаторі можуть бути підключені до NVR за допомогою одного кабель.

Обмеження розміщення або порту: Оскільки камери просто потрібно підключити до вашої мережі LAN, щоб підключитися до вашого NVR, ви більше не обмежені відстанню між камерами та відеореєстратором. Оскільки NVR заснований на програмному забезпеченні і не має портів, ви також усунете це обмеження.

Power over Ethernet (PoE): комутатори Power over Ethernet дозволяють вашим сигнальним кабелям подавати живлення і на камери, зменшуючи потребу в цих додаткових кабелях.

Бездротові можливості: Системи цифрових охоронних камер дуже добре працюють у бездротовій мережі. Вони не сприйнятливі до тих самих типів перешкод, які впливають на аналогові аналоги, тому за бажанням ви можете легко переглядати живу стрічку з більш віддалених місць.

Шифрування: Багато цифрових камер безпеки мають вбудоване шифрування, тому ваші дані безпечніші від початку подорожі до кінця.

Недоліки:

Ускладнення під час налаштування. Якщо у вас ще не налаштована мережа та не встановлені комутатори, це може збільшити вартість та робочу силу, пов’язану з установкою системи відеоспостереження, незалежно від того, що вам потрібно менше кабелів загалом.

Вища початкова вартість: Камери та обладнання (крім кабелів), як правило, коштують дорожче в індивідуальному порядку порівняно з аналоговими аналогами (хоча вам може знадобитися менше їх, тому витрати можуть збалансуватись).

Вимоги до високої пропускної здатності: Системи IP-камер безпеки зазвичай вимагають набагато більшої пропускної здатності, ніж аналогові.

Охоронне відеоспостереження

Основною функцією такого типу відеоспостереження - запис відеоінформації з камер в архів і надійне зберігання архіву протягом заданого проміжку часу. Інформація з архіву може бути використана для вирішення наступних завдань: розбір надзвичайних ситуації виникли на об'єкті, в тому числі крадіжка, розбійні напади; розбір спірних ситуацій, що виникають між співробітниками, відвідувачами та клієнтами. Іноді така інформація може служити доказовою базою в суді. На рис. 3.4 зображений принцип роботи охоронного відеоспостереження.

Рисунок 3.4 Принцип роботи охоронного відеоспостереження

Технологічне відеоспостереження

Системи технологічного відеоспостереження (ТБ) використовуються для моніторингу виробничих процесів і контролю якості роботи співробітників на промислових підприємствах і заводах.

За допомогою технологічних відеокамер можна організувати детальний і повний контроль робочого циклу підприємства. Подібні системи встановлюються на найбільш відповідальних ділянках виробничих конвеєрів.

Для виробничих підприємств встановлюються захищені камери, здатні працювати в несприятливих технологічних і метеоумовах, а також в складних температурних режимах.

Аналітичне відеоспотереження

Системи відеоспостереження вже давно «виросли» за рамки охоронних функцій. Можливості сучасних систем служать також для інтелектуального аналізу одержуваного відеопотоку.

За допомогою сучасних систем відеоаналітики можна істотно розширити можливості системи і скоротити задіяний персонал. Оператор відеоспостереження більше не повинен невідривно стежити за безліччю моніторів, процес виявлення порушень відбувається на основі обробки подій аналітичними програмами, а також сигналів від різних детекторів. Оператору надходить сигнал про можливе або вже скоєне порушення.

Системи відеоаналітики можуть:

1. Ідентифікувати особи розшукуваних злочинців.
2. Встановлювати факти крадіжок.
3. Розпізнавати неадекватна поведінка людей.
4. Класифікувати різні об'єкти (тварини, діти, транспорт) в зоні спостереження.

Наявність таких систем також забезпечує широкі можливості маркетингової аналітики. Наприклад, для торгових залів відкриваються можливості оцінки роботи продавців, для кращої організації розміщення товарів, підрахунок відвідувачів, боротьба з чергами та ін.

Вказівки щодо розміщення зовнішніх камер охорони

Встановіть камери на висоті 2,5-3 метри від землі. Ця висота досить низька, щоб захоплювати дрібні деталі, але досить висока, щоб бути недоступною для злодіїв та вандалів.

Не спрямовуйте камери прямо на сонце. Яскраве світло призводить до відблисків та високої контрастності на ваших кадрах, через що важко визначити, що відбувається. Враховуйте рух сонця та нахиляйте камери до непрямого світла.

Вирішіть, чи хочете ви, щоб камера була видимою чи прихованою. Видимі камери безпеки є ефективними засобами захисту від крадіжки, але вони також є об'єктами крадіжок та вандалізму. Деякі власники будинків вирішують на видному місці встановити підроблену камеру-приманку та підкріпити її справжньою, яка є трохи більш прихованою, тоді як інші додають надміцне обладнання або корпус навколо камери, щоб ускладнити пошкодження.

Захистіть камеру від стихій. Найкращі зовнішні камери охорони мають достатню погодо- та гідроізоляцію, але не всі вони створені однаково добрі. Виберіть камеру, яка відповідає вашому клімату, і поставте її під карниз або в інший напівзахищений район, якщо можете.

Вказівки щодо розміщення охорони в приміщенні

Куточки - ваші друзі. Вішання внутрішньої камери в кутку кімнати зазвичай дає вам найбільшу можливу точку зору.

Windows може спричинити проблеми з відображенням. Направлення камери у вікно може погіршити якість зображення. Багато охоронних камер мають інфрачервону (ІЧ) світлову технологію, яка допомагає виявляти рух і дозволяє камерам функціонувати в умовах недостатнього освітлення. ІЧ-світло може відбиватися від вікон та інших скляних предметів і затемнювати ваші кадри, особливо в темряві. Якщо ваші кадри виглядають вимитими або побіленими, ймовірно, проблема з відображенням триває.

Якщо необхідно спрямувати камеру у вікно, розташування об’єктива якомога ближче до скла та / або підсвічування зовнішньої території (можливо, за допомогою вогнів детектора руху) - це два заходи, що мінімізують відблиски. Також може бути корисно, якщо ваша камера має технологію широкого динамічного діапазону (WDR).

Кут для непрямого світла. Знову ж таки, пряме світло змиє ваші кадри. З внутрішніми камерами пам’ятайте про лампи, світильники та світлі вікна. Намагайтеся не спрямовувати камеру безпосередньо до будь-якого з цих джерел світла.

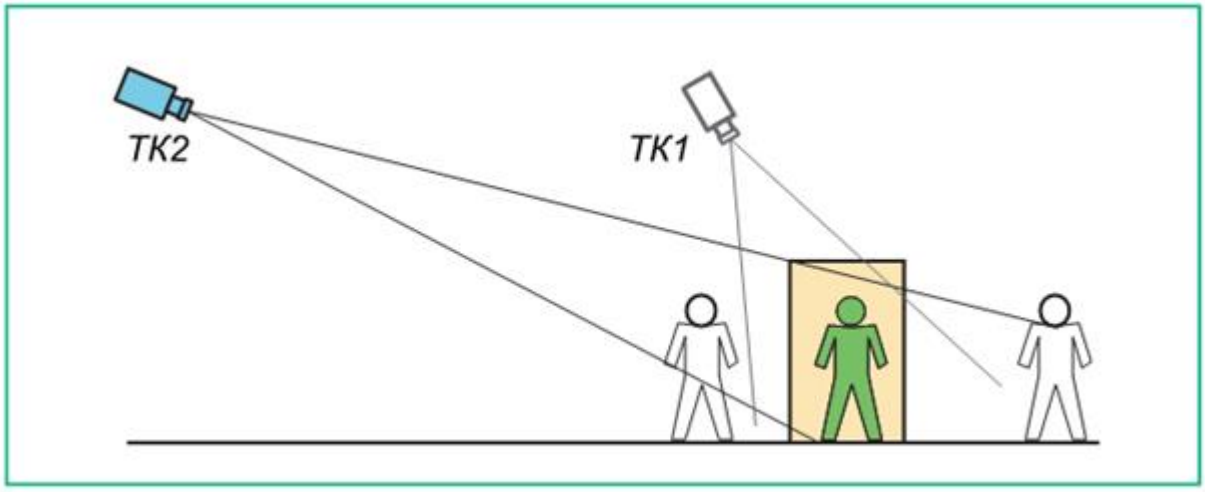


Рисунок 3.5 - Вигляд камери з вищого кута огляду камери і нижчого

Як і написно в рекомендаціях, найкраще положення камери - в кутку кімнати. На малюнку 3.5 приведений приклад положення камер, показано кут огляду камери. Як ми можемо побачити, камера 1 не може дати нам чіткого зображення обличчя людини, оскільки знімає вона лише зверху, а також кут її огляду не включає в себе якісь важливі об'єкти. Камера 2 дозволяє нам побачити набагато більше інформації.

Датчики руху

Датчики руху - важливі структурні елементи багатьох охоронних, сигналізаційних, а також систем освітлення [8]. Вони широко застосовуються в житлових і офісних приміщеннях з метою:

- фіксації переміщення фізичних об'єктів, що потрапляють в зону дії пристрою;
- розпізнавання несанкціонованого проникнення на приватну територію;
- автоматизації роботи кліматичної техніки;
- економії електроенергії (освітлення вмикається і вимикається при необхідності);
- підвищення якості роботи відеоспостереження;
- оптимізації роботи систем «Розумний будинок».

Розрізняють провідні та безпровідні датчики руху. Є моделі, призначені для застосування всередині будинку, а також різновиди, які розраховані на зовнішній монтаж (Рис 3.6).

Рисунок 3.6 Внутрішні(А) і зовнішні(Б) датчики руху

В основі роботи більшості детекторів лежить аналіз хвиль, що надходять ззовні. Розрізняють такі типи датчиків:

1. Ультразвукові
2. Інфрачервоні
3. Радіохвильові
4. Комбіновані (гібридні, змішані).

Ультразвукові датчики руху виконують сканування приміщення за допомогою ультразвукових хвиль. В основі роботи такого детектора лежить вбудований генератор, який виробляє високочастотні коливання (25-40 кГц). Такі звукові хвилі не сприймаються людським вухом.

Інфрачервоні детектори спрацьовують при зміні обстановки в тепловому (інфрачервоному) діапазоні випромінювання.

Радіохвильові детектори працюють за тим же принципом, що і ультразвукові, з тією відмінністю, що мікрочіп в них генерує хвилі з частотою 2,5 ГГц. Якщо в зону поширення хвилі потрапляє фізичний предмет, то змінюється її довжина і частота, що реєструється приймачем.

З точки зору конструкції, гібридний датчик руху являє собою прилад, в якому зібрані кілька пристроїв під загальним корпусом, кожен з яких підключається до різних виходів. По-іншому такі пристрої називають «датчиками подвійний технології». Гібридні моделі компенсують недоліки тих детекторів, з яких складаються.

Датчики температур – найбільш часто використовуваний тип датчиків для визначення температури в конкретному приміщенні

Датчиків температури існує безліч типів, кожен з яких характеризується своїми особливостями і призначенням. Але головним завданням залишається:

- Вимірювання температур необхідних об'єктів з необхідними точністю, швидкодією і передача інформаційного або керуючого сигналу далі в систему
- Реалізація зворотних зв'язків в АСУТП(Автоматична Система Управління Технологічним Процесом), попередження виходу з ладу обладнання

- Окремі прилади можуть служити джерелами енергії (засновані на термопарах)

Температурні датчики представлені широким розмаїттям приладів, кожен з яких адаптований до тій чи іншій сфері діяльності.

Види датчиків температур:

a. Термоопору. Первинний перетворювач. Засновані на зміні електричного опору матеріалів під впливом температури.

b. Термопари. Первинний перетворювач. Використовує ефект виникнення термо-ЕРС в залежності від різниці температур «холодного» і «гарячого» спаювання.

c. Перетворювачі температури і вологості (датчики температури повітря). Електронні прилади з аналоговими / цифровими виходами (+ дисплей), що поєднують в собі функції датчика вологості і температури. Краще застосування знаходять в системах вентиляції і кондиціонування, в приміщеннях різних типів.

d. Багатоточкові перетворювачі температур. Призначені для температурного контролю по всьому об'єму у великих резервуарах. Краще застосування знаходять в харчовій промисловості і с / х, де використовуються в силосах з зерном і подібним продуктом.

e. Безконтактні датчики температури. Використовуються з віддаленими / важкодоступними об'єктами в широкому діапазоні t ° C, в небезпечних для людини умовах. До них також відносяться:

- Датчики гарячого металу. Різновид безконтактних датчиків для відповідних галузей виробництва.
- Дистанційні датчики температури.
- Інфрачервоні датчики температури.
- Датчики температури з аналоговим виходом. Обширний клас приладів, що об'єднуються способом передачі інформації.

3.4 Охоронна сигналізація підприємства «Інфосервіс»

Охоронна сигналізація - це складний ланцюжок цифрових приладів і датчиків, що здатен швидко аналізувати і реагувати на певні подразники (світло, звук, рух). Коректна і професійна установка охоронної сигналізації в офісі, будинку, готелі, готелі забезпечує якісну систему безпеки, оперативного реагування порушень меж території.

Всі системи, що існують на ринку, діляться на дві великі категорії:

- автономна;
- з сигналом на пульт охорони.

Перший варіант краще купити в приватне житло (котедж, будинок, квартира). При виявленні небезпеки автоматично включаються звукові і світлові сигнали відлякування. При цьому інформація про незаконне проникнення нікуди не передається. У невеликі системи вбудована відправка повідомлення господареві, що може скасувати сигнали тривоги.

Але така недорога охоронна сигналізація має і недоліки:

1. Після отримання сигналу проходить занадто багато часу, поки господар викличе правоохоронні органи і вони приїдуть. Грабіжники можуть вже втекти.

2. Неможливо перевірити помилковий це сигнал чи ні. Особливо незручно, коли ви перебуваєте занадто далеко.

Що стосується другого типу, то він є більш комерційним. У магазини, офіси, підприємства, готелі сигналізації встановлюють з прив'язкою до приватних служб охорони. При спрацьовуванні датчиків тривоги на об'єкт виїжджає група спецсотрудніков швидкого реагування. Даний тип ефективно застосовується повсюдно. При визначенні помилкової тривоги - виклик скасовується.

Є і третій тип систем охоронної сигналізації – GSM. З'явилася вона на ринку не так давно, але вже придбала величезну популярність. Вона буває дротовою і бездротовою.

Переваги:

- Легкість в установці
- Широка зона дії
- Можливість віддаленого керування

Якщо говорити про недоліки, то при дуже низьких температурах може швидко розрядитися акумулятор у бездротових моделей. Також може бути дуже великий проміжок часу між спрацьовуванням і моментом реагування.

Охоронно-пожежна сигналізація - інтеграція систем для захисту вашого будинку

Крім охоронної, виділяють ще одне групу - система охоронно-пожежної сигналізації. Цей комплекс сучасних технічних засобів призначений для миттєвого оповіщення про пожежу в приміщенні і автоматичного гасіння джерела пожежі.

Об'єднання двох систем дозволяє максимально ефективно справлятися зі своїми завданнями, дає вагому перевагу при виникненні пожежі (з допомогою відеокамер оперативно виявити осередок загоряння і надалі розслідувати фактори виникнення пожежі).

Працювати вони можуть і окремо: периметральна охоронна сигналізація виявляє незаконне проникнення на територію, що охороняється, а пожежна - моніторинг периметра на виникнення загоряння.

3.5 Висновки

Після проведення аналізу програмного та апаратного захисту підприємства було визначенно, що наразі підприємство майже не захищене. Були запропоновані заходи для посилення безпеки такі як:

Встановлення камер відеонагляду, що є обов’язковим будь-якого підприємства, камери можуть бути як приховані, так і на видному місці, проте

саме камера на видному місці краще допоможе захистити приватну власність, оскільки злочинець буде знати, що це місце під наглядом

Встановлення датчиків руху на температури, оскільки не завжди є можливість найняти нічного охоронця, а часто немає такої потреби, датчики руху в цьому дуже допоможуть, як тільки буде зафіксовано рух, коли його бути не повинно, буде надіслано сигнал в службу охорони. Датчики температури вбережуть підприємство від раптових пожеж через погану проводку чи навіть підпалів.

Окрім цього необхідно використовувати ключі доступу, на вході потрібно встановити пристрій для перевірки доступу, наприклад двері з електронним ключем.

4 ПРОЕКТУВАННЯ СИСТЕМИ БЕЗПЕКИ ПІДПРИЄМСТВА «ІНФОСЕРВІС»

4.1 Проектування системи відеонагляду підприємства «Інфосервіс»

Встановлення системи відеонагляду розпочинається з розробки проекта системи, в якій визначаються місця для встановлення камер та зони їх огляду, виходячи з практичної необхідності. Після розробки схеми розміщення камер, розраховується необхідна кількість кабелю для передачі відеосигналу до місця встановлення відеореєстраторів та провода живлення до встановлюваного обладнання

Схема розміщення обладнання та камер системи відеонагляду

ВК – відеокамера

БЖ – блок живлення

ПД – панель домофону

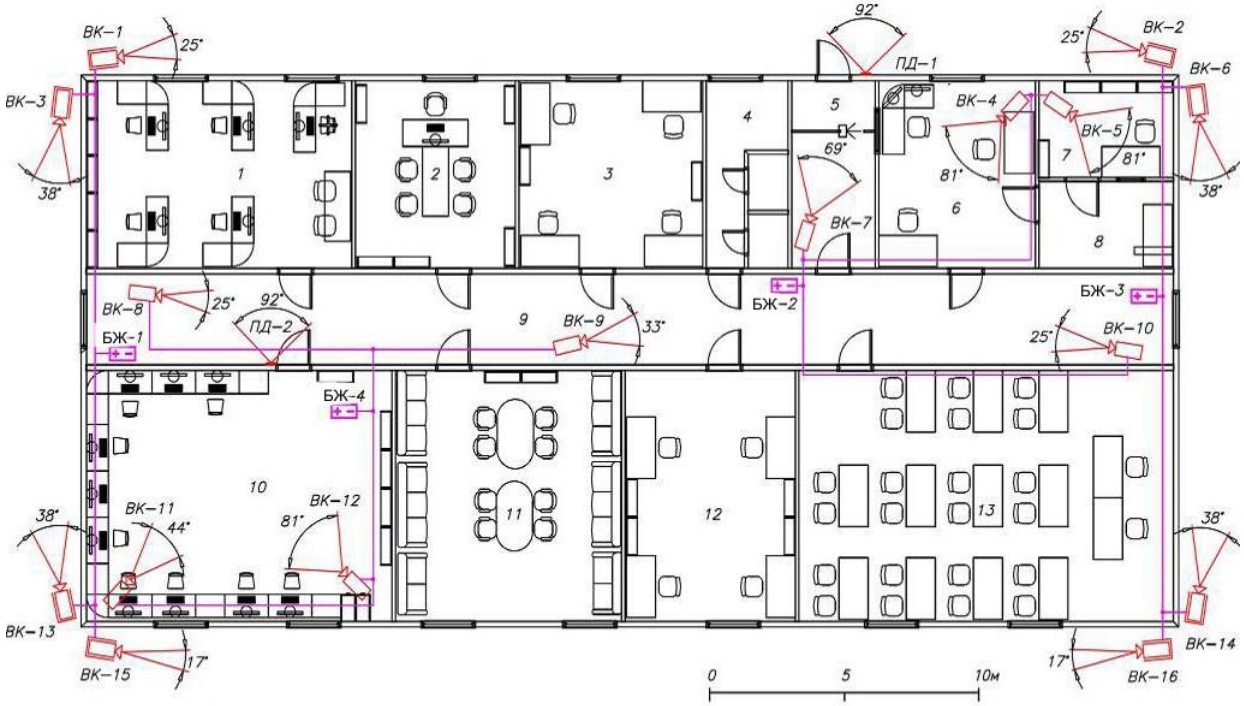


Рисунок 4.1 – План розтащування камер на підприємстві

4.2 Розрахунок кутів огляду відеокамер та їх розширення в ближній та дальній зоні спостереження

Розрахунок кутів огляду відеокамер та їх розширення зробимо за допомогою програми ViewDesigner. Ця програма відноситься до категорії безкоштовного програмного забезпечення і надана представництвом компанії “Dallmeier electronic”.

Звісно можливо використовувати і інші подібні програми, наприклад:

- програма CCTVLens. Доступна на сайті www.cctv-labs.ru/support/cctvlens/cctvl/;

- Web версія програми розрахунку зони огляду відеокамери компанії “ivtechno” на сайті https://www.ivtechno.ru/zona_obzora

- програма IP Video System Design Tool компанії JVSG (www.jvsg.com);

- програма VideoCAD (www.cctvcad.com) і т.д.

Це програмне забезпечення, як і безліч іншого такого, значно полегшує роботу проектувальників систем відеоспостереження. ViewDesigner дозволяє під правильним кутом і на правильній відстані розмістити камери на проектованому об'єкті, а так само підібрати об'єктив з правильною фокусною відстанню і відповідним кутом огляду. Програма дозволяє візуально визначити, що потрапить в поле зору відеокамери виходячи з висоти її установки, кута нахилу і технічних характеристик камери.

Розглянемо графічний інтерфейс програми ViewDesigner. У верхній частині робочого вікна програми виставляються такі параметри камери як розмір матриці камери (CCD-Chip) і фокусна відстань (focal length).

Рисунок 4.2 – Параметри камери в програмі ViewDesigner

Нижче знаходиться область настройки зони спостерігання з двома закладками - полем спостереження у вертикальній і горизонтальній площині. Сцена налаштовується п'ятьма повзунками, які дозволяють виставити такі параметри як висота установки камери і кут нахилу камери по вертикалі, відстань до віддаленого об'єкта, що спостерігається і зростання умовного людини в кадрі.

Праворуч ми бачимо що отримується з заданими настройками зображення. У кадрі присутні задані на схемі дві людини - один на кордоні необхідної дальності спостереження, другий на ближній межі кадру, що проходить по підлозі приміщення.

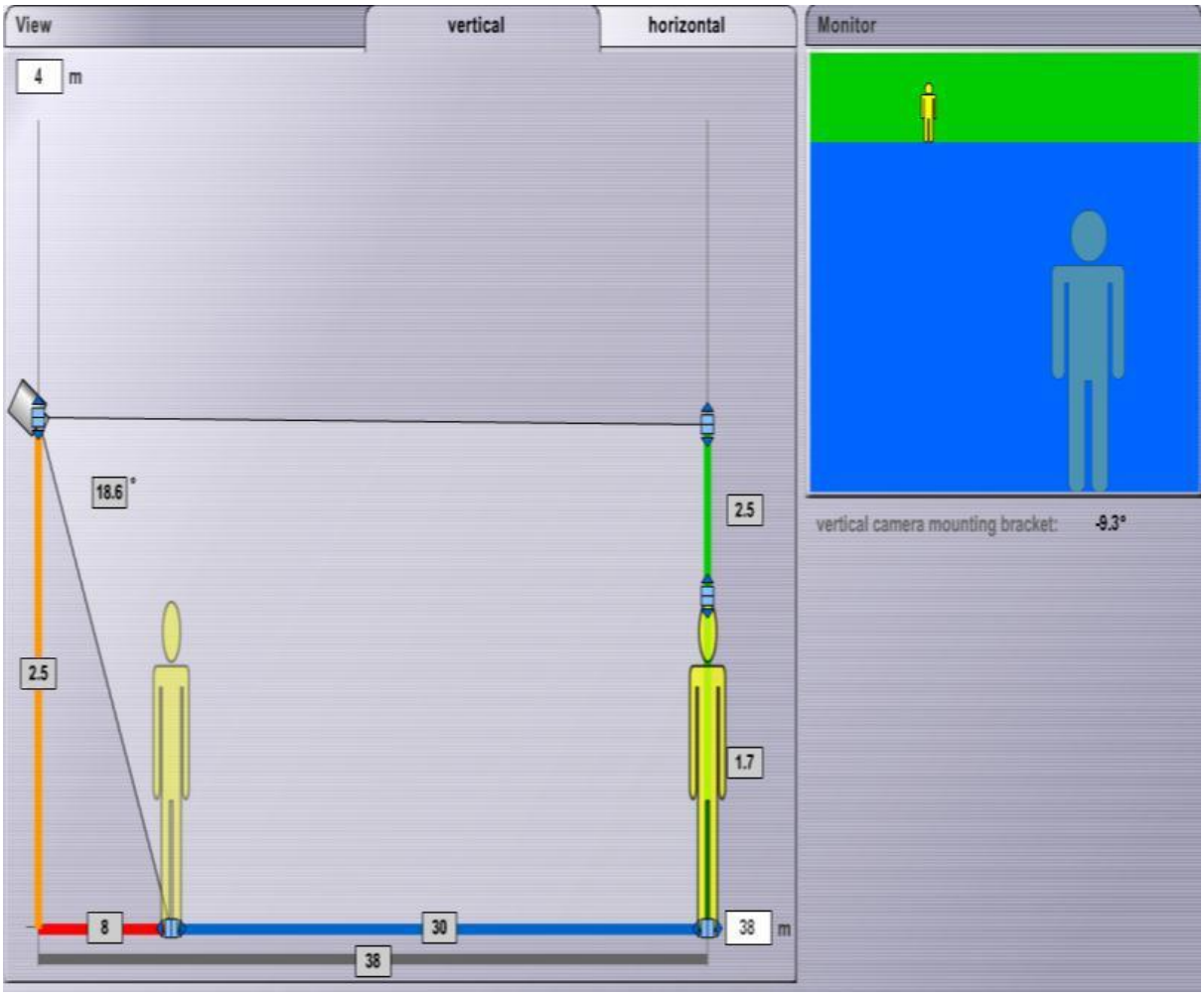


Рисунок 4.3 – Встановлення зони спостереження

У закладці horizontal відображається область огляду камери в горизонтальній площині. Слід врахувати, що матриці, застосовані в відеокамерах, мають прямокутну форму. Отже, кут огляду в горизонтальній площині буде ширше, ніж у вертикальній.

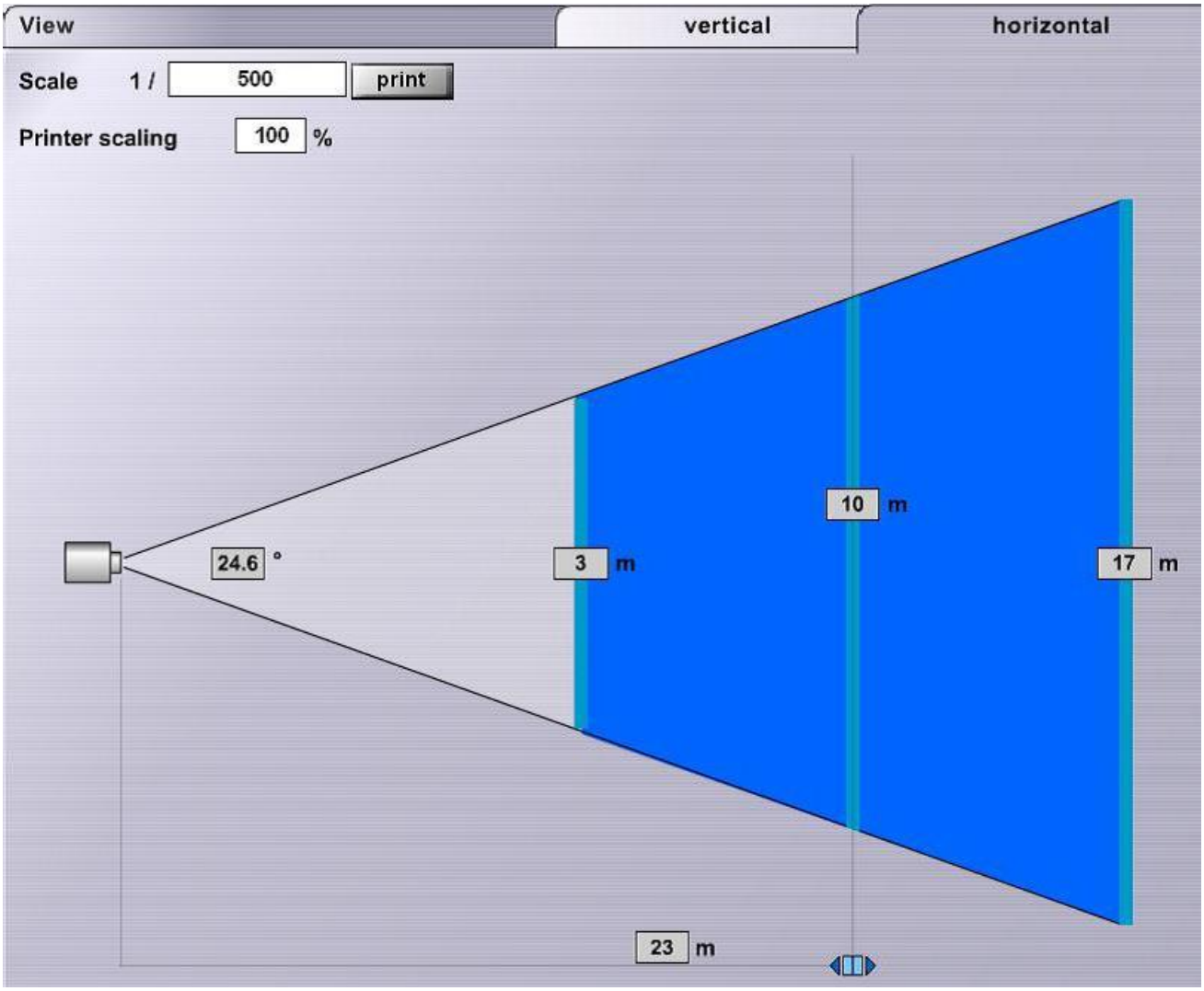
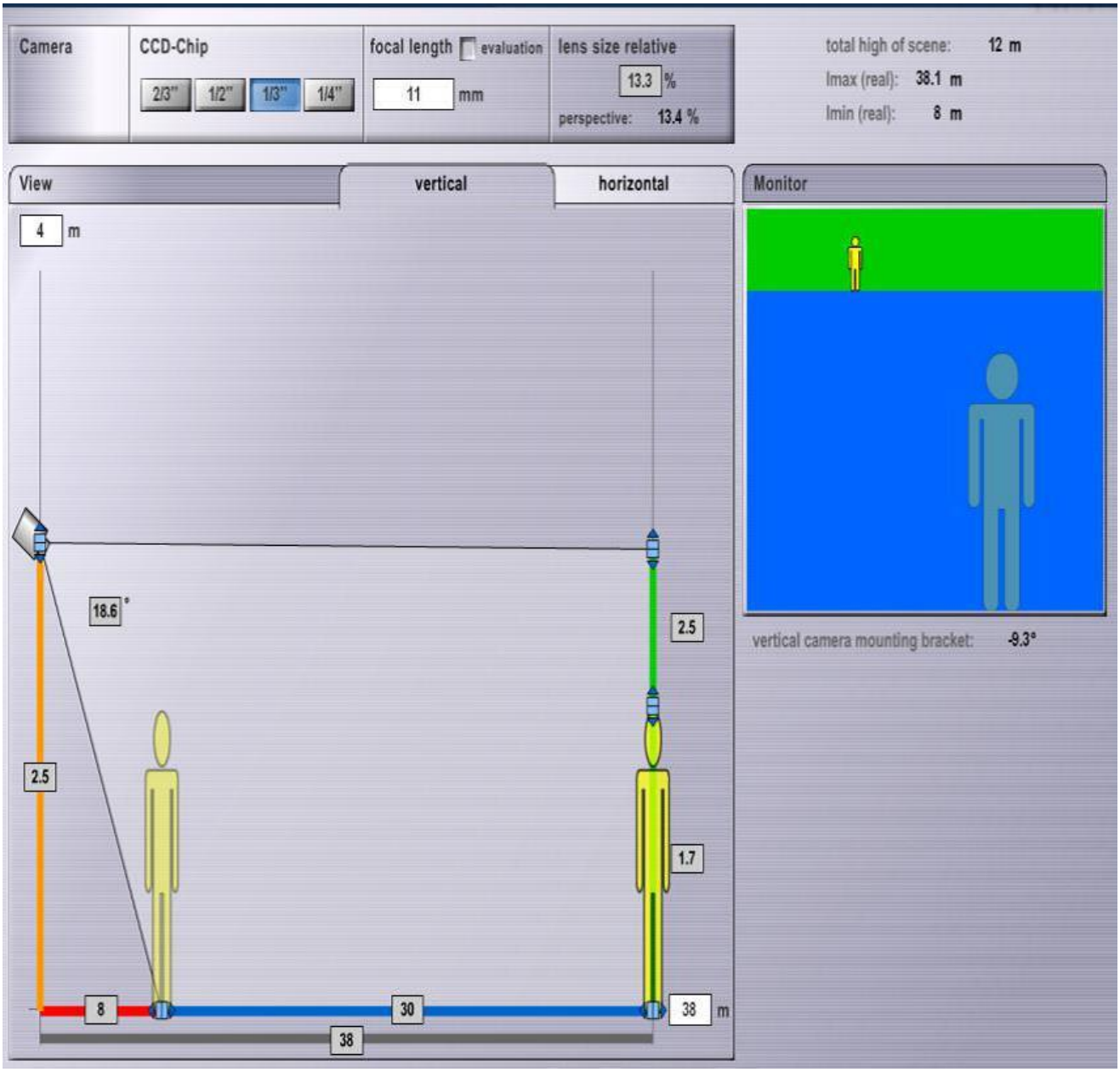


Рисунок 4.4 – Встановлення зони спостереження в горизонтальному положенні

Розрахунок для телевізійних камер ВК-1, ВК-2.

Характеристики:

- фокусна відстань об'єктива - 11 мм;
- кут зору по горизонту - 24,6º;
- відстань до об'єкта спостереження - 38 м.


Camera
CCD-Chip
2/3"
1/2"
1/3"
1/4"
focal length
evaluation
11
mm
lens size relative
13.3
%
perspective:
13.4 %
total high of scene:
12 m
lmax (real):
38.1 m
lmin (real):
8 m
View
vertical
horizontal
Monitor
4
m
18.6
2.5
2.5
1.7
8
30
38
m
38
vertical camera mounting bracket:
-9.3°

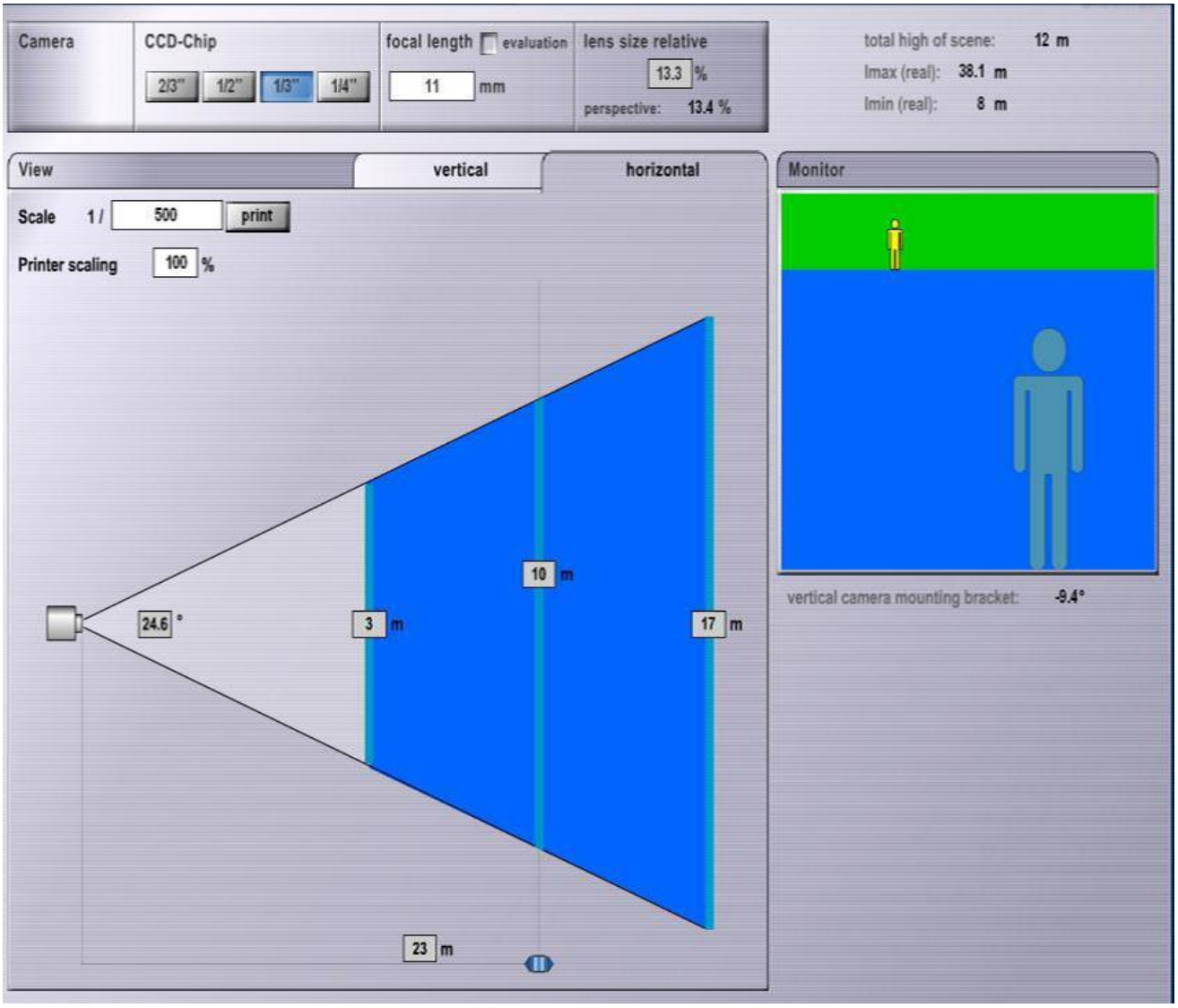
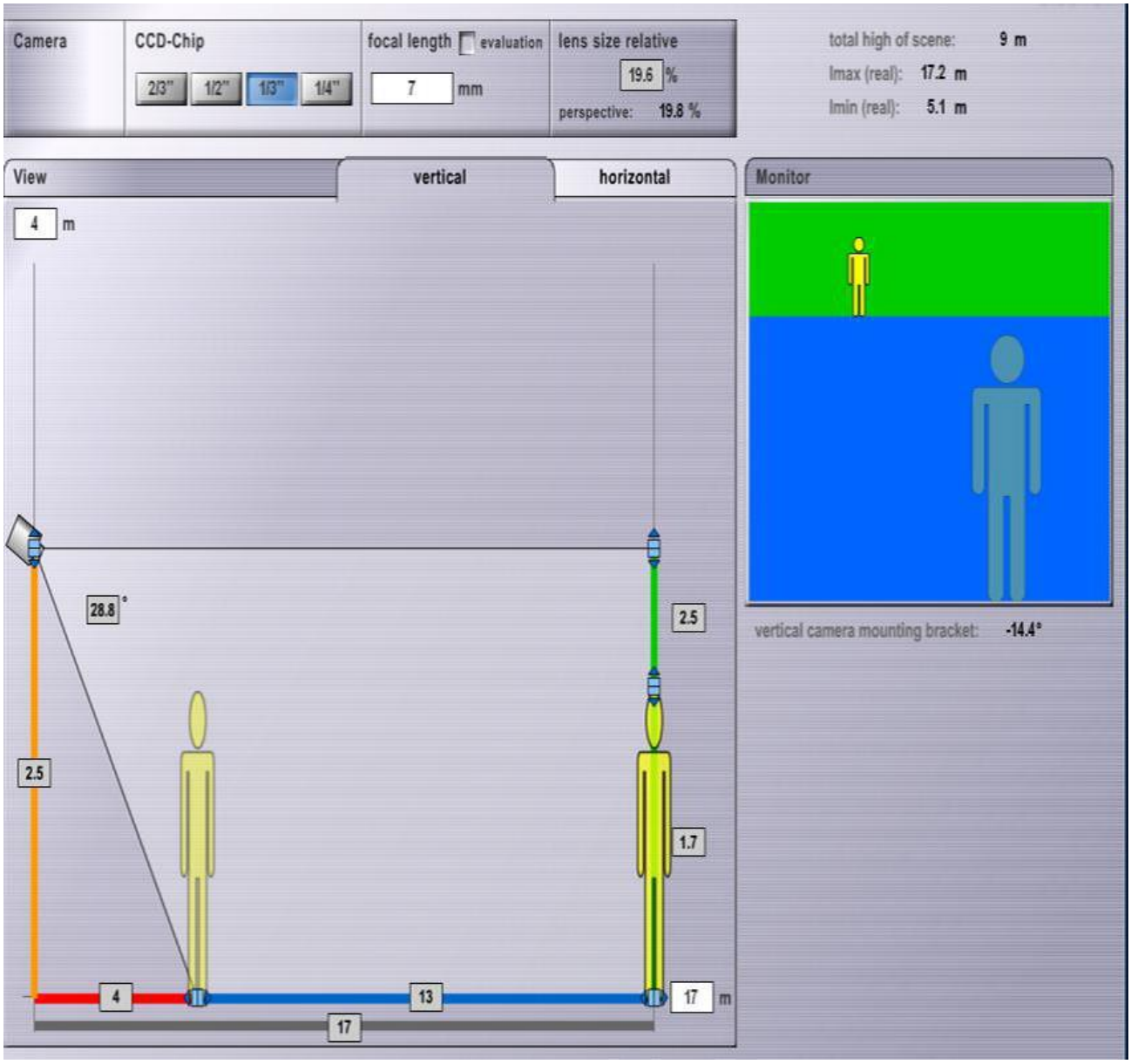


Рисунок 4.5 – Розрахунки для камер ВК-1 та ВК-2

Розрахунок для телевізійних камер ВК-3, ВК-6, ВК-13, ВК-14.

Характеристики:

- фокусна відстань об'єктива - 7 мм;
- кут зору по горизонту - 37,8º;
- відстань до об'єкта спостереження - 17 м.


Camera
CCD-Chip
2/3"
1/2"
1/3"
1/4"
focal length
evaluation
7
mm
lens size relative
19.6 %
perspective: 19.8 %
total high of scene: 9 m
lmax (real): 17.2 m
lmin (real): 5.1 m
View
vertical
horizontal
Monitor
4 m
28.8°
2.5
2.5
1.7
4
13
17 m
17
vertical camera mounting bracket: -14.4°

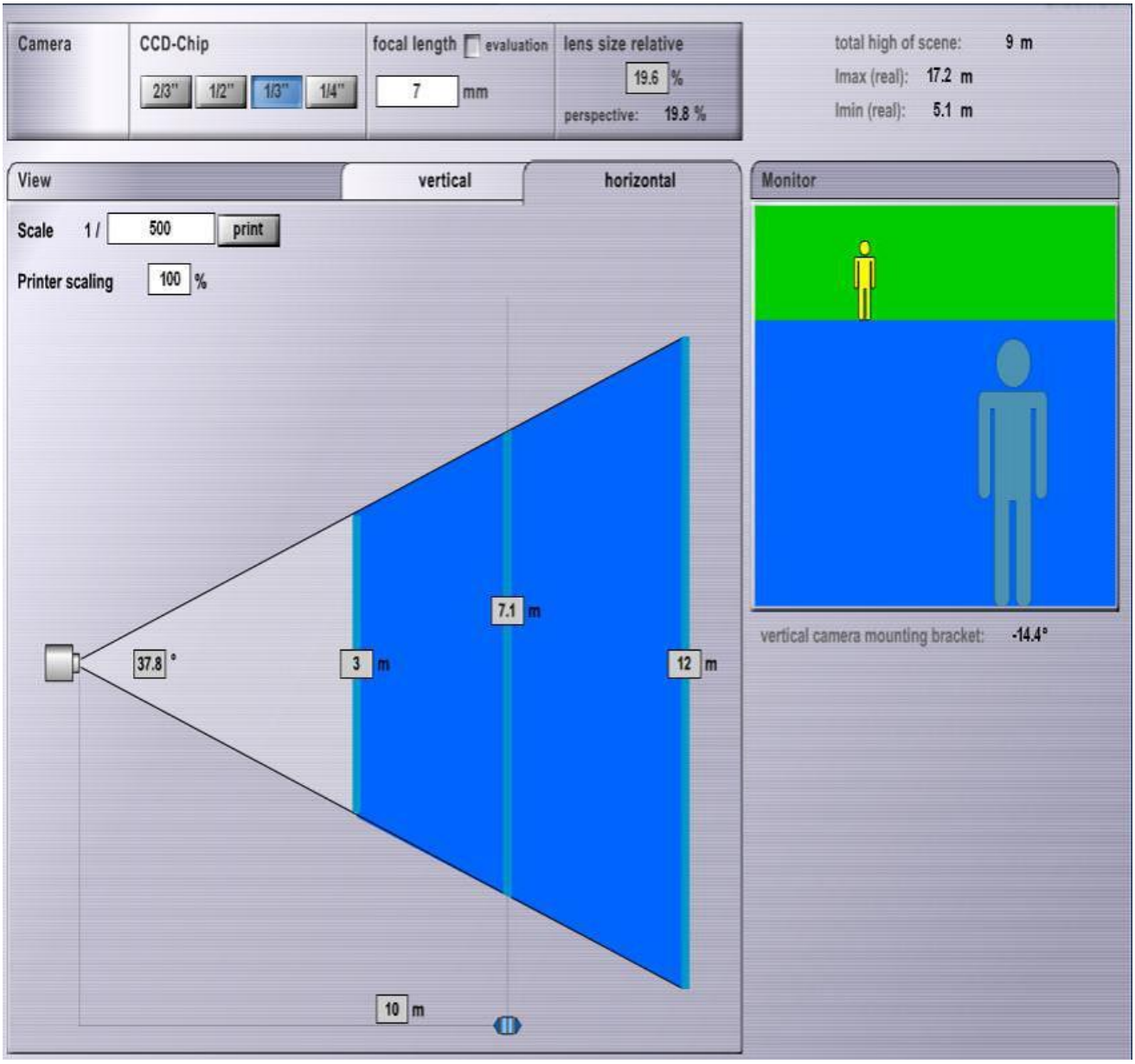


Рисунок 4.5 – Розрахунки для камер ВК-3, ВК-6, ВК-13, ВК-14

Оскільки розрахунок для інших телевізійних камер в програмі ViewDesigner аналогічний, далі наводимо вже готові значення розрахункових показників.

Розрахунок для телевізійних камер ВК-4, ВК-5.

Характеристики:

- фокусна відстань об'єктива - 2,8 мм;
- кут зору по горизонту - 81,2º;
- відстань до об'єкта спостереження - 10 м.

Розрахунок для телевізійної камери ВК-7.

Характеристики:

фокусна відстань об'єктива - 3,5 мм;

- кут зору по горизонту - 68,9º;

- відстань до об'єкта спостереження - 5 м.

Розрахунок для телевізійної камери ВК-9.

Характеристики:

- фокусна відстань об'єктива - 8 мм;

- кут зору по горизонту - 33,4º;

- відстань до об'єкта спостереження - 14 м.

Розрахунок для телевізійних камер ВК-8, ВК-10.

Характеристики:

фокусна відстань об'єктива - 11 мм;

- кут зору по горизонту - 24,6º;

- відстань до об'єкта спостереження - 30 м.

Розрахунок для телевізійної камери ВК-11.

Характеристики:

- фокусна відстань об'єктива - 6 мм;

- кут зору по горизонту - 43,6º;

- відстань до об'єкта спостереження - 10 м.

Розрахунок для телевізійної камери ВК-12.

Характеристики:

- фокусна відстань об'єктива - 2,8 мм;

- кут зору по горизонту - 81,2º;

- відстань до об'єкта спостереження - 10 м.

Розрахунок для телевізійних камер ВК-15, ВК-17

Характеристики:

- фокусна відстань об'єктива - 16 мм;

- кут зору по горизонту - 17,1º;

- відстань до об'єкта спостереження - 37 м.

4.3 Загальна схема системи відеоспостереження

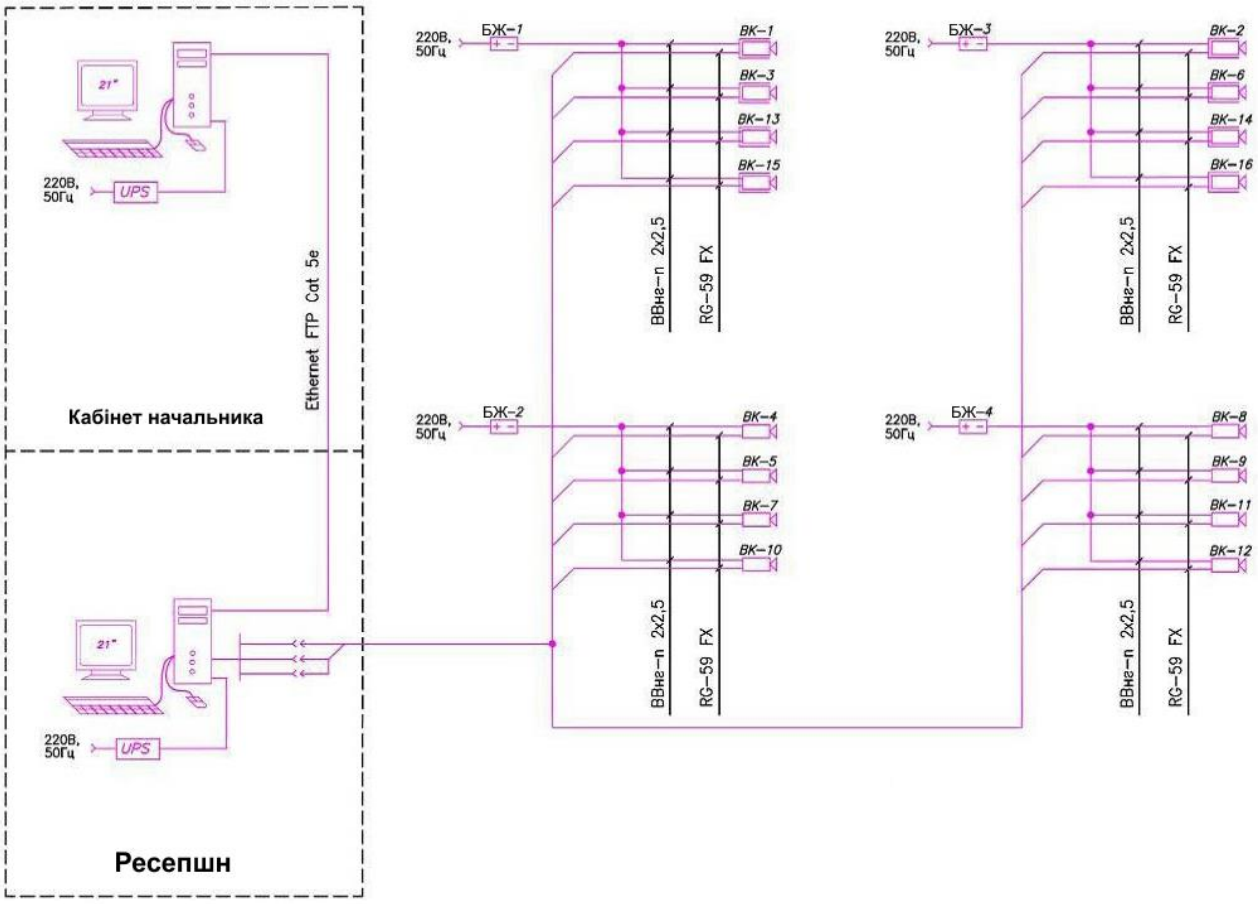


Рисунок 4.6 – Загальна схема системи відеоспостереження

4.4 Кабельна мережа та монтаж електропроводок

Кабелі системи відеоспостереження прокладаються окремо від проводки понад 60 В в окремому електрокоробах. Поза приміщенням кабелі прокладаються в металевому електрокоробах. Між поверхами кабелі прокладаються в металевій трубі d = 60 мм.

Для передачі сигналу від телевізійних камер на мультиплексори і монітори застосовується кабель типу RG-59.

Як канальної середовища для передачі відеоінформації між відеосерверамі в цифровому вигляді використовується екранована кручена пара FTP категорії 5е.

Електроживлення до відеокамер підводиться кабелем типу ВВнг-п 2х2,5. Вибір перетину дроту пояснюється прагненням отримати падіння напруги в лінії живлення менше 5% від номінального значення.

При паралельному прокладанні відстань між проводами і кабелями системи охоронної телевізійної та силовими проводами повинно бути не менше 0,5 м. При необхідності прокладки цих проводів і кабелів на відстані менше 0,5 м вони повинні мати захист від наведень (прокласти в металлорукаве або в металевій трубі). Допускається зменшити відстань до 0,25 м від проводів і кабелів без захисту від наводок до одиночних проводів системи освітлення та контрольних кабелів. Відстань від кабелів та ізольованих проводів, що прокладаються відкрито, безпосередньо за елементами будівельних конструкцій приміщення до місць відкритого зберігання (розміщення) горючих матеріалів повинна бути не менше 0,6 м.

При перетині проводів і кабелів з металевими трубопроводами відстань між ними має бути не менше 50 мм. При паралельному прокладанні відстань від проводів до трубопроводів повинно бути не менше 10 мм.

4.5 Живлення та заземлення

Живлення має здійснюватися від мережі електроживлення І-ої категорії, від окремої групи.

Устаткування (відеосервери, монітори і джерела живлення), встановлене на центральному посту охорони, живиться від мережі 220В, 50Гц. Відеокамери живляться від вторинних спеціалізованих джерел електроживлення.

Для живлення телевізійного обладнання постійною напругою 12В необхідні спеціалізовані джерела живлення, оскільки багато джерел живлення,

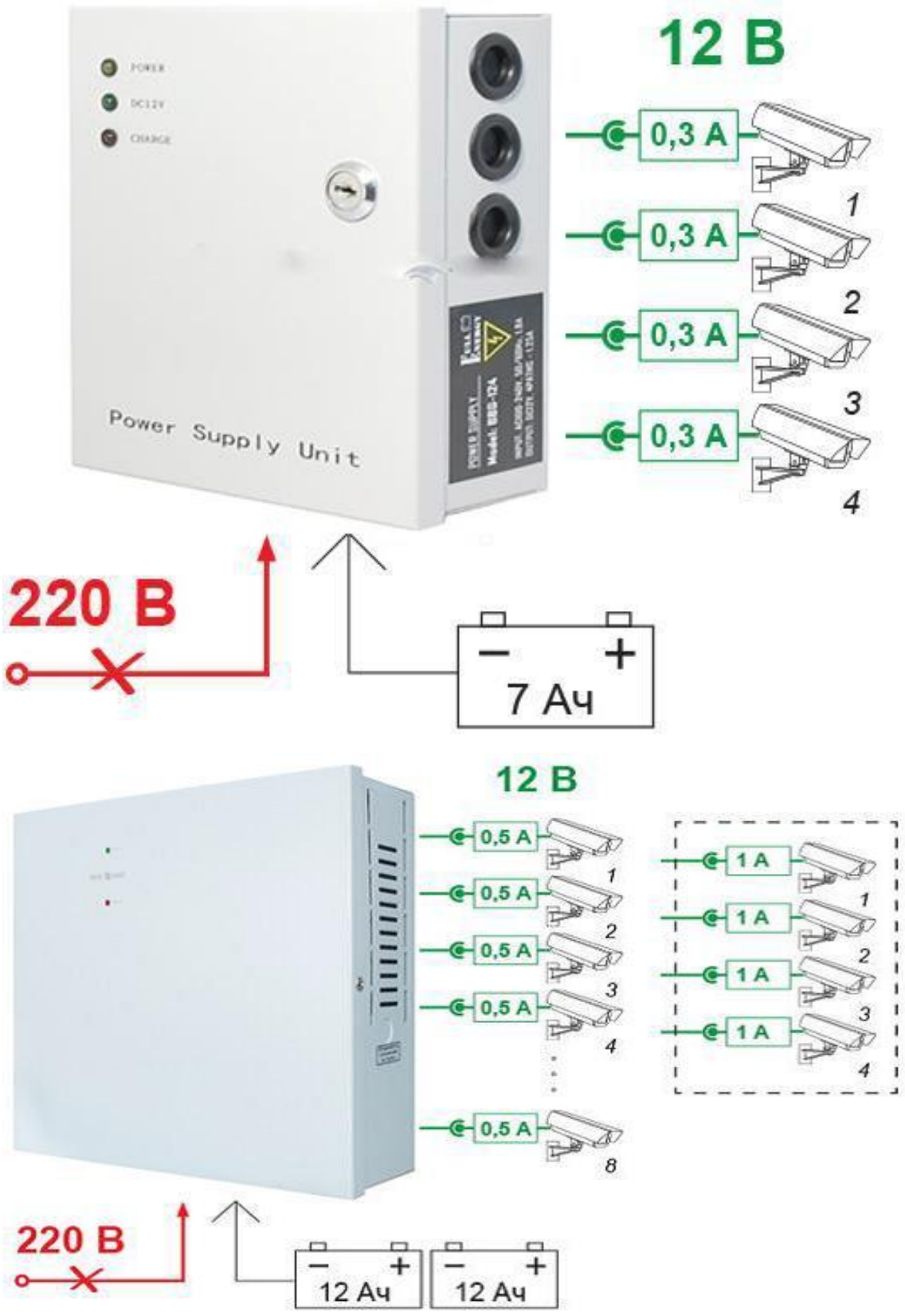
які використовуються для роботи з охоронно-пожежною технікою мають на виході 13,8 В при паспортному значенні в 12 В. Такий розкид напруги для охоронно-пожежної техніки не є критичним параметром через великий діапазон робочих напруг в цих виробах. Однак багато телевізійних камер вкрай критичні як до підвищеної, так і зниженої напруги живлення. Тому необхідно використовувати блок живлення з регульованим діапазоном напруг і зниженою напругою пульсацій на номінальному струмі навантаження (рівень пульсацій не повинен перевищувати 10 мВ).

Загальним правилом при виборі блоку живлення є необхідність мати 30% запас по потужності. Багато блоків живлення при роботі на максимальній потужності різко збільшують рівень пульсацій, а при цьому значно скорочується робочий ресурс блоку живлення.

Виходячи з цих міркувань, для живлення внутрішніх відеокамер пропонується використовувати блоки живлення типу «BBG-124/4». Зрозуміло, допускається використання інших блоків живлення, що мають близькі до вказаних блоків живлення характеристики.

Кожен блок живлення має 4 виходи на відеокамери, плавне регулювання виходу 12-15 В. Струм кожного виходу - до 0,35 А. Можливо підключати навантаження з струмом до 1,4 А до одного виходу; сумарна потужність навантажень 18 Вт. АКБ 4-7 Ач.

Для живлення зовнішніх відеокамер використовується блок живлення типу «BBG-1210/8». Блок живлення призначений для живлення по восьми виходів відеокамер та інших навантажень з номінальним напругою живлення 12 В і номінальним струмом споживання по кожному виходу 0,5 А. У даному випадку організовано 4 виходи з струмом споживання 1 А по кожному виходу. Робота здійснюється від мережі змінного струму напругою 220 В і в режимі резерву - від акумуляторної батареї з номінальною напругою 24 В. Необхідна установка 2 АКБ 7-12 Ач.



Мал. 7.1 Блоки живлення «ВВG-124/4» і «ВВG-1210/8»

Заземлення устаткування і пристроїв повинно виконуватися відповідно до вимог ПУЕ 2017, технічної документації підприємств-виробників.

При відсутності резервного зовнішнього електроживлення (додаткового мережевого фідера) необхідно забезпечити автономне електроживлення системи від бензогенератора необхідної потужності.

Приміщення, де встановлено генератор, має бути опалювальним, температура всередині нього не повинна опускатися нижче + 5 ° С, повинні бути дотримані всі норми і стандарти протипожежної та електробезпеки. Розміри приміщення повинні дозволяти проводити регламентні і ремонтні роботи генератора.

Генератор встановлюється на фундаменті, маса якого становить не менше 1.5 маси генератора або електростанції, при цьому фундамент повинен мати рівну горизонтальну поверхню і не повинен бути пов'язаний з несучими конструкціями будівлі. Генератор закріплюється анкерами, перетяжка анкерів не допускається.

Для ефективного охолодження обладнання необхідна система вентиляції, для відводу вихлопних газів повинна бути змонтована вихлопна труба, яка виходить через отвір в стіні, із застосуванням спеціальних термоизолирующих вставок. З'єднання елементів труби здійснюється за допомогою фланців і хомутів, оскільки проведення зварювальних робіт на генерує обладнанні не допускається.

У приміщенні, де розташовується генератор, необхідно передбачити місце для установки настінного блоку управління і комутації навантаження. З генератором блок управління з'єднується силовим і інформаційним кабелем. Кабель прокладається в кабель - каналах або гофротрубі.

ВИСНОВКИ

В діній роботі було розглянуто, наскільки важливою складовою є забезпечення інформаційної безпеки для підприємств в наш час. Описані основні проблеми інформаційної безпеки та заходи для забезпечення захисту від загроз інформаційної безпеки. Найбільше уваги було зосережденона системі відеонагляду, оскільки це чи не найкращий захист від загроз та надає низку переваг. Можливо контролювати роботу працівників віддалено, навіть коли ви у відпустці, зниження ризиків грабежів, підпалів і тд., моніторинг приміщень з обмеженим доспупом.

В ході розробки даної комплексної системи , було досліджено предметну область, аналізовано теоретичну інформацію про різноманітні засоби захисту інформації, від фізичної до електронної (цифрової), а також були освоєні навички планування та аналізу. На початку роботи я проаналізував актуальність розробки даного проєкту і вирішив розробити комплексну систему захисту інформації для свого підприємства. Завдяки правильному розміщенню камер та розрахунків вся територія навколо підприємства гарно оглядається, неможливо непоміченим потрапити на територію фірми. Також всі важливі об’єкти всередині під цілодобовим наглядом. Був створенний план, на якому показано як краще проложити кабелі живлення та блоки живлення, приведений приклад технічного оснащення.

В ході реалізації проєкту, проєктування було використано середовище CorelDRAW 2018, і додатковим ПЗ, та програма ViewDesigner.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Кібербезпека у системі національної безпеки України: пріоритетні напрями розвитку: збірник матеріалів наукового круглого столу, м. Маріуполь, 26 квітня 2018 р. / Маріупольський державний університет; уклад. Проценко О.Б., Меркулова К.В. – Маріуполь: МДУ, 2018. – 145 с

2. Бурячок В. Л. Основи інформаційної та кібернетичної безпеки. [Навчальний посібник]. / В. Л. Бурячок , Р. В. Киричок, П. М. Складанний – К. , 2018. – 320 с.

3. Tang J, Wang D, Ming L, Li X. A Scalable Architecture for Classifying Network Security Threats. Science and Technology on Information System Security Laboratory; 2012.

4. Howard JD. An Analysis Of Security Incidents On The Internet 1989 – 1995. Doctoral Dissertation, Carnegie Mellon University Pittsburgh, PA, USA; 1998.

5. Geric S, Hutinski Z. Information system security threats classifications. Journal of Information and Organizational Sciences; 2007. 31: 51.

6. Cheswick W.R., Bellovin S.M. Firewalls and Internet Security: Repelling the Wily Hacker. - Addison-Wesley, 1994. - 275 с.

7. Swiderski F, Snyder W. Threat Modeling. Microsoft Press; 2004.

8. Meier J, Mackman A, Vasireddy S, Dunner M, Escamilla R, Murukan A. Improving we application security: threats and counter measures. Satyam Computer Services, Microsoft Corporation; 2003.

9. Alhabeeb M, Almuhaideb A, Le P, Srinivasan B. Information Security Threats Classification Pyramid. 24th IEEE International Conference on Advanced Information Networking and Applications Workshops: 2010. p. 208-213.

10. Гайкович В., Першин А. Безопасность электронных банковских систем. - М.: "Единая Европа", 1994. - 264 с.

11. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.

12. Ruf L, AG C, Thorn A, GmbH A, Christen T, Zurich Financial Services AG, Gruber B, Credit Suisse AG., Portmann R, Luzer H, Threat Modeling in Security Architecture - The Nature of Threats. ISSS Working Group on Security Architectures, http://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture_Threat-Modeling_Lukas-Ruf.pdf

13. Левин В.К. Защита информации в информационно-вычислительных системах и сетях // Программирование. - 1994. - N5. - С. 5-16.

14. ДСТУ 8302:2015. Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання. – Уведено вперше ; чинний від 2016–07–01. – Київ : ДП «УкрНДНЦ», 2016. – 17 с.

15. Текстові документи. Загальні вимоги. СОУ 207.01:2017 / Ю. Бойко, Г. Красильникова, Л. Першина, Т. Касянчук. – Хмельницький : ХНУ, 2017. – 45 с.

16. Богуш, В.М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.

17. Юдін, О.К. Захист інформації в мережах передачі даних / Юдін О.К., Корченко О.Г., Конахович Г.Ф. – К.: Вид-во ТОВ «НВП»ІНТЕРСЕРВІС», 2009. – 716 с.

18. Гленсдорф, П. Термодинамическая теория структуры, устойчивости и флуктуаций: Пер с англ. / Гленсдорф П Пригожин И. Изд. 2-е. – М.: Едиториал УРСС, 2003. – 280 с. (Синергетика: от прошлого к будущему).

19. Малинецкий, Г.Г. Нелинейная динамика и хаос. Основные понятия: Учебное пособие. / Г.Г. Малинецкий. - М.: КомКнига, 2006. – 240 с. (Синергетика: от прошлого к будущему).

20. Тарасевич, Ю.Ю. Математическое и компьютерное моделирование. Вводный курс: Учебное пособие. / Ю.Ю. Тарасевич. – М.: Эдиториал УРСС. 2004. 2004. – 152 с.

21. Управление риском / [Электронный ресурс] под ред. Г.Г. Малинецкого. М.: РАН, 2000. – 249 с. – Режим доступа: http://risk.keldysh.ru/risk/risk.htm.

22. . Милованов, В.П. Неравновесные социально-экономические системы: синергетика и самоорганизация. / В.П. Милованов. – М.: Эдиториал УРСС, 2001. – 264 с.

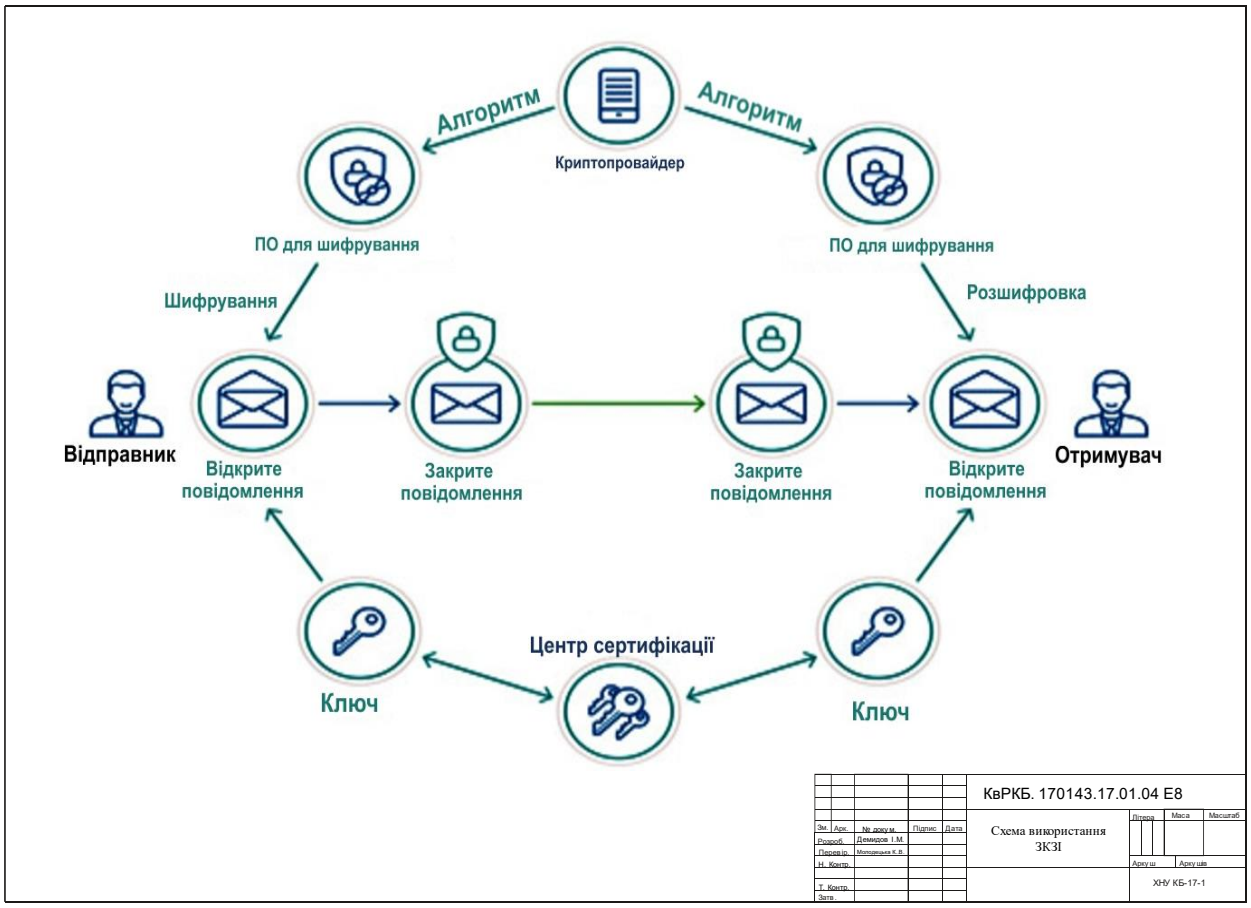
23. Колесников, А.А. Синергетические методы управления сложными системами: Теория системного синтеза. / А.А. Колесников. – М.: КомКнига, 2006. – 240 с.

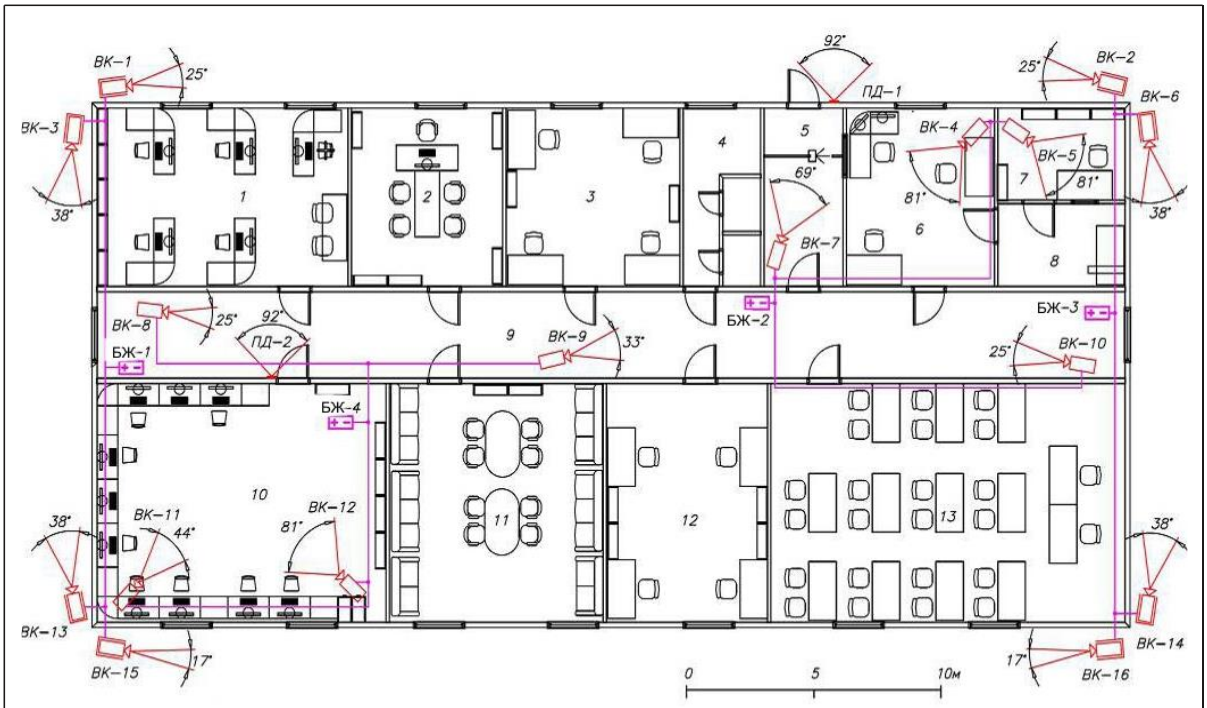
24. ISO. Information Processing Systems-Open Systems Interconnection-Basic Reference Model. Part 2: Security Architecture, ISO 7498-2; 1989

ДОДАТОК А

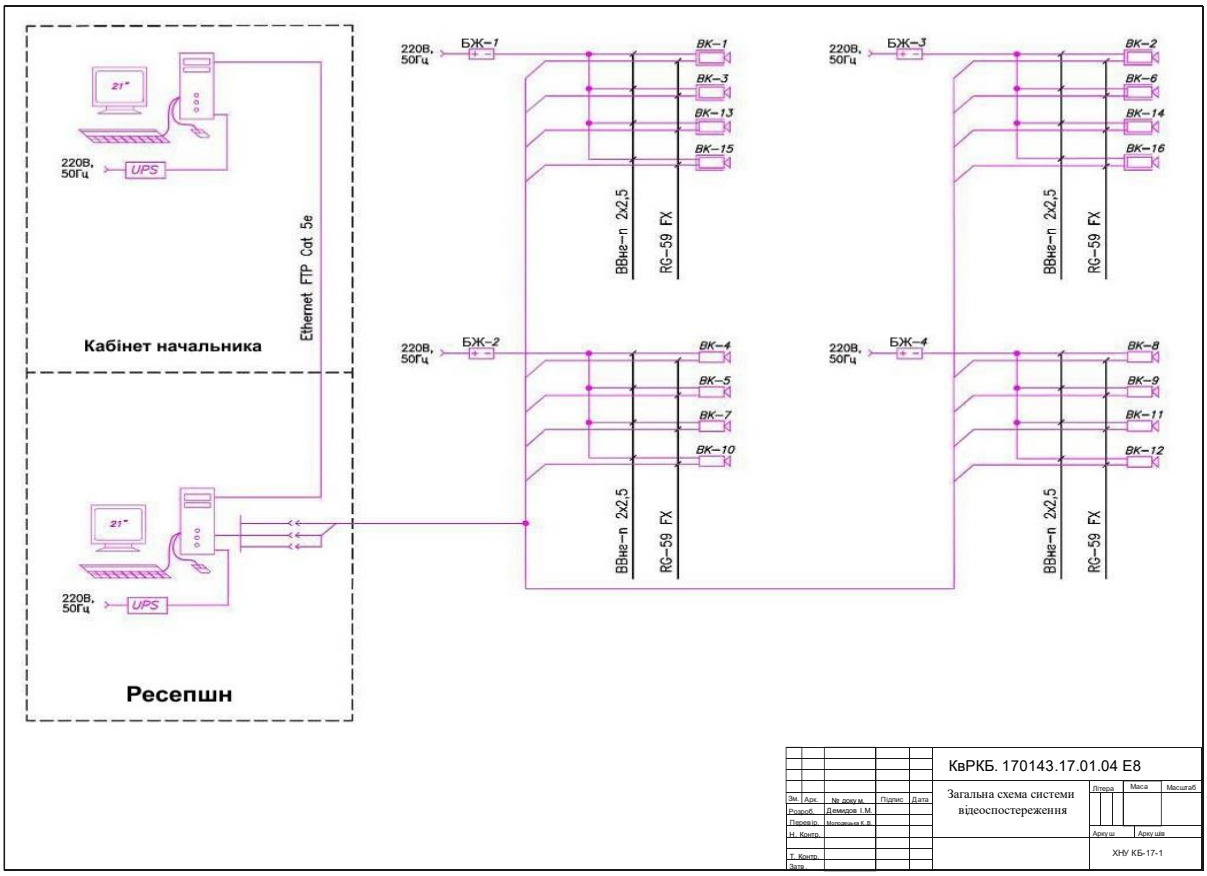
(Обов’язковий)

Копія графічної частини



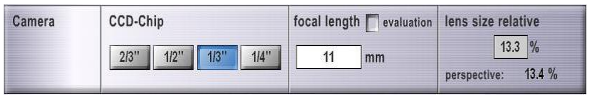


					КвРКБ. 170143.17.01.04 Е8		
					План розташування камер на підприємстві	Літера	Маса / Масштаб
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Демидов І.М.				Аркуш	Аркушів
Перев.р.		Молодецька К.В.					
Н. Контр.						ХНУ КБ-17-1	
Т. Контр.							
Затв.							

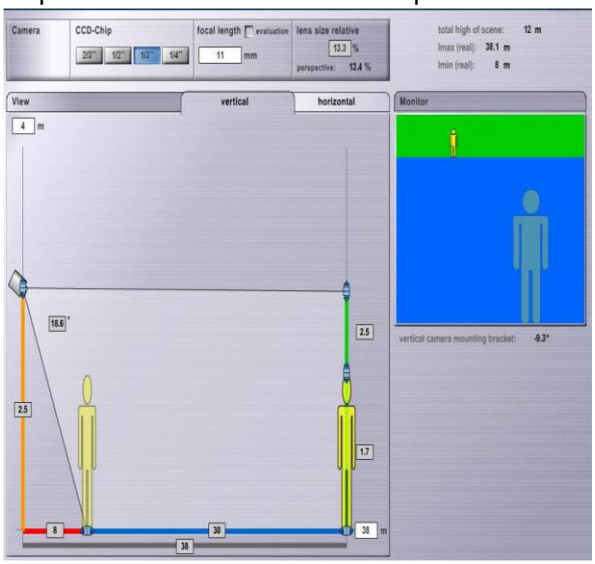


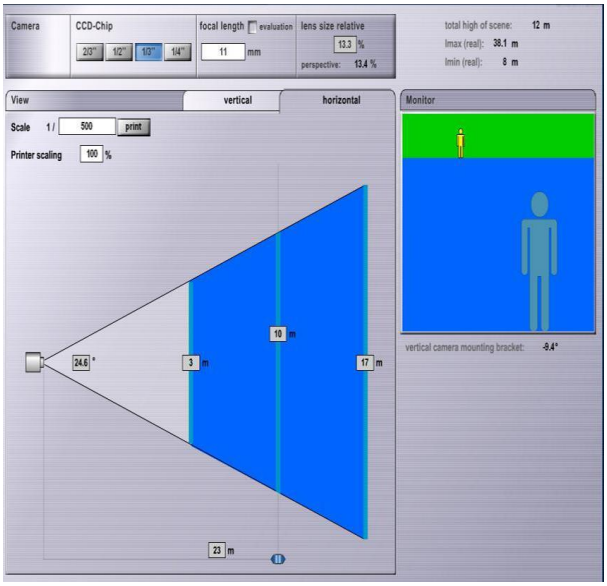
					КвРКБ. 170143.17.01.04 Е8		
					Загальна схема системи відеоспостереження	Літера	Маса / Масштаб
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Демидов І.М.				Аркуш	Аркушів
Перев.р.		Молодецька К.В.					
Н. Контр.						ХНУ КБ-17-1	
Т. Контр.							
Затв.							

Параметри камер



Вертикальна область спостереження





Горизонтальна область спостереження

					КвРКБ. 170143.17.01.04 Е8		
					Встановлення зони спостереження	Літера	Маса	Масштаб
Зм.	Арк.	№ докум.	Підпис	Дата				
Розроб.		Демидов І.М.						
Перевір.		Молодкина К.В.				Аркуш	Аркушів
Н. Контр.							
Т. Контр.						ХНУ КБ-17-1	
Затв.							

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС»

Автор: Демидов Ігор Миколайович

Спеціальність: 125 – Кібербезпека

Освітня програма: Кібербезпека

Керівник: Молодецька Катерина Валеріївна. д.т.н., проф.

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних). Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи.	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	
5	Інше:	

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та прототипів, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформленні посилання;
3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості, складає 0.87% що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ К.В. Молодецька

Завідувач кафедри КбКСМ, гарант ОП _____ Ю.П. Кльоц

Дата: 16.06.2021

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Демидов Ігор Миколайович

Тема Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС»

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «магістр»:

кількість листів креслень 4 ; кількість сторінок записки 76

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено комплексну систему забезпечення інформаційної безпеки.

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині роботи

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У вступі подана загальна характеристика поставленої задачі, чітко визначено об'єкт, предмет та методи дослідження, сформульована актуальність. Визначені задачі, які необхідно вирішити для досягнення поставленої мети, практична цінність отриманих результатів, їхня новизна та наведені відомості про публікації. У першому розділі проведено огляд використовуваних в комп'ютерних системах методів захисту конфіденційної інформації, виконане обгрунтування актуальності теми дослідження і виконана постановка задачі. В другому розділі наведені засоби та технології використані для побудови системи захисту. В третьому розділі визначено основні положення системи. Четвертий розділ було присвячено реалізації системи захисту.

4. Позитивні сторони роботи Кваліфікаційна робота має комплексну практичну цінність. Практична цінність полягає у розробці модуля лексичного аналізу з допомогою якого визначається ступінь конфіденційності даних. На основі даного аналізу в подальшому здійснюється керуючий вплив на витік конфіденційних даних. Практична цінність результатів кваліфікаційної роботи полягає у створені системи захисту від витоків даних, що може бути підлаштована для будь якої категорії даних, і у описі оптимальних моделей функціонування систем захисту подібного характеру.

5. Негативні сторони роботи В роботі недостатньо уваги приділено захисту від зовнішніх атак, також не наведено програмно – апаратне забезпечення яке використовується на підприємстві для вирішення заданої проблеми.

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження Окремі описи в пояснювальній записці необхідно доповнити та більш детально пояснити, для кращого розуміння теми проекту.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «відмінно».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Пилипчук Єлизавета Геннадіївна, доцент кафедри комп'ютерної інженерії та системного програмування, к.т.н., доцент Хмельницького національного університету

«16» 06 2021. (підпис)

UNICHECK

User name:
Кафедра кибербезпеки

Check ID:
1008311497

Check date:
16.06.2021 12:35:34 EEST

Check type:
Doc vs Internet

Report date:
16.06.2021 12:36:47 EEST

User ID:
100005590

File name: **ДПКБ Демидов пл**

Page count: **73** Word count: **12823** Character count: **98011** File size: **4.51 MB** File ID: **1008379032**

0.87% Matches

Highest match: **0.27%** with Internet source (**https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20zitks.doc**)

0.87% Internet sources	74	Page 75

No Library search was conducted

0% Quotes

Exclusion of quotes is off

Exclusion of references is off

0% Exclusions

No exclusions

Modifind

Text modifications detected. Find more details in the online report.

Replaced characters	1

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 1.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 6%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 94198 Название: Комплексне забезпечення інформаційної безпеки на підприємстві ТОВ НТФ «ІНФОСЕРВІС» Добавлено в БД: 2021-06-16 Авторы: Демидов І.М.. Руководители: Молодецька К.В. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	86226	706	1220 (1%)	15 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы