Міністерство освіти і науки України
ПОЛТАВСЬКИЙ ДЕРЖАВНИЙ АГРАРНИЙ УНІВЕРСИТЕТ

Навчально-науковий інститут економіки, управління, права та інформаційних технологій

М А Т Е Р І А Л И

науково-практичної конференції
за підсумками проходження виробничої практики
здобувачів вищої освіти
спеціальності
126 Інформаційні системи та технології
Випуск VII (II частина)

кафедра інформаційних систем та технологій

17 жовтня 2023 р.

Полтава – 2023

Редакційна колегія:

Матеріали науково-практичної конференції за підсумками проходження виробничих практик здобувачів вищої освіти спеціальності 126 Інформаційні системи та технології, кафедра інформаційних систем та технологій Полтавського державного аграрного університету, 17 жовтня 2023 р. Вип. VII (ІІ частина). Полтава: ПДАУ, 61 с.

У збірнику надруковані матеріали досліджень, оприлюднених на науково-практичній конференції за підсумками проходження здобувачами вищої освіти виробничих практик «Стажування з фаху» за освітньо-професійною програмою «Інформаційні управляючі системи та технології» та «Організаційно-аналітична практика» за освітньо-професійною програмою «Інформаційні управляючі системи» спеціальності 126 Інформаційні системи та технології кафедри інформаційних систем та технологій Полтавського державного аграрного університету. У публікаціях зроблені узагальнення теоретичних знань та практичних навичок, набутих під час практики на базі підприємств, організацій.

Відповідальність за зміст та редакцію тез несуть автори та наукові керівники.

ЗМІСТ

Радченко Владислав, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.с.-.г.н., доцент Протас Надія
ДІАГНОСТИКА І ВИЯВЛЕННЯ ПОМИЛОК МЕРЕЖЕВИХ ПРИСТРОЇВ І ОПЕРАЦІЙНИХ СИСТЕМ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ, ЩО ПРОГРАМНО–КОНФІГУРУТЬСЯ 6

Щербина Ілля, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник : к.с.-.г.н., доцент Протас Надія
АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА ПП «НАДЕЖДА» 8

Засядько Дмитро, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Рябий Мирослав
РОЗРОБКА КОМПЛЕКСУ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ 11

Каян Ігор, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.с.-.г.н., доцент Протас Надія
ВИБІР ТЕХНОЛОГІЙ ПІДКЛЮЧЕННЯ І ТАРИФНОГО ПЛАНУ У ПРОВАЙДЕРА ДОСТУПУ В МЕРЕЖУ ІНТЕРНЕТ 13

Безрук Віктор здобувач вищої освіти СВО «Бакалавр»
Науковий керівник: к.т.н., доцент Рябий Мирослав
ВИБІР ТЕХНОЛОГІЙ ПІДКЛЮЧЕННЯ І ТАРИФНОГО ПЛАНУ У ПРОВАЙДЕРА ДОСТУПУ В МЕРЕЖУ ІНТЕРНЕТ 15

Липоватий Владислав, здобувач СВО Бакалавр
Науковий керівник: к. ф.-м. н., доцент Копішинська Олена
СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ 17

Міров Даниїл, Здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.с.-г.н., доцент Протас Надія
МЕТОДИ КОПІЮВАННЯ, АРХІВУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ 20

Михно Тимофій, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Одарущенко Олена
РОЗРОБКА МОДЕЛІ WEB-САЙТУ ДЛЯ ОРГАНІЗАЦІЇ НА БАЗІ WORDPRESS 22

Сосновський Антон, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Рябий Мирослав
МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА 24

Коваленко Руслан, здобувач СВО Бакалавр,
Науковий керівник: к.т.н., доцент Дегтярьова Лариса

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗБЕЦІ ПІДПРИЄМСТВА 26

Мулько Андрій здобувач вищої освіти СВО «Бакалавр»
Науковий керівник: к.т.н., доцент Рябий Мирослав
АНАЛІЗ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА 28

Павлов Егор, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Рябий Мирослав
СПЕЦІАЛІЗОВАНІ ЗАСОБИ ДЛЯ БОРОТЬБИ З ВІРУСАМИ, НЕСАНКЦІОНОВАНИМИ РОЗСИЛКАМИ ЕЛЕКТРОННОЇ ПОШТИ, ШКІДЛИВИМИ ПРОГРАМАМИ 30

Срібна Єва, здобувач СВО Бакалавр
Науковий керівник:к.т.н., доцент Одарущенко Олена
ОРГАНІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА І МОЖЛИВОСТІ ЇЇ ОПТИМІЗАЦІЇ ТА РОЗШИРЕННЯ 32

Турбай Євгеній здобувач вищої освіти СВО «Бакалавр»
Науковий керівник: к.т.н., доцент Одарущенко Олена
ОРГАНІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТ 34

Коряк Владислав, здобувач СВО Бакалавр,
Науковий керівник: к. с.-г. н., доцент Протас Надія
ЗАСОБИ ДІАГНОСТИКИ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ІНТЕРНЕТ 36

Масич Андрій, здобувач вищої освіти СВО «Бакалавр»
Науковий керівник: к.т.н., доцент Одарущенко Олена
ФІЗИЧНЕ СЕРЕДОВИЩЕ ПЕРЕДАЧІ ДАНИХ КОМП'ЮТЕРНОЇ МЕРЕЖІ (ХАРАКТЕРИСТИКИ КАНАЛІВ ЗВ'ЯЗКУ, ТИП КАБЕЛЮ, ЯКЩО У ЯКОСТІ НОСІЯ ВИКОРИСТОВУЄТЬСЯ КАБЕЛЬ) 40

Москаленко Ілля, здобувач вищої освіти СВО Бакалавр
Науковий керівник: к.ф.-м.н., доцент Копішинська Олена
ПЛАНУВАННЯ МОДЕРНІЗАЦІЇ МЕРЕЖЕВИХ ПРИСТРОЇВ І ОПЕРАЦІЙНИХ СИСТЕМ ПРОГРАМНО-КОНФІГУРУЮЧИХ КОМУНІКАЦІЙНИХ СИСТЕМ 43

Ціпановська Дар'я, здобувач СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Одарущенко Олена
СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ 46

Арініч Антон, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Одарущенко Олена
ІНТЕРНЕТ-ЗАГРОЗИ ТА ЗАХИСТ ВІД ВІРУСІВ 49

Базилєв Владислав здобувач вищої освіти СВО «Бакалавр»
Науковий керівник: к.т.н., доцент Одарущенко Олена

ЗАХИСТ І ОБРОБКА КОНФІДЕНЦІЙНИХ ДОКУМЕНТІВ НА ПІДПРИЄМСТВІ 50

Єфремов Андрій, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Одарущенко Олена
ЯК СТВОРЮЄТЬСЯ ДИЗАЙН ДЛЯ ВЕБ САЙТУ 51

Пасько Денис, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Дегтярьова Лариса
ЗАБЕЗПЕЧЕННЯ СВОЄЧАСНОГО КОПІЮВАННЯ, АРХІВУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ Є ЗАПОРУКОЮ НАДІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЇ КОМПАНІЇ 54

Розумій Антон, здобувач СВО «Бакалавр»
Науковий керівник:к.ф.-м.н., доцент Копішинська Олена
АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА 55

Стаднік Максим., здобувач СВО «Бакалавр»,
Науковий керівник: к.ф.-м.н., доцент Одарущенко Олена
АНАЛІЗ БЕЗПЕКИ ТА АУТЕНТИФІКАЦІЇ ЗА ДОПОМОГОЮ RFID 58

Білокінь Олександр, здобувач вищої освіти СВО «Бакалавр»,
Науковий керівник: к.т.н., доцент Рябий Мирослав
ТЕХНІЧНІ ЗАСОБИ ОХОРОНИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ 60

Радченко Владислав, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 *Інформаційні системи та технології*
Науковий керівник: к.с.-г.н., доцент Протас Надія

ДІАГНОСТИКА І ВИЯВЛЕННЯ ПОМИЛОК МЕРЕЖЕВИХ ПРИСТРОЇВ І ОПЕРАЦІЙНИХ СИСТЕМ ІНФОКОМУНІКАЦІЙНИХ МЕРЕЖ, ЩО ПРОГРАМНО–КОНФІГУРУТЬСЯ

Розвинена інфокомунікаційна інфраструктура сьогодні стала необхідною складовою успішного функціонування будь-якого підприємства. Інформаційні технології, мережі зв'язку, програмне забезпечення стали не просто інструментами для збору та обробки інформації, але й каталізаторами для інновацій, взаємодії з клієнтами, оптимізації процесів та підвищення ефективності господарювання. Однією з ключових задач при впровадженні інформаційних систем є забезпечення високого рівня стабільності, надійності та ефективності інфокомунікаційної інфраструктури підприємства. Інтеграція мережевих ресурсів, серверів та баз даних в єдиний інформаційний простір вимагає комплексного підходу до моніторингу та діагностики. В даній роботі пропонується методика для діагностики та моніторингу інфраструктури підприємства за допомогою системи Zabbix.

Метою дослідження є аналіз методики для діагностики та моніторингу інфраструктури підприємства за допомогою системи Zabbix та оцінка можливостей для її впровадження на підприємстві.

Система Zabbix забезпечує можливість постійного моніторингу різних параметрів інфраструктури підприємства, включаючи сервери, мережеві пристрої та бази даних[1]. Zabbix може автоматично надсилати сповіщення про можливі проблеми або відхилення в роботі системи. Система дозволяє аналізувати довгострокові дані про продуктивність і надійність інфраструктури підприємства для вдосконалення стратегій та процесів.

Вільне програмне забезпечення з відкритим кодом, що знижує загальні витрати на впровадження і утримання системи моніторингу. Zabbix може бути налаштована для моніторингу різноманітних технологій та пристроїв, що дозволяє підприємствам з різних секторів ефективно використовувати цю систему. З врахуванням вищезазначених переваг, впровадження системи на підприємстві може сприяти ефективнішому контролю за інфраструктурою, зменшенню часу простою та підвищенню загальної продуктивності.

Методика для діагностики та моніторингу інфраструктури підприємства за допомогою Zabbix розпочинається з попереднього аналізу. На цій стадії вивчається специфіка підприємства та ідентифікуються ключові апаратні та програмні ресурси. Після збору необхідної інформації переходимо до фази планування та конфігурації. Тут встановлюється Zabbix сервер, налаштовуються Zabbix агенти на цільових системах та створюються шаблони для збору даних [2].

Із завершенням планування розпочинається фаза реалізації моніторингу. Збір даних ініціюється активацією Zabbix агентів. Одночасно створюються

тригери для автоматичного виявлення аномалій та налаштовуються механізми сповіщення.

Після отримання перших даних моніторингу, наступна фаза – аналіз та реалізація. Використовуючи дашборди Zabbix, ведеться відстеження ключових показників, проводиться оцінка ефективності системи моніторингу та вносяться корективи в конфігурацію, якщо це необхідно.

Заключна фаза – це документація та підтримка. Створюється детальна технічна документація, яка описує всі аспекти роботи системи. Крім того, розробляється план для подальшої підтримки та оптимізації системи моніторингу.

Запропонована методика забезпечує комплексний підхід до моніторингу та діагностики мережевих ресурсів і систем, враховуючи специфіку підприємства.

Вибір Zabbix як системи для моніторингу і управління мережею обґрунтований кількома ключовими факторами. По–перше, Zabbix має відкритий код, що забезпечує гнучкість та можливість детальної настройки під конкретні потреби підприємства. По–друге, ця система підтримує широкий спектр мережевих протоколів і стандартів, що є критично важливим для інтеграції з різноманітним обладнанням [3]. По–третє, співвідношення "ціна/якість" в даному випадку є найбільш оптимальним, особливо якщо врахувати можливість масштабування системи в майбутньому.

З урахуванням специфіки підприємства, вибір Zabbix як інструменту для моніторингу та діагностики є вдалим рішенням. Такий інструмент надає гнучкість в конфігурації, масштабованість та можливість інтеграції з іншими системами, що є критично важливим для забезпечення надійності та ефективності інфокомунікаційної інфраструктури на підприємстві.

Запропонована методика для діагностики та моніторингу через Zabbix забезпечить: моніторинг учасників мережі; створення тригерів; налаштування сповіщень. Розроблений підхід, зокрема застосування системи моніторингу Zabbix, враховує не тільки технічні аспекти операцій, але й економічні реалії, які є невід'ємною частиною ведення бізнесу. Розроблений метод та проведені розрахунки стають базою для планування бюджетних та ресурсних витрат, і, як результат, підвищують конкурентну перевагу підприємства на ринку.

Враховуючи специфіку підприємства, запропонована система моніторингу Zabbix є доцільною і обґрунтованою. Її гнучкість, широкий спектр підтримуваних протоколів та зручність у масштабуванні забезпечують можливість адаптації під зростаючі потреби підприємства. Також, слід зазначити можливість впровадження системи автоматизованого управління конфігураціями. Це не тільки поліпшить надійність мережі, але і дозволить ефективно адаптуватися до змінних умов ринку та технологічного прогресу.

Список використаних джерел:

1. Особливості Zabbix. [Електронний ресурс]. URL: http://www.zabbix.com/features.php.

2. Мейерс М.,Джерніган С. CompTIA Network+ Certification All-in-One Exam Guide. 7-е вид. Нью-Йорк: McGraw–Hill, 2018. 960 с.
3. Воробієнко П. П. , Нікітюк Л. А. , Резніченко П. І. . Телекомунікаційні та інформаційні мережі: Підручник [для вищих навчальних закладів]. Київ: САММІТ-Книга, 2010. С. 59–79.

Щербина Ілля, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник : к.с.-г.н., доцент Протас Надія

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА ПП «НАДЕЖДА»

ПП «Надежда» – це компанія, яка лідирує в галузі імпорту якісного пального. Швидкий розвиток і розширення ринкової присутності ставлять підвищені вимоги до забезпечення інформаційної безпеки.

Окреслимо можливі етапи комплексного аналізу потенційних загроз інформаційній безпеці ПП «Надежда»:

– перший етап аналізу – ідентифікація ключових інформаційних активів компанії. Для цього проводиться аудит, який охоплює бази даних клієнтів, договори з постачальниками, фінансову інформацію та інші активи. Цей процес допомагає точно визначити, яка інформація є найціннішою й потребує особливого найвищого захисту[2]. Це має стати фундаментом для подальших заходів. Наприклад, база даних клієнтів містить важливу інформацію про партнерів компанії, їхні замовлення та угоди. Втрата цієї інформації може призвести до втрати довіри клієнтів та фінансових втрат.

– SWOT-аналіз. Виконання SWOT-аналізу допомагає визначити сильні та слабкі сторони компанії в контексті інформаційної безпеки. Зокрема, він допомагає зрозуміти, які можливості та загрози існують для інформаційної безпеки.

Сильні сторони можуть включати наявність досвіду у впровадженні передових технік захисту даних, а також високий рівень свідомості серед персоналу.

Слабкі сторони можуть включати відсутність власного центру безпеки інформації та нестачу фінансових ресурсів для модернізації інфраструктури.

– оцінка ризиків. Даний етап полягає у визначенні ймовірності та впливу різних загроз на підприємство. Ці дії дозволяють ідентифікувати потенційні ризики та встановити їхні пріоритети для подальшого управління. Наприклад, ризик несанкціонованого доступу до бази даних клієнтів може бути визнаний як високий пріоритет через можливі наслідки для клієнтів і репутації компанії.

– реалізація заходів забезпечення. На цьому етапі розробляються конкретні заходи забезпечення для мінімізації загроз та вразливостей. Це включає в себе встановлення брандмауерів для контролю вхідного та вихідного трафіку, використання антивірусного програмного забезпечення для

виявлення та блокування шкідливих програм, а також шифрування даних для забезпечення конфіденційності.

– вибір програмного забезпечення. Вибір правильного програмного забезпечення є ключовим аспектом стратегії інформаційної безпеки. Обґрунтування вибору необхідного програмного забезпечення для моніторингу, виявлення та реагування на загрози є критичним.

Аналіз потенційних загроз інформаційній безпеці ПП «Надежда» виявився надзвичайно важливим етапом для забезпечення надійного та стійкого функціонування компанії в умовах сучасного інформаційного середовища. Проведені етапи дослідження дозволили визначити ключові питання та прийняти стратегічні рішення для забезпечення інформаційної безпеки. Проте, важливо пам'ятати, що поява загроз – постійно змінюваний і адаптивний процес, тому важливо й надалі продовжувати слідкувати за новітніми технологіями та змінами в загрозах і активно оновлювати свої стратегії та заходи забезпечення, щоб забезпечити найвищий рівень інформаційної безпеки в майбутньому.

Наступним етапом аналізу може бути оцінка внутрішніх та зовнішніх загроз [3]. Внутрішні загрози можуть включати недостатню освіченість персоналу щодо правил інформаційної безпеки, недостатній контроль над доступом до інформації, а також можливі недоліки в інфраструктурі та програмному забезпеченні. Зовнішні загрози можуть включати кібератаки, зловмисний соціальний інжиніринг, а також загрози, пов'язані зі змінами в законодавстві та регулюючими вимогами.

Після ідентифікації загроз важливо розробити план відповіді на них. Цей план повинен включати проактивні [1] та реактивні заходи для мінімізації ризику та відновлення інформаційної безпеки в разі виникнення проблем. Проактивні заходи можуть включати в себе посилення навчання персоналу щодо інформаційної безпеки, проведення аудитів інфраструктури та перевірок на вразливості, а також регулярне оновлення політик та процедур інформаційної безпеки. Реактивні заходи, у свою чергу, повинні визначити, як реагувати на конкретні загрози та інциденти, включаючи процедури відновлення даних та систем.

Додатково до зазначених етапів аналізу інформаційної безпеки, важливо враховувати інноваційні технології та тренди в цій області. Швидкий технологічний розвиток може привести до нових викликів і загроз, таких як розвиток штучного інтелекту для кібератак, що вимагає постійного вдосконалення заходів забезпечення.

Зокрема, у світі інтернету речей (IoT), де пристрої стають все більш підключеними, з'являється новий рівень складнощів у забезпеченні безпеки. ПП "Надежда" повинно вивчати та імплементувати заходи безпеки для власних систем IoT, щоб уникнути можливих атак на підприємство через цей вектор.

Враховуючи глобальний характер використання хмарних технологій та обробки великих обсягів даних, підприємство також повинно звертати увагу

на безпеку своїх даних в хмарному середовищі. Заходи з шифрування даних, аутентифікації та контролю доступу стають надзвичайно важливими.

У світлі постійних змін у законодавстві та вимогах до захисту персональних даних, таких як GDPR (Загальний регламент про захист персональних даних), підприємство повинно забезпечувати відповідність із сучасними нормами і стандартами в області інформаційної безпеки.

Усі ці аспекти потребують постійного вдосконалення стратегій інформаційної безпеки, а також підтримки високої свідомості персоналу. Важливо створити культуру безпеки в організації, що включає в себе не тільки технічні заходи, але й постійну освіту та навчання працівників щодо сучасних технік та загроз інформаційної безпеки.

Важливим аспектом у забезпеченні інформаційної безпеки є інтеграція в сучасні тенденції кіберзахисту, такі як машинне навчання та аналіз великих даних для виявлення аномалій та реагування на потенційні загрози у реальному часі. Застосування інтелектуальних систем може значно полегшити виявлення та усунення інцидентів, а також підвищити реагування на нові види загроз.

Паралельно із технологічними заходами, важливо приділяти увагу соціальним та організаційним аспектам інформаційної безпеки. Забезпечення високого рівня обізнаності персоналу щодо загроз та правил безпеки може значно зменшити ризик людських помилок та соціального інжинірингу.

Найсучасніші технології, такі як квантові обчислення, також мають потенціал змінити ландшафт інформаційної безпеки. Розробка стратегій забезпечення повинна передбачати можливі наслідки та виклики, які можуть виникнути в результаті впровадження нових технологій.

На кожному етапі аналізу інформаційної безпеки важливо також забезпечити відповідну свідомість та навички персоналу, щоб вони були активними учасниками у забезпеченні безпеки компанії. Навчання та стажування щодо інформаційної безпеки можуть знизити ризик людських помилок та недбалості, що можуть призвести до інформаційних витоків чи інших проблем.

Завершивши аналіз потенційних загроз інформаційній безпеці, ПП "Надежда" може відчувати себе більш впевнено в забезпеченні безпеки своїх інформаційних активів та захисті від можливих загроз. Проте важливо пам'ятати, що інформаційна безпека - це неперервний процес, і ризики можуть змінюватися з часом. Тому важливо продовжувати слідкувати за новими технологіями та загрозами, а також активно оновлювати свої стратегії та заходи забезпечення для забезпечення найвищого рівня інформаційної безпеки у майбутньому.

Список використаних джерел:

1. Бондаренко В. І. Системи захисту інформації в корпоративних мережах. Дніпро: Ліра. 2013. 156 с.

2. Лисенко О. В. Інформаційна безпека в сучасних комунікаційних системах. Львів: Видавництво Львівської політехніки. 2015. 210 с.

3. Peterson, A.B., and Harper, M.C. Information Security Fundamentals. Boston: Pearson, 2012. pp. 67–190.

Засядько Дмитро, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Рябий Мирослав

РОЗРОБКА КОМПЛЕКСУ ОРГАНІЗАЦІЙНИХ ЗАХОДІВ ЩОДО ЗАХИСТУ ІНФОРМАЦІЇ НА ОБ'ЄКТІ

Система захисту об’єктів від витоку інформації складається, в основному, із організаційних і технічних заходів, метою яких є ліквідація або суттєве зменшення можливості витоку конфіденційної інформації, а також контролю захищеності технічних засобів в період їх експлуатації. Організаційний захід – це захід по захисту інформації, проведення якого не потребує застосування спеціально розроблених технічних засобів [1, 2].

Основні організаційні і режимні заходи включають такі:

1. проведення заходів з захисту інформації, здійснюваних організаціями, які мають ліцензію на діяльність у сфері захисту інформації, що надана відповідними органами.
2. категоризація та атестація об'єктів технічного захисту проти несанкціонованого доступу і виділення приміщень для проведення закритих заходів, забезпечуючи дотримання вимог захисту інформації згідно з її рівнем конфіденційності.
3. використання на об'єкті сертифікованих технічних засобів захисту інформації та додаткових технічних заходів безпеки.
4. встановлення контрольованої зони біля об'єкта та дотримання вимог безпеки на підприємстві.
5. залучення до робіт з будівництва, реконструкції об'єктів технічного захисту і монтажу спеціальних засобів охорони, здійснюваних організаціями з відповідною ліцензією.
6. організація контролю та обмеження доступу до об'єктів технічного захисту і виділених приміщень.
7. введення територіальних, частотних, енергетичних, просторових та часових обмежень на використання технічних засобів захисту [2].

Згідно з ДСТУ 3396.1-96 [3] організаційні заходи захисту інформації — комплекс адміністративних та обмежувальних заходів, спрямованих на оперативне вирішення задач захисту шляхом регламентації діяльності персоналу і порядку функціювання засобів (систем) забезпечення інформаційної діяльності та засобів (систем) забезпечення.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня безпеки інформації.

Для захисту інформації створюються спеціальні служби безпеки, які підпорядковуються, як правило, керівництву установи і саме вони організують

створення й функціонування систем захисту інформації. На організаційному рівні завдання забезпечення безпеки інформації включають:

– розроблення та впровадження політик, процедур та стандартів безпеки інформації в організації;

– організація навчання та інструктажу з питань безпеки інформації для персоналу;

– визначення ролей і відповідальності з питань безпеки інформації серед персоналу;

– проведення аудитів безпеки інформації та контроль за їх виконанням;

– встановлення та підтримка механізмів виявлення та реагування на інциденти безпеки інформації;

– забезпечення фізичної безпеки приміщень, обладнання та інфраструктури, що використовуються для обробки інформації;

– управління ризиками, пов'язаними з безпекою інформації, та розроблення стратегій їх зменшення або усунення;

– впровадження систем управління безпекою інформації, таких як ISO/IEC 27001, для забезпечення стабільності та ефективності заходів безпеки.

– оцінка ефективності функціонування системи захисту інформації;

– контроль виконання встановлених правил роботи в системи.

Організаційні методи є базисом комплексної системи захисту інформації в системи. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації системи для забезпечення захисту інформації.

Таким чином, в якості основних рекомендацій щодо використання методів і засобів організаційного захисту, можна назвати обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів; розмежування доступу до інформаційних ресурсів і процесам (встановлення правил розмежування доступу, шифрування інформації при її зберіганні і передачі, виявлення та знищення апаратних і програмних закладок); резервне копіювання найбільш важливих з точки зору втрати масивів документів; систематичне оновлення програмного забезпечення та застосування патчів для виправлення виявлених вразливостей; профілактику зараження комп'ютерними вірусами і визначення чітких правил і процедур збереження, обробки та передачі інформації в організації; оцінка потенційних загроз і ризиків для інформаційної системи та прийняття заходів для їх зменшення або усунення.

Список використаних джерел:

1. Литвин В.В., Пасічник В.В., Шаховська Н.Б. Проектування інформаційних систем. Навчальний посібник. Київ: 2021. 52 с.

2. Головань С.М., Петров О.С., Хорошко В.О., Чирков Д.В., Щербак Л.М. Нормативне забезпечення інформаційної безпеки. За ред. проф. В.О. Хорошка. К.: ДУІКТ, 2008. 533 с.

3. ДСТУ 3396.1-96 ДЕРЖАВНИЙ СТАНДАРТ УКРАЇНИ Захист інформації: https://tzi.com.ua/downloads/DSTU%203396.1-96.pdf

Каян Ігор, здобувач вищої освіти СВО «Бакалавр»,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.с.-г.н., доцент Протас Надія

ВИБІР ТЕХНОЛОГІЙ ПІДКЛЮЧЕННЯ І ТАРИФНОГО ПЛАНУ У ПРОВАЙДЕРА ДОСТУПУ В МЕРЕЖУ ІНТЕРНЕТ

Інтернет став неодмінною частиною сучасного життя. Вибір провайдера та відповідного тарифного плану стало ключовим завданням не лише для звичайних користувачів, а для великих компаній та корпорацій. Сьогодні дуже складно уявить якусь мережу без підключення до інтернету. Все більше компаній активно ведуть свої сторінки в соціальних мережах (Instagram, Facebook, Telegram, Viber) для реклами своєї продукції, послуг, тощо. За даними дослідженням Strategy Analytics, у червні 2021 року на світовому ринку смартфонів відбулася знакова подія: тепер «розумними» телефонами, а, відтак, і Інтернетом, користується половина всього населення (на червень 2021 року чисельність населення планети становить близько 7,90 мільярда осіб). При цьому смартфоном володіють 3,95 мільярда жителів Землі. Сьогодні смартфонами користуються жителі найбільших мегаполісів, невеликих поселень та навіть віддалених сіл в Африці. Популярність цього гаджета обумовлена зручністю, практичністю, мобільністю та багатофункціональністю, дозволяючи вирішувати величезний масив завдань у будь-який момент. Це кишеньковий та незамінний інструмент для багатьох. За оцінками аналітиків, до 2030 року близько 5 млрд людей у всьому світі користуватимуться смартфонами [1].

Кожен користувач, хто планує роботу в Інтернет, стоїть перед вибором певної технології підключення і тарифного плану у провайдера доступу в мережу Інтернет. Окреслимо можливі варіанти технологій підключення і виділимо аспекти, на які слід звертати увагу при виборі провайдера.

Існують різні технології, такі як DSL, кабельний, оптичний та бездротовий доступ [2]. Кожен з них має свої переваги і недоліки.

– DSL і кабельний доступ часто доступні за доступними цінами і забезпечують прийнятну швидкість, але можуть бути вразливими до перевантажень у годинах пік;

– оптичний доступ (наприклад, оптичний волоконний кабель) надає найвищу швидкість та надійність, але він може бути обмеженим доступністю у деяких регіонах та високими вартостями;

– бездротовий доступ, такий як 4G або 5G, дозволяє користувачам мати доступ до Інтернету в будь-якому місці, але його швидкість і стабільність може коливатися в залежності від місця розташування та покриття мережі.

Після вибору технології підключення, користувачам слід розглянути різні тарифні плани провайдера. Ключові питання, на які варто при цьому звернути увагу:

– швидкість передачі даних: Користувачам потрібно визначити, яка швидкість їм потрібна для виконання їхніх завдань. Для великих обсягів завантажень і потокового відео може знадобитися вища швидкість;

– обсяг обміну даними: Якщо користувачі часто завантажують або вивантажують великі файли, їм слід обрати тариф із великим обсягом обміну даними;

– цінова політика: Важливо розуміти загальну вартість тарифного плану, включаючи приховані платежі та знижки за пакетні пропозиції.

Як показує практика, чим популярніший провайдер тим вигідніші умови він дає. Сервіс Steam на мапі статистики завантажень показав топ-10 українських інтернет-провайдерів за швидкістю завантаження й обсягом переданих даних [3]:

– Lanet – 94,3 Мбіт/с;
– Triolan – 65,5 Мбіт/с;
– Freenet – 57 Мбіт/с;
– Volia – 55 Мбіт/с;
– Tenet – 54,7 Мбіт/с;
– Datagroup – 50,9 Мбіт/с;
– Fregat – 46,8 Мбіт/с;
– «Київстар» – 45,3 Мбіт/с;
– «Уарнет» – 44,4 Мбіт/с;
– «Укртелеком» – 26,8 Мбіт/с.

При виборі провайдера і тарифного плану для домашнього інтернету, окрім основних запитів щодо швидкості, обсягу трафіку і ціни, також слід звернути увагу на:

– додаткові послуги. Провайдери можуть пропонувати у тарифі такі послуги як телевізійні пакети чи послуги технічної підтримки, безкоштовні тарифні підписки на онлайн кінотеатри тощо;

– гарантія якості. Не зайвим дізнатися про якість обслуговування та репутацію провайдера в вашому регіоні, можливо, почитавши відгуки і рекомендації від інших користувачів це сформує вашу остаточну думку, та бачення про провайдер;

– контракт і терміни: Варто ретельно читати умови контракту, звернути увагу на строк дії тарифу та умови розірвання контракту.

Отже, вибір технологій підключення і тарифного плану у провайдера є важливим рішенням, яке впливає на зручність користування мережею та витрати. Важливо ретельно розглянути всі вище зазначені аспекти та враховувати свої потреби та можливості. Лише за такого аналізу можна знайти оптимальний баланс між доступністю, якістю та вартістю послуг Інтернету.

Список використаних джерел:

1. Кошелева І. Цифра дня: скільки у світі користувачів смартфонів. Andro-news. URL: https://andro-news.com/ua/news/cifra-dnya-skolko-polzovateley-smartfonov-v-mire.html (дата звернення: 07.09.2023).
2. Ніжна К., Пух В., Новосьолов М. Типи і види інтернет з'єднання. IPkey. URL: http://ipkey.com.ua/uk/faq/1092-internet-connection-types.html (дата звернення: 07.09.2023).
3. Морозов О. Ось топ-10 інтернет-провайдерів в Україні за швидкістю завантаження. The Village Україна. URL: https://www.the-village.com.ua/village/business/news/335137-os-top-10-internet-provayderiv-v-ukrayini-za-shvidkistyu-zavantazhennya (дата звернення: 07.09.2023).

Безрук Віктор здобувач вищої освіти СВО «Бакалавр»
спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Рябий Мирослав

ВИБІР ТЕХНОЛОГІЙ ПІДКЛЮЧЕННЯ І ТАРИФНОГО ПЛАНУ У ПРОВАЙДЕРА ДОСТУПУ В МЕРЕЖУ ІНТЕРНЕТ

Існує кілька основних технологій підключення до Інтернету, які відрізняються за швидкістю, надійністю та зручністю:

– Ethernet - це найпоширеніша технологія підключення, яка забезпечує високу швидкість і надійність [1]. Для підключення по ethernet використовується кабель, який підключається до комп'ютера або роутера.

– Wi-Fi - це бездротова технологія підключення, яка забезпечує зручність використання, але може бути менш надійною, ніж ethernet [2]. Для підключення по wi-fi використовується wi-fi-роутер, який роздає сигнал по всьому приміщенню.

– Кабельне телебачення - це технологія підключення, яка використовується операторами кабельного телебачення [3]. Для підключення по кабельному телебаченню використовується кабель, який підключається до комп'ютера або роутера. Кабельне телебачення забезпечує високу швидкість і надійність.

– Оптоволоконний інтернет - це найновіша технологія підключення, яка забезпечує найвищу швидкість [4]. Для підключення по оптоволоконному інтернету використовується волоконно-оптичний кабель. Оптоволоконний інтернет забезпечує високу швидкість і надійність.

При виборі технології підключення слід враховувати такі фактори:

– доступність. не всі провайдери доступу в мережу інтернет пропонують всі технології підключення.

– швидкість. вибір технології підключення залежить від ваших потреб у швидкості доступу до інтернету. для перегляду веб-сторінок, перегляду відео та спілкування в соціальних мережах достатньо швидкості 10-20 мбіт/с.

для завантаження файлів, онлайн-ігор та відеоконференцій необхідна швидкість від 100 мбіт/с.

– надійність. ethernet і оптоволоконний інтернет є найбільш надійними технологіями підключення. wi-fi і кабельне телебачення можуть бути менш надійними, особливо в умовах перешкод.

– зручність. wi-fi є найбільш зручним способом підключення до інтернету. ethernet і оптоволоконний інтернет вимагають прокладки кабелю, що може бути незручно в деяких випадках.

– вибір тарифного плану

При виборі тарифного плану слід враховувати такі фактори:

– швидкість. тарифний план повинен забезпечувати необхідну швидкість доступу до інтернету.

– обсяг трафіку. тарифний план повинен забезпечувати достатній обсяг трафіку для ваших потреб.

– додаткові послуги. деякі тарифні плани включають в себе додаткові послуги, такі як антивірус, доступ до онлайн-сервісів і т.д.

Загальні рекомендації до вибору інтернет-з'єднання:

– якщо є можливість, вибирайте оптоволоконний інтернет. він забезпечує найвищу швидкість і надійність.

– якщо немає можливості підключитися до оптоволоконного інтернету, вибирайте ethernet. він забезпечує високу швидкість і надійність.

– якщо потрібна мобільність, вибирайте wi-fi. він є найбільш зручним способом підключення до інтернету.

– при виборі тарифного плану враховуйте потреби в швидкості доступу до Інтернету, обсяг трафіку і бюджет.

Вибір технології підключення і тарифного плану є важливим рішенням, яке може вплинути на якість і надійність доступу до Інтернету, а також на вартість послуги. При виборі слід враховувати фактори, описані вище, щоб підібрати найкращий варіант для своїх потреб.

Окрім перерахованих вище технологій, існують і інші, менш поширені. Наприклад, супутниковий інтернет, який забезпечує доступ до Інтернету з будь-якої точки світу, але має низьку швидкість і високу вартість.

Тарифні плани інтернет-провайдерів можуть значно відрізнятися в залежності від країни, регіону та навіть конкретного постачальника послуг. Нижче я наведу загальну інформацію про різні типи тарифних планів, які часто пропонуються провайдерами.

– Провідний широкосмуговий інтернет: Оптоволокно (Fiber Optic): Цей тип підключення надає найвищу швидкість інтернету і доступний у великих містах. Тарифи можуть варіюватися від 100 Мбіт/с до 1 Гбіт/с і більше. Кабельний Інтернет (Cable): Швидкість у кабельних тарифах також може бути високою, зазвичай від 50 Мбіт/с до 500 Мбіт/с.

– DSL (Digital Subscriber Line): ADSL: Швидкість ADSL тарифів може варіюватися від 1 Мбіт/с до 100 Мбіт/с, зазвичай вища швидкість вимагає вищих витрат.

– Супутниковий інтернет: Супутниковий інтернет доступний в віддалених областях, де немає доступу до інших типів підключення. Тарифи можуть бути обмежені за швидкістю та обсягом витрат даних.

– Мобільний інтернет: Мобільні оператори пропонують тарифи для смартфонів і планшетів з різною швидкістю і обсягом даних. Типово, це включає 3G, 4G і 5G тарифи.

– Пакетні пропозиції: Деякі провайдери надають пакетні пропозиції, включаючи інтернет, телефонію та телебачення.

– Бізнес-тарифи: Провайдери також пропонують спеціалізовані тарифи для бізнес-клієнтів, які можуть включати велику швидкість, стабільність підключення та додаткові послуги, такі як VPN або хостинг.

– Тарифи з обмеженням обсягу даних: Деякі тарифи обмежують обсяг завантажень і завантажень даними. Це може бути актуально для тих, хто використовує Інтернет обміну файлами або стрімінговий контент.

– Тарифи з необмеженим обсягом даних: Інші тарифи надають необмежений обсяг даних, що дозволяє користувачам користуватися Інтернетом на повну потужність без обмежень.

– Тарифи для студентів та пенсіонерів: Деякі провайдери пропонують знижки для студентів та пенсіонерів, щоб зробити Інтернет доступнішим для цих груп населення.

– Тарифи з додатковими послугами: Деякі провайдери додають додаткові послуги, такі як антивірусна захист, облікові записи електронної пошти, облікові записи хостингу тощо.

Список використаних джерел

1. Ethernet URL: https://lanmarket.ua › entsiklopediya [Дата звернення 02.07.2023]

2. Wi-Fi TP-Link URL: https://www.tp-link.com [Дата звернення 09.07.2023]

3. Кабельне телебачення URL: https://www.it-tv.org [Дата звернення 15.08.2023]

4. Оптоволоконний інтернет URL: https://provider.in.ua [Дата звернення 02.07.2023]

Липоватий Владислав, здобувач СВО Бакалавр
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к. ф.-м. н., доцент Копішинська Олена

СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ

Товариство з обмеженою відповідальністю "ЗЕРНОВОЗ.ЮА" фокусується на наданні ключових інформаційних послуг, включаючи оброблення даних. У сучасному бізнес-середовищі, де дані вважаються золотою монетою, забезпечення інформаційної безпеки стає життєво важливим аспектом, що впливає на успіх підприємства та довіру клієнтів.

Детальний аналіз поточних механізмів захисту вказує, що компанія використовує сучасні технології, починаючи від базових рішень, таких як Firewall та Antivirus, і завершуючи складнішими системами, наприклад, IDS [1].

Регулярне оновлення та розширення захисних можливостей свідчать про гнучкість підприємства в адаптації до сучасних цифрових викликів.

У зв'язку із стрімким розвитком кіберзагроз та технологічних інновацій, настійно рекомендується регулярно переглядати та модернізувати системи безпеки для відповіді на зростаючі вимоги ринку. Зокрема, оновлення антивірусних баз даних, впровадження двоетапної аутентифікації, розширення VPN мережі та проведення регулярних аудитів та навчання співробітників можуть підвищити ефективність систем інформаційної безпеки.

Ураховуючи динаміку кіберзагроз та зростання обсягів обробки даних, ТОВ "ЗЕРНОВОЗ.ЮА" має прагнути залишатися на передових рубежах технологічного розвитку. Додаткові заходи, такі як впровадження SIEM для аналізу подій та інформації безпеки, рішення EDR для виявлення і реагування на загрози на кінцевих пристроях, і стратегія Zero Trust Security для посилення конфіденційності доступу, можуть стати ключовими компонентами ефективної системи захисту.

Враховуючи важливість гармонійної інтеграції існуючих та майбутніх систем безпеки, слід також пам'ятати, що технологічний прогрес несплочено росте. Регулярний перегляд стратегії інформаційної безпеки та впровадження нововведень є ключовим для забезпечення безпеки даних та активів підприємства [2].

З метою підвищення ефективності систем інформаційної безпеки, рекомендується впроваджувати такі кроки [3]:

1. Оновлення антивірусних баз даних: Регулярне оновлення антивірусних баз даних допомагатиме протистояти новим загрозам та зберігати інформацію віддалено від шкідливих програм.

2. Впровадження двоетапної аутентифікації: Впровадження системи двоетапної аутентифікації для користувачів додасть додатковий шар захисту, забезпечуючи конфіденційність доступу.

3. Розширення VPN мережі: Розширення та оптимізація VPN мережі забезпечить безпечний доступ до корпоративних ресурсів для співробітників, незалежно від їхнього місця розташування.

4. Проведення регулярних аудитів та тренінгів: Регулярні аудити та навчання співробітників щодо питань інформаційної безпеки допоможуть виявляти слабкі місця та підвищувати усвідомленість з цих питань.

Враховуючи зміни в інформаційних технологіях та зростання кількості цифрових загроз, підприємства по всьому світу активно впроваджують нові системи безпеки. Динамічний розвиток та збільшення обсягів обробки даних вимагають від компанії ТОВ "ЗЕРНОВОЗ.ЮА" постійного оновлення та модернізації систем безпеки. На їхньому фоні особливо актуальним є глибокий аналіз потреб підприємства та вибір оптимальних рішень.

Для забезпечення ефективності впровадження нових систем безпеки в ТОВ "ЗЕРНОВОЗ.ЮА" розроблено специфічний підхід, який базується на послідовних етапах. Цей процес розпочинається з аудиту поточної системи безпеки, що допомагає ідентифікувати поточні слабкі місця та визначити напрямки для вдосконалень. Після аналізу ринку інформаційної безпеки обираються найбільш оптимальні системи. Перед фінальним впровадженням проводиться тестування, а після успішної імплементації - моніторинг та оптимізація роботи систем.

Цей підхід дозволяє не лише забезпечити ефективний захист інформаційних ресурсів підприємства, але й оптимізувати витрати на впровадження та підтримку систем безпеки, що є важливим аспектом для успішної комерційної діяльності ТОВ "ЗЕРНОВОЗ.ЮА". Охорона інформації та даних є важливою складовою успіху підприємства. ТОВ "ЗЕРНОВОЗ.ЮА" не лише підтримує існуючі системи безпеки в актуальному стані, але й регулярно оновлює та модернізує їх відповідно до змінюючогося цифрового ландшафту.

Отже, після докладного вивчення систем інформаційної безпеки на підприємстві ТОВ "ЗЕРНОВОЗ.ЮА" можна зробити кілька важливих висновків:

1. Сучасний бізнес-ландшафт вимагає від підприємств не лише технологічного розвитку, але й посилення уваги до питань безпеки. Інформаційна безпека стає критичною складовою успіху будь-якої комерційної організації.

2. ТОВ "ЗЕРНОВОЗ.ЮА" вже використовує ряд ефективних систем захисту, дозволяючи забезпечити захист від більшості сучасних загроз. Однак, світ технологій постійно розвивається, тому постійний моніторинг та модернізація систем безпеки є обов'язковим.

3. Впровадження нових систем безпеки вимагає не лише технічних рішень, але й глибокого розуміння потреб підприємства. Аудит та стратегічне планування дозволяють обрати оптимальні рішення та ефективно їх імплементувати.

4. Забезпечення інформаційної безпеки є постійним процесом, який вимагає від компанії гнучкості та готовності до швидкої адаптації до змін в загрозах та технологіях.

Отже, компанія ТОВ "ЗЕРНОВОЗ.ЮА" знаходиться на правильному шляху в забезпеченні безпеки своєї інформації та готова до майбутніх викликів у цифровому середовищі.

Список використаних джерел:

1. Досьє компанії ТОВ «ЗЕРНОВОЗ.ЮА». URL: https://youcontrol.com.ua/catalog/company_details/42486721/ (дата звернення: 05.09.2023).

2. ТОВ "ЗЕРНОВОЗ.ЮА" код ЄДРПОУ 42486721 – опендатабот. Опендатабот. URL: https://opendatabot.ua/c/42486721 (дата звернення: 05.09.2023).

3. Яковина В. С. Основи безпеки комп’ютерних мереж: Навчальний посібник. Львів : НВФ "Українські технології", 2008. 396 с.

Міров Данiїл, Здобувач вищої освіти СВО «Бакалавр»,
Спеціальність Інформаційні системи та технології
Науковий керівник: к.с.-г.н., доцент Протас Надія

МЕТОДИ КОПІЮВАННЯ, АРХІВУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ

Існує кілька основних методів копіювання, архівування та резервування даних:

Локальне копіювання - це копіювання даних на зовнішні носії, які зберігаються на місці. Цей метод є простим і доступним, але він має ряд недоліків, зокрема:

Ризик втрати даних у разі виникнення аварії

Обмежена пропускна здатність

Необхідність регулярної перевірки працездатності копій

Хмарне зберігання - це зберігання даних на віддалених серверах, які надаються сторонньою компанією. Цей метод має ряд переваг, зокрема:

Зручний доступ до даних з будь-якого місця

Безпека

Автоматичне резервування даних

Однак, цей метод також має ряд недоліків, зокрема:

Залежність від інтернет-з'єднання

Вартість підписки

Архівування - це компресія та зберігання даних, які вже не активно використовуються. Цей метод дозволяє зменшити обсяг зберіганої інформації, що може бути корисно для економії місця на носії. Однак, архівовані дані можуть бути недоступні для швидкого доступу.

Резервне копіювання - це створення копій даних для відновлення в разі втрати або пошкодження. Цей метод є найважливішим для захисту даних від втрати.

При виборі технології копіювання, архівування та резервування даних необхідно враховувати такі фактори:

- Обсяг даних
- Важливість даних
- Ризики втрати даних
- Бюджет

Наприклад, для невеликого підприємства, яке зберігає невеликий обсяг даних, може бути достатньо використовувати локальне копіювання даних на зовнішні носії. Для крупного підприємства, яке зберігає великі обсяги даних, може знадобитися використання хмарних технологій або централізованих систем резервування.

Після вибору технології необхідно розробити та налаштувати систему копіювання, архівування та резервування даних. Це включає в себе такі етапи:

- Вибір обладнання та програмного забезпечення
- Налаштування параметрів системи
- Тестування системи

При розробці системи необхідно врахувати такі параметри:

- Частота копіювання даних
- Тип носіїв, на які будуть зберігатися резервні копії
- Місце розташування резервних копій

Після настройки системи необхідно провести її тестування та валідацію. Це дозволить переконатися в роботі системи та її відповідності вимогам підприємства.

Після тестування та валідації системи необхідно впровадити її на підприємстві та провести навчання персоналу її використанню.

Після впровадження системи необхідно провести оцінку її результатів. Це дозволить оцінити ефективність системи та виявити можливі недоліки.

Ось кілька додаткових рекомендацій щодо забезпечення своєчасного копіювання, архівування та резервування даних:

- Створіть план копіювання, архівування та резервування даних. Цей план допоможе вам упорядкувати процес і забезпечити його ефективність.
- Регулярно перевіряйте резервні копії. Це допоможе вам переконатися, що вони є актуальними та придатними для використання.
- Зберігайте резервні копії в безпечному місці. Це допоможе вам захистити їх від втрати або пошкодження.

Забезпечення своєчасного копіювання, архівування та резервування даних є важливим завданням для будь-якого підприємства. Це дозволяє захистити дані від втрати або пошкодження, що може призвести до серйозних фінансових і репутаційних втрат.

Для ефективного захисту даних необхідно ретельно продумати та реалізувати систему копіювання, архівування та резервування. При цьому необхідно враховувати такі фактори, як:

- Обсяг і важливість даних
- Ризики втрати даних
- Бюджет

Важливо також регулярно перевіряти резервні копії та тестувати систему копіювання, архівування та резервування. Це допоможе переконатися в їхній ефективності та придатності до використання.

Список використаних джерел:

1. Браун, Д., & Гордон, Ч. (2016). Копіювання даних для дурня: весь світ MySQL. Видавництво "Пітер".

2. О'Рейлі, Т., & Реймонд, Е.С. (2002). Програмування для Unix. Видавництво "Вільямс".

3. Могильов О.В. та ін Інформатика: Навч. посібник для студ. пед. ВНЗ. - М: Вид. центр «Академія», 2000. – 816с.

Михно Тимофій, здобувач вищої освіти СВО «Бакалавр»,
Спеціальність 126иІнформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

РОЗРОБКА МОДЕЛІ WEB-САЙТУ ДЛЯ ОРГАНІЗАЦІЇ НА БАЗІ WORDPRESS

Сучасний світ веб-розробки пропонує безліч різних технологій і платформ, проте обрання правильного інструменту є ключовим фактором для досягнення успіху в цьому процесі. Зараз розглянемо детальніше, які переваги приніс CMS WordPress у розробки сайтів.

Легкість використання платформи WordPress

WordPress славиться своєю легкістю використання, що робить його ідеальним вибором для організацій та підприємств, які не мають в команді людину з глибокими знаннями web-розробки[1]. Ось докладніше про те, як саме WordPress відзначається своєю легкістю використання та чому це важливо:

– інтуїтивний інтерфейс: WordPress пропонує інтуїтивний та дружній інтерфейс, який легко зрозуміти людям без технічних навичок. Це означає, що користувачі можуть легко орієнтуватися на адміністративній панелі та знаходити необхідні функції;

– візуальний редактор контенту: один з ключових компонентів легкості використання WordPress - це візуальний редактор контенту, який нагадує текстовий редактор;

– можливість додавання контенту без програмування: WordPress дозволяє додавати та редагувати контент на сайті без необхідності програмування;

– масштабованість: навіть якщо організація починає з невеликого сайту, WordPress може легко масштабуватися з ростом потреб;

– широкий вибір тем і плагінів: WordPress пропонує безліч безкоштовних та платних тем і плагінів, які допомагають налаштувати сторінку за власними потребами, зберігаючи при цьому легкість використання.

Усі ці фактори роблять WordPress ідеальним вибором для організацій, установ та підприємств, які прагнуть створити та підтримувати власний сайт без значних витрат часу та ресурсів на розробку. Легкість використання дозволяє зосередитися на створенні вмісту та спілкуванні з аудиторією, не витрачаючи зайвих зусиль на технічні аспекти.

Розширюваність та плагіни в WordPress

Однією з ключових переваг WordPress є його здатність до будь-якого розширення функціональності завдяки широкому спектру доступних плагінів[2]. Розглянемо цей аспект більш детально:

– широкий вибір плагінів: спільнота WordPress активно розробляє та підтримує тисячі різних плагінів, які покривають практично будь-яку функціональність. Можна знайти плагіни для SEO оптимізації, аналітики, соціальних медіа, контактних форм, безпеки та багато інших галузей;

– простота встановлення та використання: більшість плагінів встановлюються та налаштовуються за кілька кліків;

– спеціалізовані рішення: Завдяки різноманітності плагінів, можна знайти спеціалізовані рішення для конкретних завдань;

– регулярні оновлення та підтримка: багато популярних плагінів мають активну спільноту розробників, які постійно оновлюють їх і надають технічну підтримку. Це важливо для забезпечення безпеки та сумісності плагінів з оновленими версіями WordPress.

Отже, розширюваність за допомогою безлічі плагінів в WordPress створюють ідеальні умови для розробки сайту, який відповідає унікальним потребам та завданням підприємства, без зайвих зусиль та витрат.

Велика спільнота та підтримка в WordPress

WordPress користується дуже активною та великою спільнотою користувачів та розробників. Ця спільнота є однією з найбільших і найактивніших у світі веб-розробки, і вона має величезні переваги для тих, хто обрав WordPress[3]:

– доступ до ресурсів та знань: будь-яке питання чи проблему, яка може виникнути під час розробки або експлуатації сайту, можна легко вирішити завдяки широкому спектру доступних ресурсів;

– підтримка від розробників: завдяки активній спільноті розробників, які створюють теми, плагіни та розширення для WordPress, користувачі можуть з легкістю знайти інструменти для розширення функціональності.

Усі ці фактори роблять WordPress надзвичайно потужним інструментом, що забезпечує користувачам велику підтримку та можливість розвивати свої проєкти на цій платформі.

Шаблони та дизайн в WordPress

Однією з ключових переваг WordPress є доступ до широкого вибору готового дизайну і шаблонів для створення web-сайту:

– різноманітність шаблонів: великий вибір шаблонів означає, що можна знайти дизайн, який відповідає потребам і стильовим уподобанням підприємства, організації, установи, тощо;

– легкість кастомізації: WordPress надає можливість кастомізувати шаблони під потреби підприємства без необхідності глибоких знань веб-дизайну або програмування. Можна змінювати кольори, шрифти, макети, додавати власні логотипи і зображення, щоб створити унікальний вигляд;

– мобільна сумісність: багато шаблонів вже оптимізовані для мобільних пристроїв, що важливо в сучасну епоху;

– вартість та економія: багато шаблонів доступні безкоштовно або за доступну ціну, що значно зменшує витрати на дизайн сайту.

Безпека та оновлення в WordPress

Безпека є надзвичайно важливим аспектом для будь-якого сайту. WordPress дбає про цей аспект та надає кілька переваг:

– регулярні оновлення: WordPress систематично випускає нові версії, які містять покращення безпеки та виправлення вразливостей;

– оновлення плагінів і тем: важливо також регулярно оновлювати плагіни та теми, які використовуються на сайті. Багато розробників плагінів і тем також підтримують їх і випускають оновлення для забезпечення сумісності та безпеки;

– захист від зламу: WordPress включає ряд заходів безпеки, таких як можливість обмежувати спроби несанкціонованого доступу та автоматичне блокування великої кількості невдалих спроб входу.

Загалом, WordPress робить все можливе, щоб забезпечити безпеку веб додатку та дозволяє легко оновлювати його для забезпечення надійності та стабільності.

Усі ці аспекти роблять WordPress ідеальною платформою для розробки web-сайту для організації. Завдяки великій та активній спільноті користувачів та розробників, WordPress забезпечує підтримку, безпеку та безперервний розвиток. Великий вибір шаблонів та можливість кастомізації дозволяють створювати привабливий та унікальний дизайн без великих витрат часу. Розширюваність через плагіни робить можливим додавання будь-якої функціональності за лічені хвилини. Основні функції та безпеку забезпечено системою, а підтримка спільноти допомагає вирішувати будь-які запитання чи проблеми.

Список використаних джерел:

1. Brad Williams “Professional WordPress: Design and Development” 3rd Edition (January 12, 2015), 512 pages.

2. Brad Williams “Professional WordPress Plugin Development”, 2nd Edition (May 21, 2020), 480 pages.

3. Dr. Andy Williams “WordPress for Beginners 2021: A Visual Step-by-Step Guide to Mastering WordPress” Kindle Edition (December 20, 2020), 256 pages.

Сосновський Антон, здобувач вищої освіти СВО «Бакалавр»,
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Рябий Мирослав

МОНІТОРИНГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Моніторинг інформаційної безпеки корпоративної мережі підприємства ТОВ "НВФ "Урожай" є важливим завданням для запобігання витоку конфіденційної інформації, атакам хакерів та іншим загрозам інформаційній безпеці.

Монітнінг інформаційної безпеки корпоративної мережі дозволяє підприємству:

— виявляти потенційні загрози на ранніх стадіях, що може допомогти запобігти інцидентам інформаційної безпеки;

— оперативно реагувати на інциденти інформаційної безпеки, що може допомогти мінімізувати збитки;

— оцінювати ефективність заходів щодо підвищення інформаційної безпеки.

Для ефективного моніторингу інформаційної безпеки корпоративної мережі підприємства ТОВ "НВФ "Урожай" необхідно використовувати комплексний підхід, який включає в себе використання різних засобів і методів.

Комплексний підхід до моніторингу інформаційної безпеки передбачає використання різних засобів і методів, таких як:

— системи аналізу безпеки;
— системи виявлення вторгнень;
— системи управління відповідями на інциденти.

Рекомендації щодо моніторингу інформаційної безпеки корпоративної мережі підприємства ТОВ "НВФ "Урожай":

— впровадити систему аналізу безпеки;
— впровадити систему виявлення вторгнень;
— розробити план реагування на інциденти.

Розгорнуте пояснення:

Система аналізу безпеки допоможе підприємству відстежувати всі події в мережі та виявляти потенційні загрози. Системи аналізу безпеки можуть збирати та аналізувати різні дані, такі як мережевий трафік, журнали подій, поведінку користувачів та т.д.

Система виявлення вторгнень допоможе підприємству захистити мережу від несанкціонованого доступу. Системи виявлення вторгнень використовують різні методи для виявлення несанкціонованого доступу, такі як аналіз мережевого трафіку, виявлення аномалій поведінки користувачів та т.д.

План реагування на інциденти допоможе підприємству оперативно реагувати на інциденти інформаційної безпеки. План реагування на інциденти повинен визначати відповідальних осіб, порядок дій та ресурси, які будуть використовуватися для реагування на інциденти.

Заходи щодо підвищення інформаційної безпеки корпоративної мережі підприємства ТОВ "НВФ "Урожай":

— запровадити політику безпеки;
— запровадити систему аутентифікації та авторизації;
— запровадити систему шифрування;
— запровадити систему резервного копіювання.

Політика безпеки повинна визначати правила і процедури, які повинні дотримуватися співробітники підприємства для захисту інформації. Політика безпеки повинна бути зрозумілою та доступною для всіх співробітників підприємства.

Система аутентифікації та авторизації допоможе захистити мережу від несанкціонованого доступу. Система аутентифікації повинна використовувати надійну систему аутентифікації, наприклад, двофакторну аутентифікацію. Система авторизації повинна визначати, які ресурси і функції доступні кожному користувачеві.

Система шифрування допоможе захистити конфіденційну інформацію від витоку. Система шифрування повинна використовувати надійну систему шифрування, наприклад, шифрування на основі відкритого ключа.

Система резервного копіювання допоможе захистити інформацію від втрати в разі інциденту. Система резервного копіювання повинна регулярно створювати резервні копії даних і зберігати їх в безпечному місці.

Впровадження комплексу заходів щодо моніторингу та підвищення інформаційної безпеки корпоративної мережі підприємства ТОВ "НВФ "Урожай" допоможе підприємству захистити свою інформацію від несанкціонованого доступу, атак хакерів та інших загроз.

Впровадження комплексу заходів щодо моніторингу та підвищення інформаційної безпеки корпоративної мережі підприємства ТОВ "НВФ "Урожай" допоможе підприємству:

— захистити свою інформацію від несанкціонованого доступу, атак хакерів та інших загроз;

— мінімізувати збитки в разі інциденту інформаційної безпеки;

— підвищити рівень довіри до підприємства з боку

Моніторинг інформаційної безпеки є важливим для попередження загроз інформаційній безпеці підприємства. Комплексний підхід з використанням систем аналізу безпеки, виявлення вторгнень, та плану реагування на інциденти є ефективним способом забезпечити цю безпеку. Заходи по підвищенню інформаційної безпеки, такі як політика безпеки, аутентифікація, шифрування та резервне копіювання, грають ключову роль в захисті інформації та підвищенні довіри.

Список використаних джерел:

1. Загрози інформаційної безпеки: http://datami.ua

2. Методи моніторингу інформаційної безпеки: http://integritysys.com.ua

3. Підвищення інформаційної безпеки: https://dslua.org

4. Могильов О.В. та ін Інформатика: Навч. посібник для студ. пед. ВНЗ. - М: Вид. центр «Академія», 2000. – 816с.

Коваленко Руслан, здобувач СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Дегтярьова Лариса

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗБЕЦІ ПІДПРИЄМСТВА

Інформаційна безпека є надзвичайно важливим аспектом для сучасних підприємств у цифровій епохі. Загрози, які можуть виникнути у сфері інформаційної безпеки, постійно зростають в розмірах і складності. Тому аналіз потенційних загроз стає невід'ємною частиною стратегії забезпечення інформаційної безпеки підприємства [1].

Підприємство «Інфосвіт ІТ-Сервіс» має великий обсяг інформації, яка зберігається, обробляється та передається щоденно. Однак із зростанням

значущості інформації зростають і загрози її безпеці. Було розглянуто потенційні загрози інформаційній безпеці підприємства «Інфосвіт ІТ-Сервіс» та способи їх запобігання:

- кібератаки. Кібератаки — це навмисні спроби несанкціонованого доступу, пошкодження чи зміни комп'ютерних систем або мереж. Наслідки кібератак можуть бути різноманітними та серйозними: втрата конфіденційності даних; пошкодження інтегрітету даних; порушення доступності сервісів, мереж або веб-сайтів; фінансові втрати: фінансові втрати через втрату даних, штрафи за порушення законодавства про захист даних, витрати на відновлення систем тощо; порушення репутації; психологічні наслідки. Отже підприємство «Інфосвіт ІТ-Сервіс» повинно мати надійні системи захисту, оновлювати ПЗ та вдосконалювати процедури моніторингу для виявлення аномальних активностей;
- витоки інформації. Підприємство має забезпечувати регулярне навчання свого персоналу з питань безпеки даних і встановлювати жорсткі правила доступу до ключової інформації.
- внутрішні загрози. Підприємство має розробити внутрішню політику безпеки та встановити механізми моніторингу діяльності співробітників.
- віруси та зловмисне ПЗ. Необхідно регулярно оновлювати антивіруси та вживати заходів для контролю за ПЗ, яке встановлюють співробітники.
- соціальна інженерія, яку зловмисники використовують маніпуляцію та інші хитрощі, щоб отримати доступ до цінної інформації. Підприємство повинно навчати своїх співробітників розпізнавати такі атаки та дотримуватися строгих правил безпеки.
- застарілі технології та відсутність резервних копій.

Після визначення загроз і їх імовірності слід розробити стратегію запобігання. Ефективна стратегія запобігання загрозам інформаційної безпеки включає такі ключові етапи:

Оцінка ризиків: проведення аналізу потенційних загроз інформаційній безпеці, визначення вразливостей і оцінка ризиків для інформаційних активів.

Розробка політики безпеки: створення документованої політики безпеки, що визначає стандарти, процедури та вимоги щодо ЗІ.

Організація навчання персоналу: навчання персоналу щодо правил безпеки, процедур і заходів, необхідних для запобігання загрозам інформаційної безпеки.

Реалізація технічних заходів безпеки: впровадження технічних засобів захисту: антивірусне ПЗ, брандмауери, системи виявлення вторгнень тощо.

Контроль доступу: встановлення механізмів контролю доступу до інформаційних ресурсів, таких як паролі, двофакторна аутентифікація.

Моніторинг і виявлення інцидентів: постійний моніторинг мережі та систем на предмет виявлення аномальних активностей і потенційних загроз.

Реагування на інциденти: розробка і впровадження планів реагування на інциденти, які включають процедури реагування на виявлені загрози та відновлення систем після інциденту.

Оновлення та підтримка: систематичне оновлення ПЗ, використання патчів безпеки та інших заходів для забезпечення актуальності захисту.

Аудит та вдосконалення: проведення регулярних аудитів безпеки для виявлення слабких місць і вдосконалення стратегій запобігання загрозам.

Таким чином підприємство «Інфосвіт ІТ-Сервіс» повинно ретельно аналізувати та впроваджувати заходи безпеки для захисту своєї інформаційної інфраструктури від потенційних загроз. Це включає в себе технічні, організаційні та навчальні заходи для забезпечення безпеки даних і збереження довіри клієнтів та партнерів. Тільки так підприємство може успішно функціонувати в сучасному інформаційному середовищі.

Список використаних джерел:

1. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : Навч. посіб. для студ. вищ. навч. закл. Київ : Кондор, 2014. 384 с.

2. Актуальні проблеми забезпечення інформаційної безпеки держави : зб. матеріалів наук.-практ. конф.: Київ, 20 берез. 2009 р. Київ : Нац. акад. СБУ, 2009. 200 с.

Мулько Андрій здобувач вищої освіти СВО «Бакалавр»
спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Рябий Мирослав

АНАЛІЗ СИСТЕМИ ЗАХИСТУ КОРПОРАТИВНОЇ МЕРЕЖІ ПІДПРИЄМСТВА

Корпоративна мережа підприємства - це мережа, яка об'єднує комп'ютери, сервери, периферійні пристрої та інші мережеві компоненти, що використовуються для роботи підприємства. Ця мережа є критичною для бізнесу, оскільки в ній зберігаються та обробляються конфіденційні дані, здійснюється доступ до інтернету та інших зовнішніх мереж.

Система захисту корпоративної мережі підприємства спрямована на запобігання несанкціонованому доступу до мережі, її ресурсів та інформації, а також на виявлення та реагування на інциденти безпеки [1].

Основними компонентами системи захисту корпоративної мережі є:

Фізичний захист - це заходи, спрямовані на запобігання несанкціонованому доступу до мережевих компонентів, таких як сервери, маршрутизатори, комутатори. До фізичного захисту відносяться:

- контроль доступу до будівель та приміщень, де розташовані мережеві компоненти;
- системи відеоспостереження;
- системи контролю доступу до серверних кімнат та інших критичних зон.

Мережевий захист - це заходи, спрямовані на запобігання несанкціонованому доступу до мережі ззовні, а також на захист мережевих ресурсів від атак. До мережевого захисту відносяться [2]:

- мережеві фільтри;

- системи виявлення та запобігання вторгненням (IDS/IPS);
- системи управління доступом (ACL);
- vpn-мережеві з'єднання.

Програмний захист - це заходи, спрямовані на захист програмного забезпечення та даних від несанкціонованого доступу, модифікації, видалення або знищення. До програмного захисту відносяться [3]:

- антивірусні програми;
- антиспам-фільтри;
- системи захисту від шкідливих програм;
- системи управління правами доступу (rbac).

Людський фактор - це важлива складова системи захисту корпоративної мережі. Працівники підприємства повинні бути обізнані про ризики безпеки та дотримуватися правил безпеки.

Найбільш важливою проблемою, яка може призвести до витоку інформації на підприємстві, БСТ "Проектбудмонтаж" є людський фактор.

Підприємству необхідно вжити заходів для підвищення обізнаності співробітників про правила і процедури захисту інформації, а також для забезпечення контролю за доступом до інформації та мотивації співробітників до дотримання правил безпеки.

Для ефективного захисту корпоративної мережі необхідно регулярно проводити аналіз системи безпеки. Цей аналіз повинен включати в себе наступні етапи:

Оцінка загроз - це процес виявлення та оцінки потенційних загроз для корпоративної мережі. До загроз можуть відноситися:

- зовнішні атаки: хакерські атаки, ddos-атаки, атаки на критичну інфраструктуру;
- внутрішні атаки: несанкціонований доступ, крадіжка даних, розголошення конфіденційної інформації.

Оцінка ризиків - це процес визначення ймовірності та впливу потенційних загроз.

Оцінка системи безпеки - це процес оцінки ефективності існуючої системи безпеки.

Рекомендації - це список заходів, які необхідно вжити для підвищення ефективності системи безпеки.

Аналіз системи безпеки корпоративної мережі дозволяє виявити слабкі місця в системі та розробити рекомендації щодо їх усунення. Це допоможе підвищити рівень захисту мережі та зменшити ризик інцидентів безпеки.

Рекомендації щодо підвищення ефективності системи захисту корпоративної мережі підприємства

Для підвищення ефективності системи захисту корпоративної мережі підприємства необхідно вжити наступних заходів:

- посилення фізичного захисту - це може включати в себе встановлення додаткових систем безпеки, таких як камери відеоспостереження, датчики руху, системи контролю доступу;

– вдосконалення мережевого захисту - це може включати в себе розширення використання мережевих фільтрів, впровадження систем ids/ips, використання vpn-мереж для доступу до корпоративної мережі ззовні;

– удосконалення програмного захисту - це може включати в себе використання більш сучасних антивірусних програм, систем захисту від шкідливих програм, систем управління правами доступу;

– посилення навчання працівників з питань безпеки - працівники підприємства.

Корпоративна мережа підприємства є критичною для бізнесу. Система захисту корпоративної мережі повинна бути комплексною та включати в себе фізичний, мережевий, програмний захист та людський фактор. Регулярний аналіз системи безпеки дозволяє виявити слабкі місця в системі та розробити рекомендації щодо їх усунення.

Список використаних джерел:

1. Організація комп’ютерних мереж URL: https://ela.kpi.ua/bitstream/123456789/22890/1/Organizacia_komputernyh_merezh_Konspekt_lekciy.pdf (дата звернення 10.09.2023)
2. Мережевий захист інформації URL: https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf (дата звернення 10.09.2023)
3. Програмний захист інформації. URL: https://pzks.fpm.kpi.ua/documents/sylabusy/ukr/bakalavry/vybirkovi/Sylabus_ProgramSecurity.pdf (дата звернення 11.09.2023)

Павлов Егор, здобувач вищої освіти СВО «Бакалавр»,
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Рябий Мирослав

СПЕЦІАЛІЗОВАНІ ЗАСОБИ ДЛЯ БОРОТЬБИ З ВІРУСАМИ, НЕСАНКЦІОНОВАНИМИ РОЗСИЛКАМИ ЕЛЕКТРОННОЇ ПОШТИ, ШКІДЛИВИМИ ПРОГРАМАМИ

Віруси, несанкціоновані розсилки електронної пошти та шкідливі програми є серйозною загрозою для інформаційної безпеки. Ці загрози можуть призвести до втрати даних, пошкодження обладнання та програмного забезпечення, а також до фінансових втрат.

– Віруси - це шкідливі програми, які можуть завдати шкоди комп'ютеру або мережі. Вони можуть зашифрувати дані, видалити файли або навіть знищити систему.
– Несанкціоновані розсилки електронної пошти - це електронні листи, які надсилаються без дозволу. Вони часто містять шкідливе програмне забезпечення або інші небажані файли.
– Шкідливі програми - це програми, які можуть завдати шкоди комп'ютеру або користувачеві. Вони можуть красти особисті дані,

отримувати доступ до конфіденційної інформації або навіть відстежувати користувача.

Спеціалізовані засоби для боротьби з вірусами, несанкціонованими розсилками електронної пошти, шкідливими програмами можна розділити на кілька категорій:

- Антивірусні програми - це програми, які призначені для виявлення та видалення вірусів. Вони використовують різні методи для виявлення вірусів, включаючи сигнатурне аналізування, динамічне аналізування та штучний інтелект.
- Фільтри спаму - це програми, які призначені для фільтрації несанкціонованих розсилок електронної пошти. Вони використовують різні методи для виявлення спаму, включаючи аналіз заголовків електронних листів, вмісту електронних листів та поведінки користувачів.
- Засоби захисту від шкідливих програм - це програми, які призначені для захисту від шкідливих програм. Вони використовують різні методи для виявлення шкідливих програм, включаючи сигнатурне аналізування, динамічне аналізування та штучний інтелект.

Основні функції спеціалізованих засобів для боротьби з вірусами, несанкціонованими розсилками електронної пошти, шкідливими програмами:

- Виявлення - це здатність програми виявити вірус, несанкціоновану розсилку електронної пошти або шкідливу програму.
- Ідентифікація - це здатність програми ідентифікувати тип вірусу, несанкціонованої розсилки електронної пошти або шкідливої програми.
- Видалення - це здатність програми видалити вірус, несанкціоновану розсилку електронної пошти або шкідливу програму.
- Профілактика - це здатність програми запобігти зараженню вірусом, несанкціонованою розсилкою електронної пошти або шкідливою програмою.

Заходи для підвищення ефективності спеціалізованих засобів для боротьби з вірусами, несанкціонованими розсилками електронної пошти, шкідливими програмами:

- Оновлення програмного забезпечення - виробники антивірусних програм регулярно випускають оновлення, які містять нові сигнатури вірусів. Важливо регулярно оновлювати антивірусне програмне забезпечення, щоб забезпечити максимальний захист від вірусів.
- Використання брандмауера - брандмауер допомагає захищати комп'ютер від несанкціонованого доступу з Інтернету. Брандмауер може блокувати несанкціоновані розсилки електронної пошти, шкідливі програми та інші загрози.

– Обережність при використанні Інтернету - користувачі повинні бути обережними при використанні Інтернету. Не слід відкривати електронні листи від невідомих відправників, не слід завантажувати файли з ненадійних джерел і не слід переходити за посиланнями на невідомих веб-сайтах.

Для забезпечення ефективного захисту від вірусів, несанкціонованих розсилок електронної пошти та шкідливих програм важливо використовувати комплексний підхід, який включає використання декількох різних засобів захисту, а також дотримання простих правил безпеки.

Список використаних джерел:

1. Джейсон Грегорі. Game Engine Architecture, 2009. 1240 с.
2. Джессі Шелл. The Art of Game Design: A Book of Lenses, 2008. 489 с.
3. Мартин Фаулер. Рефакторинг. Улучшение проекта существующего кода, 2017. 448 с.
4. Трейсі Фуллертон. Game Design Workshop: A Playcentric Approach to Creating Innovative Games, 2008, 496 с.
5. Періс Баттфілд. Unity Game Development Cookbook: Essentials for Every Game, 2019. 408 с.

Срібна Єва, здобувач СВО Бакалавр
Спеціальність 126 Інформаційні системи та технології
Науковий керівник:к.т.н., доцент Одарущенко Олена

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА І МОЖЛИВОСТІ ЇЇ ОПТИМІЗАЦІЇ ТА РОЗШИРЕННЯ

Комп'ютерні мережі стали невід'ємною частиною функціонування сучасних підприємств, забезпечуючи зв'язок між різними відділами, спрощуючи обмін даними та забезпечуючи безпеку і ефективність роботи. Організація мережі має великий вплив на продуктивність та конкурентоспроможність підприємства.

На підприємстві використовується сучасна технологія VLAN (Virtual Local Area Network), що дозволяє створювати віртуальні локальні мережі для забезпечення кращої організації робочого середовища. Кожен VLAN є групою клієнтів з певними параметрами мережі, які взаємодіють між собою, незалежно від їх фізичного розташування [1]. Це сприяє забезпеченню безпеки, відокремленості трафіку та підвищенню ефективності мережі.

IP-адресація підприємства складається з основної мережі LAN (Local Area Network) з адресою 192.168.0.1/24. Основна мережа об'єднує комп'ютери та інші пристрої, які знаходяться в межах однієї будівлі [2]. Для забезпечення кращого управління та безпеки мережі, використовується IP-адреса 192.168.99.20, що призначена для управління пристроями на мережі і доступу адміністратора.

У структурі мережі виділяються сервери з різними функціональностями такі як: конструкторський сервер (192.168.0.6), технологічний сервер

(192.168.0.7), Data server(192.168.0.15) та сервери 1С (192.168.0.240 та 192.168.0.160).

Для забезпечення безпеки і надійності мережі використовується система резервного копіювання Bacula. Ця система дозволяє автоматизувати процес резервного копіювання та відновлення даних, що забезпечує захист від можливих втрат даних [3].

Для забезпечення безпеки і конфіденційності даних використовується VPN (Virtual Private Network) - віртуальна приватна мережа. Це дозволяє працювати з підприємством з будь-якого місця, забезпечуючи захищений канал зв'язку та шифрування даних [4].

Для оптимізації та розширення мережі на підприємстві можна вжити кілька заходів:

1. Оптимізація VLAN:

– Детальне планування VLAN: ретельне розроблення структури мережі допоможе уникнути зайвих перекритів та недоліків. Можна використовувати тегування VLAN для забезпечення відокремлення трафіку;

– Об'єднання подібних функцій у VLAN: об'єднання подібних функцій у віртуальну мережу, тобто групування пристроїв з подібними функціями (наприклад, сервери, принтери тощо) у відповідних VLAN дозволить зменшити трафік і спростити управління;

– Використання VLAN-аналізаторів: використання спеціальних інструментів дозволяє моніторити та аналізувати рух в мережі VLAN, виявляти можливі проблеми та оптимізувати конфігурацію.

2. Масштабування IP-адресації:

– IPv6 впровадження: перехід на IPv6 дозволяє забезпечити великий IP-адресний простір для подальшого розширення без проблем з дефіцитом адрес.

– Динамічне присвоєння IP-адрес: використання протоколів динамічного присвоєння IP-адрес (наприклад, DHCP) дозволяє ефективно керувати адресами та забезпечити автоматичне розширення.

3. Резервне копіювання і відновлення:

– Автоматизація резервного копіювання: Використання резервного програмного забезпечення, такого як Bacula, дозволяє автоматизувати процес резервного копіювання для всієї мережі.

– Зберігання на хмарних платформах: Вивчення можливостей зберігання резервних копій на хмарних платформах допомагає забезпечити безпечне зберігання даних.

– Тестування відновлення: Регулярне тестування процесу відновлення даних допомагає переконатися, що система готова до відновлення після випадку неполадок.

Організація комп'ютерної мережі на підприємстві є важливим аспектом його функціонування. Використання технології VLAN, IP-адресації, серверів, резервного копіювання та додаткових технологій сприяє ефективному обміну даними, забезпечує безпеку та допомагає досягти високої продуктивності підприємства. Оптимізація та розширення мережі є важливим кроком для забезпечення зростання підприємства та відповідності вимогам ринку.

Список використаних джерел:

1. VLAN. URL: https://tadex.com.ua/about-vlan/ (дата звернення 15.08.2023).
2. Що таке локальна мережа (LAN)? URL: https://ua.savtec.org/articles/howto/what-is-a-local-area-network-lan.html (дата звернення 15.08.2023).
3. Bacula. URL: https://en.wikipedia.org/wiki/Bacula (дата звернення 15.08.2023).
4. Що таке VPN, і як ним безпечно користуватись. URL: https://cip.gov.ua/ua/news/sho-take-vpn-i-yak-nim-bezpechno-koristuvatis (дата звернення 15.08.2023).

Турбай Євгеній здобувач вищої освіти СВО «Бакалавр»
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ОРГАНІЗАЦІЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ПІДПРИЄМСТВА І МОЖЛИВОСТІ ЇЇ ОПТИМІЗАЦІЇ, РОЗШИРЕННЯ

Комп’ютерна мережа – це сукупність комп’ютерів, які з’єднані лініями зв’язку і оснащені комунікаційним обладнанням та комунікаційним програмним забезпеченням [1]. Комп'ютерні мережі є важливою частиною інфраструктури компанії, оскільки вони забезпечують ефективне функціонування бізнес-процесів, дають змогу здійснювати комунікацію та обмін інформацією між співробітниками, а також сприяють розвитку нових можливостей для бізнесу.

Основними елементами корпоративної комп'ютерної мережі є такі:

– фізичні компоненти включають у себе кабелі, мережеве обладнання (наприклад, комутатори, маршрутизатори, точки доступу) і комп'ютери;

– програмні компоненти включають операційні системи, мережеві протоколи та програмне забезпечення для управління мережею.

Залежно від масштабу підприємства комп'ютерні мережі можуть бути локальними (LAN), регіональними (MAN) або глобальними (WAN).

– локальні обчислювальні мережі (LAN) об'єднують комп'ютери в одному місці, наприклад, в одному офісі, на заводі або складі;

– регіональні мережі (MAN) об'єднують комп'ютери, розташовані в межах одного регіону, наприклад, міста або провінції;

– глобальні мережі (WAN) об'єднують комп'ютери, розташовані в різних країнах або на різних континентах.

Оптимізація комп'ютерної мережі компанії - це комплекс заходів, спрямованих на підвищення ефективності її роботи. Оптимізація включає в себе такі заходи:

– фізичне вдосконалення мережі. Наприклад, заміна застарілих кабелів на сучасні або перепроектування кабельної системи для підвищення продуктивності;

– програмне вдосконалення мережі, наприклад, оновлення операційних систем і мережевих протоколів, встановлення нового програмного забезпечення для управління мережею;

– удосконалення політики безпеки, наприклад, введення нових заходів щодо запобігання несанкціонованому доступу до мережі.

Оптимізація комп'ютерної мережі підприємства має такі позитивні результати:

– підвищення продуктивності мережі: фізична оптимізація мережі, наприклад, заміна застарілих кабелів на сучасні або перепроєктування кабельної системи, дає змогу значно збільшити пропускну спроможність мережі та знизити час затримки;

– програмна оптимізація мережі, наприклад, оновлення операційних систем і мережевих протоколів, а також установлення нового програмного забезпечення для управління мережею, дає змогу підвищити продуктивність мережі завдяки збільшенню ефективності використання ресурсів і безпеки;

– підвищення рівня безпеки мережі: впровадження нових заходів мережевої безпеки, таких як фільтрація пакетів, виявлення вторгнень і шифрування даних, дає змогу істотно знизити ризик виникнення інцидентів безпеки;

– зниження витрат на обслуговування мережі: оптимізація фізичної мережі, наприклад, заміна застарілих кабелів на сучасні або перепроєктування кабельної системи, дає змогу зменшити кількість проблем, пов'язаних із пошкодженням кабелів, і знизити витрати на обслуговування мережі.

Розширення комп'ютерної мережі компанії може знадобитися при її зростанні, розширенні діяльності або впровадженні нових технологій. Розширення може включати в себе такі дії, як:

– додавання нових фізичних компонентів, наприклад, прокладання додаткових кабелів, встановлення нових мережевих пристроїв або придбання нових комп'ютерів;

– встановлення нових програмних компонентів, наприклад, оновлення операційних систем або мережевих протоколів, а також установлення нового програмного забезпечення для управління мережею;

– удосконалення політики безпеки, наприклад, введення нових заходів щодо захисту від несанкціонованого доступу до мережі.

Розширення мережі може забезпечити доступ до неї нових користувачів і пристроїв або збільшити пропускну здатність мережі для задоволення зростаючих потреб у передачі даних.

Під час розширення комп'ютерної мережі компанії необхідно враховувати такі чинники

– топологія мережі визначає, як з'єднані комп'ютери в мережі. Під час розширення мережі слід вибирати топологію, що відповідає потребам підприємства;

– пропускна здатність мережі визначає максимальну швидкість передавання даних мережею. Під час розширення мережі необхідно

переконатися, що пропускна здатність мережі відповідає потребам підприємства;

– характеристики фізичного середовища: при розширенні мережі необхідно враховувати фізичне середовище, в якому вона встановлена. Наприклад, якщо мережу планується встановити в будівлі з великою кількістю перегородок, то може знадобитися використання кабелів з більшою довжиною хвилі.

Розширення комп'ютерної мережі підприємства може мати ряд позитивних наслідків, як для самого підприємства, так і для його працівників. До основних позитивів можна віднести:

– підвищення продуктивності праці: це дозволяє працівникам більш ефективно обмінюватися інформацією та ресурсами, що може призвести до зниження витрат часу та підвищення ефективності робочих процесів;

– покращення комунікації: це дозволяє працівникам спілкуватися один з одним незалежно від їхнього фізичного розташування. Це може сприяти підвищенню ефективності командної роботи та покращенню взаєморозуміння між працівниками;

– розширення можливостей: розширена мережа дозволяє підприємству використовувати нові технології та послуги, що може призвести до розширення його можливостей та підвищення конкурентоспроможності;

– покращення безпеки: розширена мережа може бути більш безпечною, ніж ізольована мережа. Це пов'язано з тим, що розширена мережа може використовувати більш передові засоби безпеки, такі як брандмауери та антивірусні програми.

Отже, оптимізація і розширення комп'ютерної мережі компанії - складне завдання, що вимагає залучення кваліфікованих фахівців. Для успішного вирішення цих завдань необхідно провести ретельний аналіз потреб компанії і розробити план дій, що враховує всі необхідні фактори. Комп'ютерні мережі є необхідним елементом інфраструктури сучасних підприємств, забезпечуючи ефективну комунікацію та обмін інформацією. Оптимізація та розширення цих мереж покращують продуктивність, комунікацію та безпеку, роблячи їх ключовими факторами успіху підприємства.

Список використаних джерел:

1. Комп’ютерні мережі URL: https://km.ptngu.com/lections/2.html (дата звернення 11.09.2023)

Коряк Владислав, здобувач СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к. с.-г. н., доцент Протас Надія

ЗАСОБИ ДІАГНОСТИКИ ПІДКЛЮЧЕННЯ ДО МЕРЕЖІ ІНТЕРНЕТ

Мережа Інтернет є одним з основних інструментів для роботи, навчання та спілкування в сучасному світі. Вона дозволяє організаціям обмінюватися інформацією, співпрацювати з партнерами та клієнтами, а також надавати послуги клієнтам.

Від якості підключення до мережі Інтернет залежить ефективність роботи організації, її конкурентоспроможність та репутація. Якщо підключення до мережі Інтернет нестабільно або не працює належним чином, це може призвести до таких проблем, як:

– зниження продуктивності праці;

– втрата даних;

– порушення роботи програмного забезпечення;

– зниження рівня обслуговування клієнтів;

– узагальнення теоретичних знань та практичних навичок.

Під час виробничої практики було отримано теоретичні знання та практичні навички з діагностики підключення до мережі Інтернет. Було вивчено основні поняття, пов'язані з діагностикою мережі, а також методи проведення діагностики.

Основні поняття, пов'язані з діагностикою мережі, включають:

– налаштування мережі;

– швидкість і якість підключення;

– помилки і збої.

Методи проведення діагностики мережі включають:

– аналіз налаштувань мережі;

– тестування швидкості і якості підключення;

– перевірка на наявність помилок і збоїв.

На базі підприємства ВК АГРО було проведено діагностику підключення до мережі Інтернет. Було використано наступні методи та інструменти (рисунок 1) [1]:

1. Аналіз налаштувань мережі:

– Перевірка IP-адреси, маски підмережі, шлюзу, DNS-сервера;

2. Тестування швидкості і якості підключення:

– Speedtest.net;

– Pingdom;

3. Перевірка на наявність помилок і збоїв:

– Nmap

– Wireshark

В результаті діагностики було виявлено, що мережа Інтернет на підприємстві ВК АГРО працює стабільно, але на одному з робочих місць була виявлена помилка в налаштуванні IP-адреси. Це могло викликати проблеми з доступом до мережі Інтернет.

Для підвищення ефективності діагностики підключення до мережі Інтернет на підприємстві ВК АГРО рекомендується:

1. Розробити план проведення регулярних діагностик мережі.

– План повинен передбачати проведення діагностики не рідше одного разу на квартал.

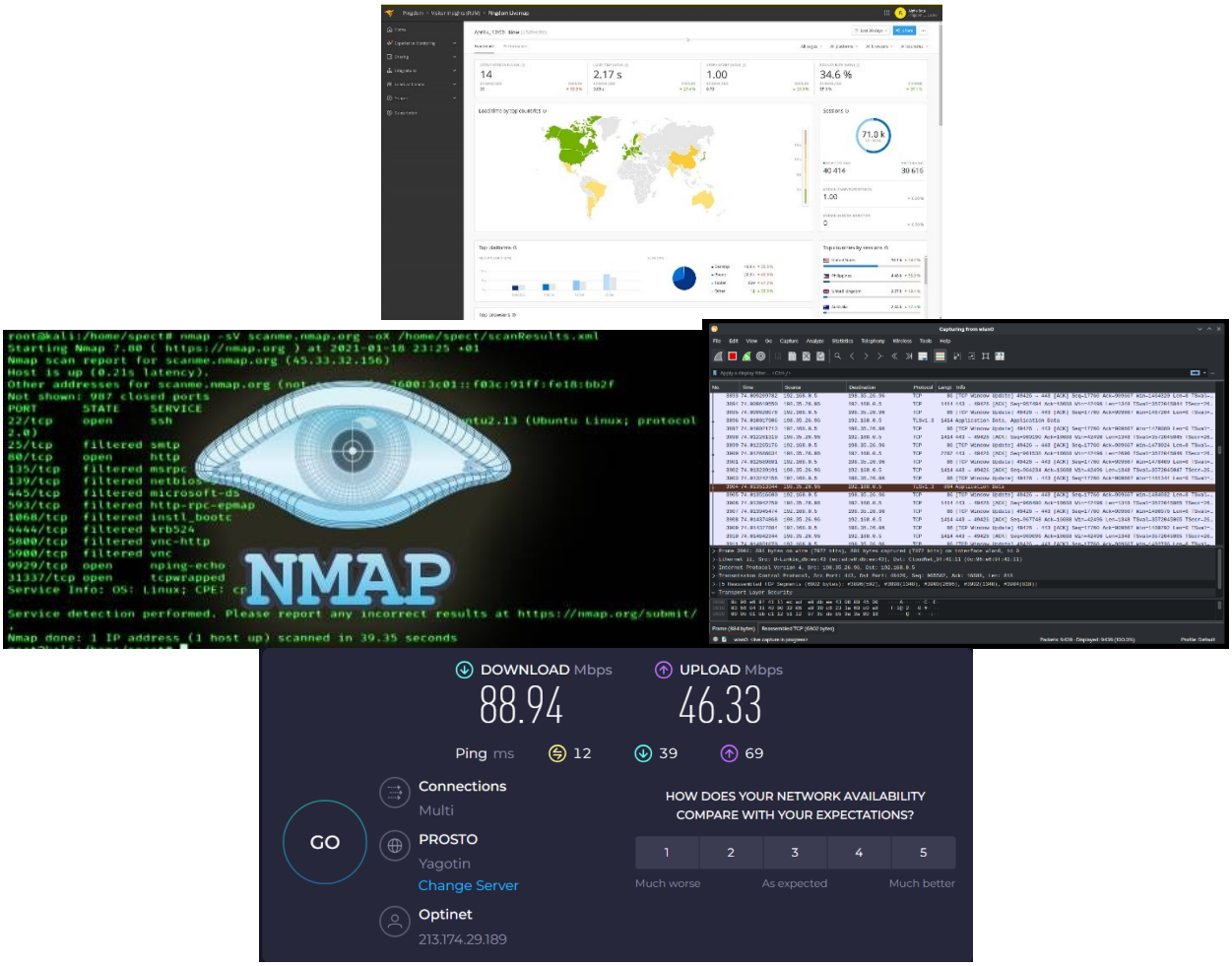

Рисунок 1 – Інтерфейс інструментів якими було проведено діагностику підключення до мережі Інтернет

2. Навчати працівників компанії основам діагностики мережі.

– Навчання можна проводити у вигляді навчальних курсів або семінарів.

3. Запровадити систему моніторингу мережі для виявлення проблем на ранніх стадіях.

– Система моніторингу може включати в себе такі інструменти, як (рисунок 2) [2]:

1) SNMP;

2) Nagios;

3) Icinga;

Для більшої інформативності тези можна доповнити інформацією про конкретні методи та інструменти, які використовувалися для проведення діагностики.

Так, можна навести приклади використання конкретного інструменту для виявлення конкретної проблеми. Наприклад, можна сказати, що для виявлення помилки в налаштуванні IP-адреси було використано інструмент Nmap.

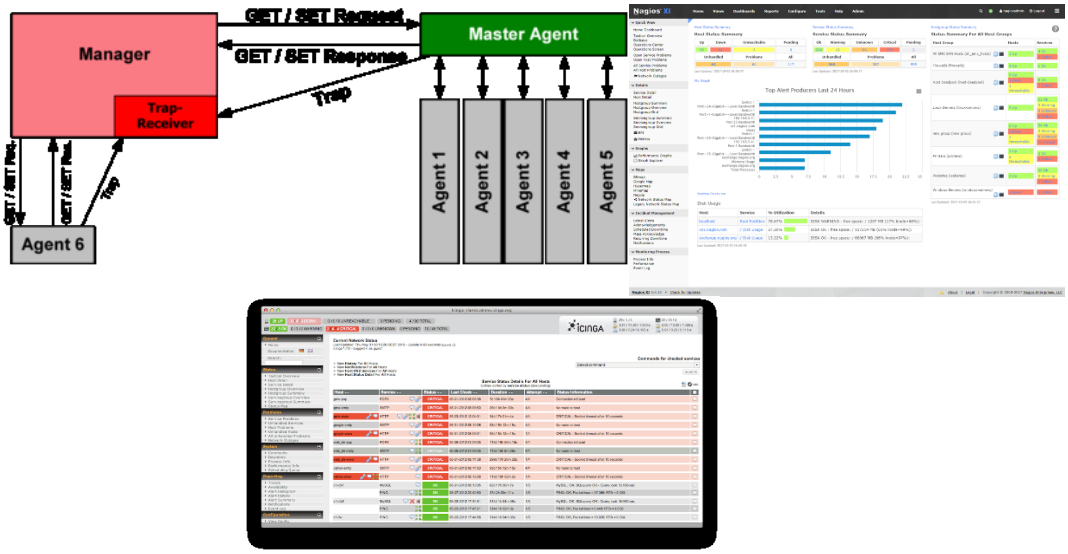

Рисунок 2 – Інструменти системи моніторингу

Також можна навести конкретні приклади проблем, які були виявлені в результаті діагностики. Наприклад, можна сказати, що в результаті діагностики було виявлено, що на одному з робочих місць IP-адреса була налаштована неправильно. Це призвело до того, що робоче місце не могло підключитися до мережі Інтернет.

Висновки та пропозиції можна доповнити рекомендаціями щодо вдосконалення системи діагностики підключення до мережі Інтернет на підприємстві ВК АГРО.

Наприклад, можна запропонувати використовувати більш сучасні інструменти для проведення діагностики, такі як (рисунок 3) [3]:

– Prometheus;

– Grafana;

Рисунок 3 – Інтерфейс сучасних інструментів для проведення діагностики

Також можна запропонувати автоматизувати процес проведення діагностики, щоб він був більш ефективним і економічним.

Список використаних джерел:

1. Діагностика інтернет-з'єднання URL: http://hi-news.pp.ua/kompyuteri/13737-dagnostika-nternet-zyednannya-sposobi-varanti.html

2. Інструмент моніторингу URL: https://czo.gov.ua/tool#:~:text
3. Записки програміста URL: https://eax.me/prometheus-and-grafana/

Масич Андрій, здобувач вищої освіти СВО «Бакалавр»
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ФІЗИЧНЕ СЕРЕДОВИЩЕ ПЕРЕДАЧІ ДАНИХ КОМП'ЮТЕРНОЇ МЕРЕЖІ (ХАРАКТЕРИСТИКИ КАНАЛІВ ЗВ'ЯЗКУ, ТИП КАБЕЛЮ, ЯКЩО У ЯКОСТІ НОСІЯ ВИКОРИСТОВУЄТЬСЯ КАБЕЛЬ)

Фізичне середовище передачі даних в комп'ютерних мережах включає провідні та безпровідні засоби передачі сигналів (провідні мережі використовують кабелі для цього). В мережах використовуються різні типи кабелів:

- коаксіальний кабель;
- вита пара;
- волокно-оптичний кабель.

Також існують безпровідні мережі.

Вибір фізичного середовища для комп'ютерної мережі залежить від багатьох факторів, таких як відстань між комп'ютерами, кількість комп'ютерів у мережі, швидкість передачі даних, яка потрібна, і бюджет.

Коаксіальний кабель - це вид кабелю для передачі даних, який має центральний провідник, що оточений ізоляційним шаром, а потім екраном. Екран може бути виготовлений з міді або алюмінію. Цей тип кабелю застосовується у різних мережах, таких як Ethernet, Token Ring та ARCNET. Він має декілька переваг, зокрема здатність передавати дані на великі відстані з високою швидкістю та стійкість до перешкод, що робить його популярним у вимогливих умовах [1]. Однак, у нього також є певні недоліки, такі як вартість та складність монтажу. Крім того, його може пошкодити гостре лезо.

Коаксіальний кабель продовжує застосовуватися в спеціалізованих областях та застарілих системах. Однак у сучасних мережах він все частіше витісняється більш передовими технологіями передачі даних, такими як волокно-оптичний кабель та бездротові з'єднання.

Вита пара – це тип кабелю для передачі даних, складається з двох провідників, які скручуються навколо один одного. Цей тип кабелю використовується в різних мережевих системах, включаючи Ethernet, Token Ring і ARCNET. Вита пара має свої переваги порівняно з іншими видами кабелів. Вона є більш доступною за вартістю, її легше встановлювати. Вита пара також володіє стійкістю до перешкод і може працювати в надзвичайних умовах. Проте у витої пари є й недоліки. Вона не може передавати дані на такі далекі відстані, як коаксіальний кабель, і менш стійка до перешкод, ніж оптичний кабель [2].

Попри свої недоліки, вита пара продовжує залишатися популярним вибором для багатьох типів мереж, зокрема локальних мереж (LAN),

домашніх та офісних мереж [2]. Вита пара постійно піддавалася технологічним вдосконаленням, що дозволяє досягати вищих швидкостей передачі даних та покращувати ефективність мережі.

Волокно-оптичний кабель – це тип кабелю, який використовується для передачі даних за допомогою світла. Він складається з центрального волокна з діелектрика, яке оточене шаром ізоляції, а потім шаром оболонки. Волокно-оптичний кабель може використовуватися для передачі даних на великі відстані з дуже високою швидкістю [3].

Волокно-оптичний кабель має певні переваги:

– висока швидкість передачі даних;

– велика відстань передачі даних;

– висока стійкість до перешкод, включаючи електромагнітні впливи і інші зовнішні впливи;

– можливість використання в жорстких умовах, таких як висока вологість, екстремальна температура та хімічна активність.

Також є деякі недоліки оптоволоконного кабелю:

– вартість виготовлення та установки може бути високою порівняно з іншими типами кабелів;

– складність монтажу та ремонту: спеціалізовані знання та обладнання можуть бути потрібні для належної установки та обслуговування кабелю;

– можливість пошкодження гострими предметами, зокрема ножами або іншими ріжучими інструментами, що може призвести до втрати сигналу та несправностей.

При виборі між волокно-оптичним кабелем та іншими типами кабелів важливо враховувати потреби мережі, вимоги до пропускної здатності, довжину передачі, надійність та бюджет. Волокно-оптичний кабель є ідеальним вибором для великих підприємств, дата-центрів та довгих дистанцій передачі даних, де надійність та швидкість мають вирішальне значення.

Бездротове середовище передачі даних – це середовище, яке використовується для передачі даних за допомогою радіохвиль. Бездротові мережі можуть використовуватися для передачі даних на короткі відстані або на великі відстані, залежно від типу бездротової мережі [4].

Самими поширеними типами безпровідних мереж є:

– Wi-Fi – найпоширеніший тип бездротової мережі. Wi-Fi мережі використовують радіохвилі для передачі даних на короткі відстані;

– Bluetooth – тип бездротової мережі, що використовується для передачі даних на короткі відстані, наприклад, між комп'ютером і принтером;

– ZigBee – тип бездротової мережі, що використовується для передачі даних на короткі відстані, наприклад, в системах автоматизації будинків.

Бездротові мережі мають ряд переваг у порівнянні з провідними мережами. Вони не потребують прокладки кабелів, що робить їх більш мобільними і зручними в установці. Бездротові мережі також можуть бути використані для передачі даних на великі відстані, якщо використовувати відповідне обладнання. Однак бездротові мережі також мають деякі недоліки.

Вони можуть бути більш уразливими до перешкод, ніж провідні мережі. Бездротові мережі також можуть бути менш безпечними, оскільки дані можуть бути перехоплені сторонніми особами [4].

В наш час найбільш високоактуальним типом кабелю для передачі даних є вита пара. Вона володіє рядом значних переваг, серед яких важливе місце посідає її низька вартість, легкість монтажу та висока стійкість до різноманітних перешкод. Вита пара використовується з успіхом у різних типах мереж, зокрема в локальних мережах (LAN), а також у домашніх та офісних середовищах.

Коаксіальний кабель натомість поступово починає відступати перед більш сучасними технологіями, такими як волокно-оптичні кабелі та бездротові з'єднання. Звичайно, слід відзначити високу швидкість передачі даних та надійність коаксіального кабелю, проте він також вважається дорогим у застосуванні та вимагає певних навичок для монтажу.

Волокно-оптичні кабелі мають найвищі показники швидкості передачі даних і непохитну стійкість до різних видів перешкод. Тут варто підкреслити, що вартість таких кабелів є однією з найвищих, а монтаж вимагає спеціалізованих знань. Вони найчастіше застосовуються в великих підприємствах, дата-центрах та системах, де вирішальну роль відіграють надійність і висока швидкість передачі даних.

Бездротові з'єднання є найзручнішим і найбільш мобільним способом передачі даних. Вони виключають потребу прокладати фізичні кабелі, забезпечуючи доступність з'єднань в будь-якому місці. Проте варто враховувати, що бездротові з'єднання можуть бути менш надійними з точки зору безпеки порівняно з провідними мережами.

Отже, на цей момент вита пара є найпопулярнішим кабелем для передачі даних. Її характеристики сприяють забезпеченню вигідного балансу між вартістю, простотою монтажу та функціональними можливостями.

Список використаних джерел:

1. Van der Burgt, Martin J. "Coaxial Cables and Applications" (PDF). Belden. p. 4. URL: http://www.belden.com/pdfs/Techpprs/CoaxialCablesandApplications.pdf
2. Олифер В. Г., Олифер Н. А. Глава 13. Коммутируемые сети Ethernet // Компьютерные сети. Принципы, технологии, протоколы. 4-е изд. СПб.:Питер, 2010. С. 438. 450 URL: https://www.bsuir.by/m/12_100229_1_85460.pdf
3. Posinna, Mariddetta (April 1, 2014). "different types of fiber optic cables". HFCL. Archived from the original on April 20, 2016. URL: https://hfcl.com
4. Буров, Євген Вікторович. Комп'ютерні мережі / Є. Буров; За ред. В. Пасічника. 2-е вид, оновлене і доп. Львів : БаК, 2003. 584 с. URL: https://www.wikidata.uk-ua.nina.az/Бездротова_мережа.html

Москаленко Ілля, здобувач вищої освіти СВО Бакалавр
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.ф.-м.н., доцент Копішинська Олена

ПЛАНУВАННЯ МОДЕРНІЗАЦІЇ МЕРЕЖЕВИХ ПРИСТРОЇВ І ОПЕРАЦІЙНИХ СИСТЕМ ПРОГРАМНО-КОНФІГУРУЮЧИХ КОМУНІКАЦІЙНИХ СИСТЕМ

Модернізація мережевих пристроїв і операційних систем програмно-конфігуруючих комунікаційних систем означає впровадження новітніх технологій, оновлення апаратного забезпечення та операційних систем з метою покращення функціональності, ефективності, безпеки та масштабованості комунікаційних мереж.

Планування є складним і важливим процесом для забезпечення ефективності, безпеки і розвитку мережі.

– Аналіз потреб і вимог: Перший крок у плануванні - це ретельний аналіз поточних і майбутніх потреб мережі та вимог користувачів. Це допоможе визначити, які конкретні зміни потрібні для модернізації.Включає в себе збір даних про поточну мережу, консультації с користувачами, аналіз трафіку, аналіз майбутніх потреб, оцінка бюджету.

– Оцінка поточного стану: Важливо оцінити стан поточних мережевих пристроїв і операційних систем, їх відповідність потребам і безпеці. Це може включати в себе аудит мережі і інвентаризацію обладнання [1].

Планування модернізації мережі.

– Планування бюджету: Визначення бюджету на модернізацію є важливим кроком. Це включає в себе оцінку витрат на нове обладнання, програмне забезпечення та послуги з налаштування.

– Вибір технологій і обладнання: Після визначення потреб і бюджету варто вибрати відповідні технології та мережеве обладнання, які підходять для модернізації.

Під час вибору технологій та обладнання для модернізації мережевої інфраструктури слід враховувати кілька ключових факторів. Деякі з них включають:

1. Сумісність з існуючим обладнанням: Важливо обирати технології та обладнання, які сумісні з існуючою мережевою інфраструктурою, щоб уникнути проблем інтеграції.

2. Масштабованість: Обирайте технології, які можна легко масштабувати для відповіді на зростаючі потреби мережі у майбутньому.

3. Безпека: Обирайте обладнання та технології з найсучаснішими заходами безпеки для захисту мережі від потенційних загроз.

4. Ефективність: Вибирайте технології, які дозволяють досягти більшої ефективності мережі, забезпечуючи високу швидкість передачі даних та мінімальні затримки.

5. Цінова політика: Ретельно оцінюйте вартість обладнання та вартість впровадження нових технологій, щоб підібрати оптимальний варіант, який відповідає фінансовим обмеженням.

6. Технічна підтримка: Оберіть технології та обладнання, які мають надійну технічну підтримку та гарантію, що забезпечить ефективне вирішення можливих проблем.

Розробка графіку і міграційного плану: Створення графіку модернізації і міграційного плану допомагає розподілити процес на етапи та забезпечити мінімальний вплив на продуктивність мережі під час оновлень. Це включає визначення етапів модернізації, планування зв’язків між етапами, визначення термінів завершення, аналіз ризиків і запобігання проблем, перевірка можливості впровадження [1].

Цикл впровадження технологічних змін

– Тестування і валідація: Перед впровадженням необхідно провести тестування нового обладнання та програмного забезпечення, а також валідацію налаштувань для переконливості в їхній працездатності та безпеці.

– Впровадження і налаштування: Після успішного тестування можна проводити впровадження нового обладнання і налаштувань відповідно до міграційного плану.

– Моніторинг і підтримка: Після модернізації необхідно забезпечити постійний моніторинг мережі і підтримку, щоб виявляти і вирішувати можливі проблеми [1].

ІТ-управління та обслуговування

– Документація і навчання персоналу: Важливо створити документацію щодо нових налаштувань та процесів, а також навчити персонал користуватися новим обладнанням і операційними системами.

– Постійна модернізація: Модернізація мережі - це процес, який триває впродовж часу. Важливо регулярно переглядати і оновлювати мережеві ресурси для забезпечення їхньої актуальності і ефективності.

– Резервне копіювання і відновлення: Важливо розробити план для резервного копіювання даних і конфігурацій перед модернізацією, а також процедури відновлення в разі непередбачених проблем [1-2].

Стратегічне планування і керування

– Управління змінами і комунікація: Забезпечення ефективного управління змінами, а також чіткої комунікації зі всіма стейкхолдерами, включаючи персонал, є важливою частиною процесу модернізації.

– Склад та кваліфікація персоналу: Визначення, які знання та навички потрібні персоналу для підтримки і керування новим обладнанням і операційними системами. Склад персоналу повинен включати такі професійні спеціалізації:

– Мережний адміністратор: Людина, яка відповідає за налаштування, керування та підтримку мережевої інфраструктури.

– Системний адміністратор: Особа, яка забезпечує ефективну роботу операційних систем та допомагає в усуненні проблем, пов'язаних з серверами та програмним забезпеченням.

– Інженер з безпеки мережі: Фахівець, який відповідає за забезпечення безпеки мережі, виявлення потенційних загроз та впровадження заходів безпеки.

– Архітектор мережі: Особа, відповідальна за розробку стратегії мережі та її майбутній розвиток.

– Спеціаліст з програмної конфігурації мережі: Експерт, який володіє навичками програмування та налаштування мережевих пристроїв.

– Технічний підтримка: Команда, яка забезпечує технічну підтримку користувачам та вирішує питання, пов'язані з використанням мережевих пристроїв та операційних систем.

– Аналіз ризиків і розробка плану невдалого випробування: Врахування можливих ризиків і розробка стратегії для вирішення проблем, які можуть виникнути під час модернізації [1-2].

Стратегічне управління

– Метрики та вимірювання успішності: Визначення ключових метрик та параметрів, які слід вимірювати для оцінки успішності модернізації. Результативність модернізації мережевої інфраструктури можна вимірювати через пропускну здатність мережі, час відновлення в разі збоїв, показники безпеки та ефективність використання ресурсів. Ці метрики дозволяють оцінити ефективність впроваджених змін та визначити відповідність нової інфраструктури вимогам бізнесу та користувачів.

– Врахування майбутніх технологій і трендів: Забезпечення сумісності інфраструктури з майбутніми технологічними змінами і трендами в індустрії.

– Забезпечення сумісності і інтеграції: Важливо переконатися, що нове обладнання і операційні системи можуть інтегруватися з існуючими ресурсами і додатками.

– Поетапна модернізація: Розгляд можливості поетапної модернізації для зниження ризиків та забезпечення неперервності роботи мережі.

Поетапна модернізація мережевої інфраструктури передбачає впровадження змін етапами з мінімальним впливом на загальну продуктивність мережі. Деякі ключові етапи такої модернізації включають оновлення основних мережевих компонентів, тестування нових технологій в обмеженому середовищі, адаптацію нових протоколів безпеки та масштабованості, а також поетапне впровадження нових функцій і можливостей, враховуючи потреби бізнесу та користувачів. Планування модернізації мережевих пристроїв і операційних систем вимагає систематичного і стратегічного підходу для забезпечення успішного розвитку мережі відповідно до потреб організації [1].

Отже, що ефективне планування модернізації мережевих пристроїв і операційних систем є критичним для забезпечення ефективності, безпеки та стійкості мережі. Враховуючи всі аспекти, такі як аналіз потреб, оцінка поточного стану, планування бюджету, вибір технологій, етапи впровадження та стратегічне управління, організація може досягти успішної модернізації мережі. Постійне моніторинг та підтримка після впровадження є так само

важливими, а також врахування майбутніх технологічних трендів для забезпечення сталого розвитку мережі. Ретельне дотримання кроків планування та управління ризиками дозволить ефективно впроваджувати і підтримувати сучасні мережеві інфраструктури, що відповідають потребам організації у нинішньому конкурентному цифровому середовищі.

Список використаних джерел:

1. Телекомунікайні та інформаційні мережі https://ktpu.kpi.ua/wp-content/uploads/2014/02/Vorobiyenko-P.P.-Telekomunikatsijni-ta-informatsijni-merezhi.pdf
2. Бехроуз, А., Фороузан (2006) Передача даних і мереж (McGraw-Hill Forouzan Networking). Видавництво “MC GRAW HILL INDIA”

Ціпановська Дар'я, здобувач СВО Бакалавр,
спеціальність 126 Інфрмаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ

Сьогоднішні підприємства, установи та організації все більше опираються на інформаційні технології, комп'ютеризовані системи та електронні бази даних. Це особливо актуально для сфер, де важлива збереженість конфіденційності, надійність та цілісність інформації, таких як фінансові установи, медичні заклади, промислові компанії та інші.

Зростаюча кількість кібератак, вірусів та інших загроз кібербезпеці створює великі виклики для підприємств у забезпеченні безпеки та захисту інформації. Навіть один незаконний доступ до конфіденційних даних чи їх витік може призвести до серйозних фінансових збитків, підірвати довіру клієнтів і негативно вплинути на репутацію компанії.

Обрана проблематика :

В контексті мого дослідження була обрана тема "Системи інформаційної безпеки на підприємстві, установі, організації". Основною ціллю проведеного дослідження було вивчення поточного стану систем інформаційної безпеки на обраному підприємстві з метою виявлення можливих вразливостей та недоліків. Подальшою метою було розробити ефективні заходи для підвищення рівня безпеки даних. Дослідження включало аналіз наявних заходів та технологій інформаційної безпеки, дослідження методів виявлення та запобігання кібератак, а також огляд структури та організації інформаційного забезпечення підприємства. Для досягнення поставленої мети дослідження було використано широкий спектр джерел інформації, включаючи наукову літературу, статистичні дані, внутрішню документацію підприємства, інтерв'ю з експертами у галузі інформаційної безпеки, а також мої власні спостереження.

Проведене дослідження дало можливість зробити висновки щодо поточного стану інформаційної безпеки на підприємстві, виявити основні ризики та загрози, а також надати рекомендації та заходи для покращення рівня безпеки даних та інформаційної інфраструктури. Під час проведення аналізу систем інформаційної безпеки на підприємстві, були отримані значущі теоретичні знання та практичні вміння, що допомогли глибше розуміти та досліджувати аспекти цієї теми.

Основною фокусною точкою мого дослідження був аналіз наявних систем інформаційної безпеки на підприємстві з метою відшукати потенційні ризики та слабкі місця. Для досягнення цієї мети, я вивчав наукові ресурси та літературні джерела, що стосуються кібербезпеки, методів захисту від кібератак, заходів для забезпечення безпеки даних та інших ключових аспектів інформаційної безпеки.

Крім цього, був проведений аналіз структури та організації інформаційного забезпечення на підприємстві. Це включало вивчення систем зберігання даних, методів обробки інформації та механізмів контролю доступу. Для цього була використана внутрішня документація підприємства, проведені інтерв'ю з інформаційними безпеки та адміністраторами систем.

Протягом дослідження також застосовувались різні методи аналізу, включаючи SWOT-аналіз, оцінку ризиків та загроз, оцінку вразливостей систем. Ці методи дозволили ідентифікувати основні проблемні аспекти в інформаційній безпеці підприємства і розробити стратегічний план заходів для їх вирішення та подальшого покращення.

Відповідно до отриманих результатів, були зроблені висновки про поточний стан інформаційної безпеки на підприємстві та ідентифіковані ключові ризики та загрози, що можуть вплинути на цю сферу. Також були розроблені рекомендації та практичні кроки для покращення наявних систем інформаційної безпеки та запобігання можливим кібератакам. Внаслідок цього дослідження систем інформаційної безпеки на підприємстві, були отримані значущі теоретичні знання та корисні практичні навички в галузі інформаційної безпеки, що буде сприяти подальшому професійному зростанню та розвитку в цьому напрямку.

Після завершення дослідження систем інформаційної безпеки на підприємстві, зроблено наступні висновки:

Актуальність проблеми: Зі зростанням кількості кіберзагроз та шкідливого програмного забезпечення системи інформаційної безпеки набувають визначальної ролі у забезпеченні захисту даних та надійного функціонування підприємств. Забезпечення інформаційної безпеки стає основним пріоритетом для бізнесу, організацій та установ, оскільки це необхідно для успішної діяльності та уникнення можливих загроз.

Ключовими аспектами інформаційної безпеки, виявленими під час дослідження, є ефективний захист від несанкціонованого доступу, запобігання кібератакам, забезпечення безпеки мережі та обов'язковий захист важливої інформації. Також важливим є своєчасне виявлення та реагування на інциденти кібербезпеки.

Рекомендації для підвищення рівня безпеки: Для забезпечення надійного захисту інформаційної безпеки на підприємстві, рекомендую впроваджувати мультифакторну автентифікацію, регулярно оновлювати програмне забезпечення та використовувати ефективні антивірусні програми.[1]

Додатково, важливо забезпечувати належну підготовку та навчання працівників з питань кібербезпеки, щоб уникнути соціального інжинірингу та інших атак, що використовують людський факторів. Важливість стратегічного планування в умовах кризових ситуацій: Системи інформаційної безпеки повинні мати чіткий план дій для реагування на кризовій ситуації, такі як кібератаки, витоки інформації або системні збої. Регулярні тренування та практикування заходів зі збереження даних сприятимуть тому, щоб підприємство ефективно реагувало на негативні події та зменшувало їх вплив на свою діяльність.

Постійне оновлення та вдосконалення: Інформаційні технології та кіберзагрози постійно розвиваються, тому важливо постійно оновлювати та вдосконалювати системи інформаційної безпеки.[2]

Пропозиції:

Впровадження мультифакторної автентифікації: Рекомендовано впровадити мультифакторну автентифікацію для всіх облікових записів співробітників та адміністраторів систем на вашому підприємстві. Цей захід значно підвищить рівень безпеки, оскільки для входу в систему буде необхідно підтвердження через додатковий фактор, такий як SMS-повідомлення, спеціальна аплікація для генерації одноразових кодів або відбиток пальця.

Також, важливим є регулярне оновлення програмного забезпечення та антивірусів. Встановіть систему автоматичного оновлення операційних систем, програмного забезпечення та антивірусних програм на всіх комп'ютерах та серверах. Це дозволить запобігти використанню застарілих та вразливих версій програм і забезпечить належний рівень захисту.

Забезпечення резервного копіювання та можливості відновлення даних: Реалізація систематичного створення резервних копій даних та впровадження плану тестового відновлення може суттєво зменшити ризик втрати даних у випадку надзвичайних ситуацій або кібератак. Наша рекомендація - зберігати резервні копії на відокремлених фізичних носіях або в надійних хмарних сервісах з надійним рівнем захисту.

Керування доступом та правами: Реалізувати жорсткий контроль над правами доступу до різних рівнів інформації та ресурсів. Дозволити користувачам лише необхідні права, що відповідають їхнім завданням. Застосовувати групові політики та норми для гарантування обмеженого доступу до конфіденційних даних.

Організація навчання в галузі кібербезпеки: Проводити періодичні тренінги та навчання для працівників з питань кібербезпеки. Викладати загрози та навчати персонал впізнавати фішингові атаки, соціальний інжиніринг та інші методи кіберзлочинців. Інформовані та підготовлені

співробітники зможуть уникнути багатьох небезпек та вчасно реагувати на підозрілі ситуації.

Список використаних джерел:

1. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 05.07.2016 № 80-VIII.
2. Зарембо Є. В. Комп'ютерна безпека: підручник / Є. В. Зарембо, В. П. Линда, І. В. Максимчук та ін. – Київ: Центр навчальної літератури, 2021. – 320 с.

Арініч Антон, здобувач вищої освіти СВО Бакалавр,
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ІНТЕРНЕТ-ЗАГРОЗИ ТА ЗАХИСТ ВІД ВІРУСІВ

З огляду на зростаючу кількість загроз у Інтернеті, кібербезпека стає надзвичайно важливою. Захист від вірусів, спаму та шкідливих програм є невід'ємною частиною безпеки для організацій та користувачів.

Зі зростанням часу кіберзагрози стають все більш складними, тому необхідно постійно оновлювати і вдосконалювати методи захисту. Одним з ключових підходів є впровадження нових технологій та методик для виявлення і захисту від загроз. Це означає використання штучного інтелекту та машинного навчання для розпізнавання неприродної поведінки та атак [1].

Одна з найбільших загроз полягає у соціальній інженерії, коли зловмисники намагаються обманути користувачів та отримати доступ до їх облікових записів. На практиці це може включати фішинг, шахрайство через електронну пошту та інші маніпуляції. Важливо тренувати співробітників у використанню навичок соціальної інженерії для розпізнавання подозрюваних ситуацій та захисту конфеденційної інформації.

Для забезпечення більшої безпеки важливо активно відслідковувати та аналізувати попередні інциденти. Це допомагає виявити шаблони атак і покращити заходи безпеки у майбутньому. Важливо також створити систему реєстрації та звітування про події, а також розглядати їх при аналізі та плануванні кроків у сфері кібербезпеки [2].

Важливо регулярно створювати копії важливої інформації та даних, щоб мати можливість відновити їх у разі атаки або непередбаченого інциденту. Збереження цих копій на окремих серверах або в хмарних системах допомагає забезпечити доступ до даних у будь-який момент.

Важливо мати доступ до експертів з кібербезпеки або здійснювати аудит безпеки системи з час від часу. Експерти можуть надати цінні рекомендації та виявити потенційні проблеми, які можуть бути незрозумілими для звичайних користувачів.

Забезпечення безпеки від вірусів, недозволених електронних листів та шкідливих програм є складною задачею, яка потребує постійного вдосконалення та використання спеціалізованих інструментів. Робота у цьому

напрямку передбачає регулярне оновлення та навчання персоналу правилам кібербезпеки [3].

Дослідження підкреслюють необхідність посилення заходів з кібербезпеки та постійного оновлення захисту від вірусів та інших загроз. Запропоновано розвивати освіту в цій галузі та використовувати спеціалізовані засоби для захисту від кіберзагроз.

Список використаних джерел:

1. Богуш В.М., Основи кіберпростору, кібербезпеки та кіберзахисту. навчальний посібник, 2021. 554 с.
2. Гапак О.М., Балога С.І. Захист інформації в комп'ютерних системах : підручник. Ужгород : ПП АУТДОР-ШАРК, 2021. 184 с
3. Остапов С.Е., Євсеєв С.П. , Король О.Г. Кібербезпека: сучасні. технології захисту. Київ: Новий світ, 2020. 678 с.

Базилєв Владислав здобувач вищої освіти СВО «Бакалавр»
Спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ЗАХИСТ І ОБРОБКА КОНФІДЕНЦІЙНИХ ДОКУМЕНТІВ НА ПІДПРИЄМСТВІ

На підприємстві "Полтававодоканал" захист і обробка конфіденційних документів є надзвичайно важливою складовою діяльності, оскільки вони містять важливу інформацію щодо фінансових, технічних, організаційних та інших аспектів підприємства[1]. Основні методи та процедури захисту документів:

Фізичний захист - включає контроль доступу до приміщень та зберігання документів в сейфах або інших захищених місцях. Застосовуються системи контролю доступу, такі як карти доступу та біометричні системи.

Електронний захист - конфіденційні електронні документи повинні бути захищені за допомогою паролів, шифрування та систем контролю доступу. Використання антивірусного та антиспамного програмного забезпечення також важливо для захисту від шкідливих програм.

Мережевий захист - захист мережі від несанкціонованого доступу із зовнішніх джерел є критичним. Використовуються брандмауери, VPN та інші засоби для захисту мережі та обміну конфіденційними даними.

Методи обробки конфіденційних документів:

Класифікація та маркування - кожен конфіденційний документ повинен бути правильно класифікований залежно від його важливості та конфіденційності. Класифікація документів допомагає визначити, хто має право доступу до них і як вони повинні бути оброблені.

Контроль доступу - важливо забезпечити, щоб тільки вповноважені особи мали доступ до конфіденційних документів. Це включає в себе систему "потреби в знаннях," де доступ дається тільки тим, хто дійсно потребує цю інформацію для своєї роботи.

Зберігання та знищення - документи повинні зберігатися в безпечному місці протягом необхідного часу. Після завершення строку зберігання, вони повинні бути належним чином знищені. Зазвичай це робиться шляхом руйнування документів або використання методів безпечного видалення електронних файлів.

Аудит та моніторинг - Наявність системи аудиту та моніторингу дозволяє відстежувати, хто і коли отримував доступ до конфіденційних документів. Це допомагає виявляти будь-які несанкціоновані спроби доступу та вживати необхідні заходи.

Свідомість персоналу:

Навчання - проводьте навчання персоналу з питань захисту та обробки конфіденційних документів.

Заходи безпеки - заохочуйте співробітників дотримуватися правил безпеки при роботі з конфіденційними документами.

Резервне копіювання:

Регулярне резервне копіювання - забезпечуйте регулярне створення резервних копій конфіденційних документів та їх безпечне зберігання.

На підприємстві "Полтававодоканал" обробка та захист конфіденційних документів є надзвичайно важливою функцією, що вимагає постійного удосконалення та дотримання сучасних стандартів безпеки. Правильна обробка та захист документів забезпечує довіру партнерів, клієнтів та ефективне функціонування підприємства.

Список використаних джерел:

1. Заплотинський Б.А. Основи інформаційної безпеки. КІІВіП НУ “ОЮА”, кафедра інформаційно-аналітичної та інноваційної діяльності, 2017. 128 с.

Єфремов Андрій, здобувач вищої освіти СВО Бакалавр,
спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Одарущенко Олена

ЯК СТВОРЮЄТЬСЯ ДИЗАЙН ДЛЯ ВЕБ САЙТУ

Визначення мети веб-сайту є першим і найважливішим кроком у процесі його створення. Ця стадія вимагає глибокого аналізу та ретельного планування, оскільки від неї залежить успішність і ефективність всього проекту. Основна ідея полягає в тому, щоб чітко визначити, які конкретні цілі і завдання має виконувати веб-сайт та який результат очікується від його наявності в Інтернеті.

Дослідження цільової аудиторії в контексті створення веб-сайту відіграє ключову роль у побудові успішної онлайн-платформи. Цей процес передбачає більше, ніж просто збір статистичних даних; він стає фундаментальною основою для створення веб-ресурсу, який зможе взаємодіяти з аудиторією на найвищому[1] рівні. На початку цього процесу проводяться дослідження, спрямовані на збір детальної інформації про цільову аудиторію. Це включає в

себе вивчення їхніх потреб, бажань, проблем і інтересів. Ретельний аналіз демографічних характеристик, таких як вік, стать, освіта, дохід, допомагає створити глибше розуміння того, хто складає вашу аудиторію.

Створення брендової ідентичності для веб-сайту - ключовий і творчий процес. Він включає вибір кольорів, логотипу і графічних елементів для унікального бренду. Основна мета - зробити бренд впізнаваним серед конкурентів. Кольори можуть відображати цінності компанії (наприклад, зелений для екології). Логотип – обличчя[3] бренду, він повинен бути легко впізнаваним і відображати цілісність компанії. Графічні елементи, такі як шрифти і стилізовані зображення, додають характеру індивідуальності (рисунок 1).

Рисунок 1 – Зовнішній вигляд створеного макету

На цьому етапі створюється візуальний макет веб-сайту, який є важливою частиною процесу розробки. Дизайнер ретельно розробляє сторінки, включаючи заголовки, меню, фотографії та текст. Макет відображає вигляд і структуру сайту, дозволяючи замовнику побачити, як виглядатиме кінцевий результат. Основна мета створення макету - візуальна репрезентація ідеї перед фактичною розробкою сайту, що дозволяє виявити та виправити потенційні недоліки у дизайні.

Правильний вибір кольорів і шрифтів - ключовий аспект створення привабливого дизайну. Кольори відображають брендові цінності і настрій веб-сайту[2], а шрифти повинні бути стильними та читабельними. Відповідність кольорів і шрифтів стильової ідентичності важлива для підтримання єдності бренду. Правильний вибір кольорів може підкреслити індивідуальність та надати візуальну ідентичність. Власне, вибір кольорів і шрифтів впливає на перше враження від веб-сайту та взаємодію з аудиторією, визначаючи сприйняття бренду.

На цьому етапі інтенсивно працюють над створенням і розміщенням вмісту, який включає текст і графіку на веб-сайті. Важливо, щоб цей вміст був

логічно розташованим і легко доступним для користувачів. Це включає в себе створення заголовків, підзаголовків, текстових матеріалів, зображень, відео та інших компонентів, які допомагають передати інформацію та взаємодію на сайті. Правильно оформлений вміст полегшує зрозумілість та приваблює відвідувачів, покращуючи їхній досвід і навігацію. Якість контенту на цьому етапі суттєво впливає на сприйняття та взаємодію користувачів з сайтом, що може визначити успіх та репутацію веб-сайту.

Сучасні веб-сайти повинні бути доступні на різних пристроях, включаючи комп'ютери, планшети і смартфони. Для цього використовується респонсивний дизайн, який адаптує вигляд і функціональність сайту під різні пристрої. Це включає адаптацію розміру і розташування елементів для зручної навігації та читабельності на мобільних пристроях. Респонсивний дизайн - ключовий елемент сучасного веб-дизайну, який забезпечує дружній користувацький досвід незалежно від типу пристрою (рисунок 2).

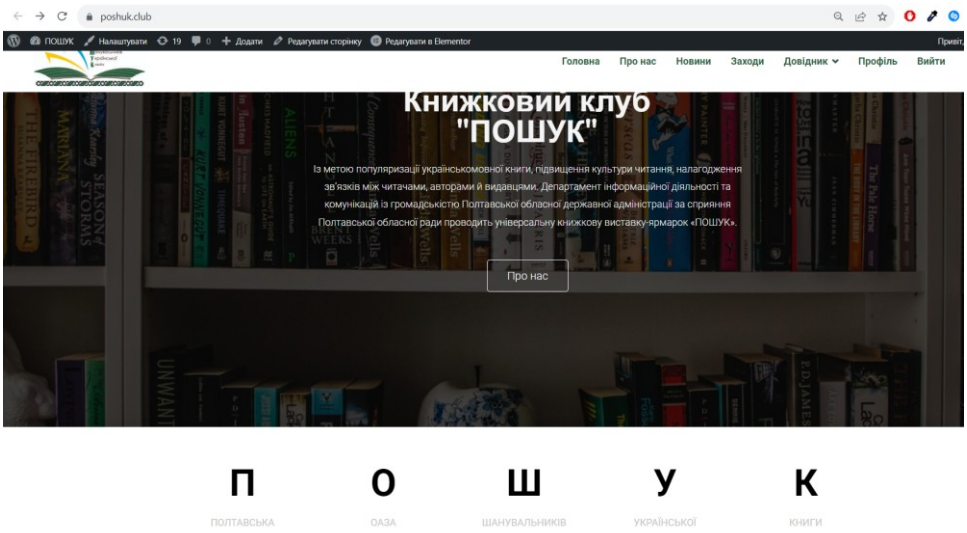

Рисунок 2 – Готовий дизайн

Створення веб-сайту - це комплексний процес, що включає в себе важливі етапи. Визначення мети сайту допомагає встановити чіткі цілі. Дослідження цільової аудиторії надає важливу інформацію про користувачів. Створення ідентичності бренду робить сайт впізнаваним. Розробка макету та вибір кольорів і шрифтів створюють естетичний дизайн. Розміщення контенту та адаптація для різних пристроїв гарантують доступність і зручність. Усі ці кроки спільно допомагають створити успішний та ефективний веб-сайт.

Список використаних джерел:

1. TRIS HUSSEY USING WORDPRESS. Б.М .: QUE, 2012. 425P.

2. CHRIS COYIER, JEFF STARR DIGGING INTO WORDPRESS V3. Б.М .: WORDPRESS, 2012. 442 P.

3. TESSA BLAKELEY SILVER WORDPRESS THEME DESIGN Б.М .: PACT PUBLISHING, 2008. 224 P.

Пасько Денис, здобувач вищої освіти СВО Бакалавр,
Спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Дегтярьова Лариса

ЗАБЕЗПЕЧЕННЯ СВОЄЧАСНОГО КОПІЮВАННЯ, АРХІВУВАННЯ ТА РЕЗЕРВУВАННЯ ДАНИХ Є ЗАПОРУКОЮ НАДІЙНОСТІ ТА БЕЗПЕКИ ІНФОРМАЦІЇ КОМПАНІЇ

Сучасний світ інформаційних технологій призвів до того, що дані стали ключовим активом для бізнесу та організацій. Захист цих даних від втрати, пошкодження та несанкціонованого доступу став однією з найважливіших задач для будь-якої компанії. Забезпечення своєчасного копіювання, архівування та резервування даних - це процеси та практики, спрямовані на забезпечення доступності та надійності інформації в комп'ютерних системах.

Регулярні Резервні Копії: регулярне створення резервних копій важливих даних є основним елементом забезпечення їх безпеки. Це може бути автоматизовано за допомогою спеціалізованого програмного забезпечення для резервного копіювання. Резервні копії можуть бути збережені на локальних серверах або комп'ютерах[1];

Хмарні Резервні Копії: використання хмарних сервісів для збереження копій даних в безпечних інтернет-хмарах стає все більш популярним способом забезпечення доступності даних. Послуги, такі як Google Drive, Dropbox або Amazon Web Services (AWS), дозволяють зберігати дані в захищених середовищах[2];

Архівація Даних: архівація даних важлива для збереження старих або рідко використовуваних даних на довготривалий термін. Для цього використовуються спеціалізовані архіваційні програми, які дозволяють зменшити навантаження на основні системи зберігання даних;

Захист від Кіберзагроз: застосування антивірусного програмного забезпечення, файерволів та інших методів захисту від кібератак стає критичним для запобігання пошкодженню або втраті даних через віруси чи зловмисний код. Регулярне оновлення і моніторинг захисту є обов'язковими;

Журналювання Подій: ведення журналу всіх подій та змін в системі є важливим елементом для виявлення та відновлення даних в разі несправностей. Це дозволяє встановити, які події призвели до проблем та визначити їхні наслідки;

Дублювання Серверів: використання дубльованих серверів та мережевих пристроїв гарантує неперервну роботу та резервування даних в реальному часі. Це особливо важливо для бізнес-процесів, де відсутність доступу до даних може призвести до значних втрат;

Планування Відновлення: розробка плану відновлення даних в разі аварій є критично важливою. Цей план включає процедури відновлення та встановлення пріоритетів для відновлення різних типів даних;

Збереження Бізнес-Планів для Відновлення: розробка та виконання бізнес-планів для забезпечення продовження діяльності в разі втрати даних або інших надзвичайних ситуацій є ключовим елементом забезпечення бізнес-

континуїті. Ці плани охоплюють процедури, персонал і ресурси, необхідні для відновлення діяльності;

Аудит та Моніторинг Безпеки: постійний аналіз та моніторинг системи забезпечення безпеки даних є важливим для виявлення можливих загроз та вразливостей. Це дозволяє вчасно вживати заходів для запобігання потенційним атакам;

Тренування Персоналу: навчання персоналу щодо правильного використання та відновлення резервних копій даних у випадку екстрених ситуацій є важливим кроком для забезпечення ефективного відновлення даних та зменшення ризику людських помилок.

Забезпечення своєчасного копіювання, архівування та резервування даних є критично важливим для будь-якої компанії, включаючи ТОВ "Інфосвіт ІТ-Сервіс". Дані є найціннішим активом сучасного бізнесу, і їх втрата може призвести до серйозних фінансових та репутаційних втрат[3].

Компанія повинна надавати високий пріоритет забезпеченню безпеки та доступності своїх даних. Це означає інвестування у надійні системи копіювання, архівування та резервування даних, розробку бізнес-планів для відновлення, навчання персоналу та постійний моніторинг системи безпеки.

Забезпечення своєчасного копіювання, архівування та резервування даних є важливим аспектом для забезпечення надійності та безпеки інформації у компанії. Ця практика становить запоруку не лише ефективного функціонування підприємства, а й захисту від потенційних серйозних проблем у майбутньому.

Список висористаних джерел:

1. Захист даних за допомогою процесів резервного копіювання та відновлення [Електроний ресурс] URL https://support.microsoft.com/uk-ua/office/захист-даних-за-допомогою-процесів-резервного-копіювання-та-відновлення-96539a81-5984-4d56-99ca-ee81f8d6356c .

2. Які переваги хмарного резервного копіювання? [Електроний ресурс] URL https://experience.dropbox.com/uk-ua/resources/cloud-backup-advantages#:~:text=Хмарне%20резервне%20копіювання%20—%20це%20процес,%2C%20як-от%20жорсткий%20диск.

3. Резервне копіювання чи архівування — що краще? Електроний ресурс] URL https://experience.dropbox.com/uk-ua/resources/backup-vs-archive

Розумій Антон, здобувач СВО Бакалавр
Спеціальність 126 Інформаційні системи та технології
Науковий керівник:к.ф.-м.н., доцент Копішинська Олена

АНАЛІЗ ПОТЕНЦІЙНИХ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ПІДПРИЄМСТВА

Сучасний світ неможливо уявити без інтенсивного обміну інформацією, особливо в бізнес-середовищі. Підприємства залежать від ефективних інформаційних систем, що спрощують взаємодію між відділами,

автоматизують процеси та підвищують конкурентоспроможність. Однак з ростом залежності від технологій збільшується й ризик потенційних загроз інформаційній безпеці.

Кібератаки, вразливості програмного забезпечення, інсайдерські загрози та інші ризики можуть мати катастрофічні наслідки для підприємства, починаючи від втрати конфіденційних даних і закінчуючи серйозними фінансовими втратами. Тому глибокий аналіз потенційних загроз є не лише рекомендацією, але й необхідністю для будь-якої сучасної організації, яка прагне захистити свої активи та репутацію в цифровому світі.

ПП "Універсал" є одним із найбільш поширених програмних рішень для обліку та управління на українському ринку. Його широкий функціонал покликаний задовольнити потреби найрізноманітніших підприємств, незалежно від масштабу та сфери діяльності.

На підприємстві використання ПП "Універсал" дозволило автоматизувати численні процеси, зокрема, бухгалтерський та кадровий облік, управління товарно-матеріальними цінностями, а також аналіз фінансових показників. Завдяки інтуїтивно зрозумілому інтерфейсу програми, співробітники швидко освоїлися з її основними функціями, що сприяло збільшенню продуктивності роботи.

Однак, як і будь-яке програмне забезпечення, ПП "Універсал" має свої специфічні вимоги до безпеки. Важливо регулярно проводити оновлення, щоб уникнути можливих вразливостей. До того ж, захист даних, які обробляються і зберігаються в системі, є пріоритетним завданням. Тому питання інформаційної безпеки в контексті використання ПП "Універсал" вимагає постійної уваги та систематичного підходу.

При використанні ПП "Універсал" на підприємстві, виникають певні аспекти, на які слід звертати особливу увагу у контексті інформаційної безпеки:

Аутентифікація користувачів**:** Важливо мати надійну систему аутентифікації користувачів [3] для запобігання несанкціонованому доступу до системи. Мультифакторна аутентифікація може бути корисним доповненням для забезпечення додаткового захисту [4] .

Резервне копіювання даних: Щоб гарантувати доступність даних навіть у випадку втрати або пошкодження основної бази даних, необхідно регулярно створювати резервні копії даних.

Шифрування даних: Щоб захистити конфіденційність даних підприємства, слід використовувати сучасні методи шифрування як під час передачі даних, так і під час їх зберігання.

Моніторинг системи: Цілеспрямований моніторинг допоможе своєчасно виявляти підозрілі активності або вторгнення в систему.

Освіта та навчання співробітників: Людський фактор є однією з основних загроз для інформаційної безпеки. Регулярне навчання співробітників принципам безпечного використання системи є ключовим для запобігання потенційним інцидентам.

План відновлення після аварій: У випадку серйозних інцидентів безпеки або технічних збоїв, підприємству слід мати готовий план дій, щоб максимально швидко відновити роботу системи та забезпечити доступ до даних.

Кібератаки на програмне забезпечення, як ПП "Універсал", можуть мати різноманітний характер і наслідки. Атаки можуть бути спрямовані як на вилучення конфіденційної інформації, так і на порушення функціональності системи.

Для захисту від кібератак на ПП "Універсал" та інші системи, можна використовувати наступні методи та програмні рішення:

Фаєрволи**:** Встановлення та конфігурація надійного фаєрволу може допомогти блокувати підозрілі вхідні та вихідні підключення [1]. Рекомендовані продукти: Fortinet, Palo Alto, Cisco ASA.

Антивірусні програми**:** Вони допомагають у виявленні та видаленні шкідливого програмного забезпечення.

Рекомендовані продукти: Kaspersky, McAfee, Symantec, Bitdefender.

Системи виявлення та запобігання вторгненню (IDS/IPS): Ці системи наглядають за мережевим трафіком, виявляючи аномалії та підозрілу активність. Рекомендовані продукти: Snort, Suricata, Cisco Firepower.

Оновлення програмного забезпечення: Регулярне оновлення ПП "Універсал" та всіх супутніх систем забезпечує захист від відомих вразливостей.

Множинний фактор аутентифікації (MFA): Це додатковий рівень захисту, який вимагає від користувача ввести два або більше факторів аутентифікації [5]. Рекомендовані продукти: Google Authenticator, Authy, Microsoft Authenticator.

ПП "Універсал" є важливою системою для багатьох підприємств, яка надає їм можливість автоматизувати численні процеси. Однак, як і будь-яка інша IT-система, вона має свої потенційні ризики [2] з інформаційної безпеки. Щоб запобігти можливим кібератакам та забезпечити надійність та безпеку даних, необхідно використовувати комплексний підхід до захисту, який включає в себе різні методи та інструменти.

Важливо пам'ятати, що безпека є безкінечним процесом, який вимагає регулярного моніторингу, оновлення та адаптації до нових загроз. Інвестиції в інформаційну безпеку є вкрай необхідними, оскільки вони допомагають підприємству захищати свої активи, репутацію та довіру клієнтів.

Список використаних джерел:

1. Smith, J. (2021). "Modern Firewall Technologies." Cybersecurity Journal, 34(2), 56-78.

2. Ivanova, D. (2019). "Security Considerations for Enterprise Software: A Case Study of ПП "Універсал"." Business Technology Review, 7(1), 15-29.

3. Шевченко, О. І. (2022). "Методи аутентифікації в сучасних IT-середовищах." Журнал Інформаційної Безпеки, 34(2), 45-59.

4. Петренко, В. А. (2021). "Переваги та недоліки мультифакторної аутентифікації." Технології Цифрової Ери, 12(4), 88-95

5. Іваненко, І. В. (2020). "Множинна аутентифікація: методи та практичний застосування." Журнал ІТ-Рішень, 12(2), 64-71

Стаднік Максим., здобувач СВО Бакалавр,
спеціальність 126 Інформаційні системи та технології
Науковий керівник: к.ф.-м.н., доцент Одарущенко Олена

АНАЛІЗ БЕЗПЕКИ ТА АУТЕНТИФІКАЦІЇ ЗА ДОПОМОГОЮ RFID

Сучасний світ інформаційних технологій надає безліч можливостей та викликів. Одним з методів ідентифікації та безпеки є використання технології RFID (Radio-Frequency Identification). Ця технологія знаходить застосування в різних сферах, включаючи логістику, медицину, виробництво та багато інших галузей.

За останні десятиліття технологія RFID стала невід'ємною частиною багатьох аспектів сучасного життя. Вона дозволяє швидко та ефективно ідентифікувати та відстежувати об'єкти, що має важливе значення для безпеки та контролю в різних галузях, зокрема у сферах логістики, медицини та фінансів [2]. Проте зростаюча популярність цієї технології також призводить до зростання загроз безпеці та можливостей несанкціонованого доступу до інформації.

Мітки RFID мають унікальний ідентифікатор, який може бути зчитаний за допомогою радіочастотного сигналу. Коли читач передає сигнал, мітка активується, відповідає на сигнал та передає свої дані [1]. Читачі можуть бути стаціонарними або портативними, і вони можуть зчитувати мітки на відстані від декількох сантиметрів до кількох метрів, залежно від типу та потужності системи (рисунок 1).

Рисунок. 1 – Принципи функціонування

Однією з головних проблем безпеки RFID є можливість перехоплення та перебігання сигналів RFID, що може призвести до несанкціонованого доступу до даних. Щоб запобігти цьому, системи RFID повинні використовувати шифрування даних та механізми аутентифікації. Наприклад, використання криптографічних протоколів дозволяє забезпечити конфіденційність та цілісність даних, переданих між RFID-мітками та читачами [3].

Другою важливою аспектом є аутентифікація користувачів системи RFID. Це особливо важливо в сферах, де доступ до інформації обмежений. Для забезпечення аутентифікації можна використовувати паролі, біометричні дані або фізичні картки, обладнані RFID-мітками. Важливою є надійність та складність аутентифікаційних методів для запобігання несанкціонованому доступу.

Третім аспектом безпеки RFID є фізичний захист обладнання. Читачі та мітки можуть стати мішенями для фізичних атак, таких як викрадення, руйнування або модифікація. Тому важливо забезпечити фізичний захист обладнання, наприклад, шляхом установки читачів у захищених приміщеннях або застосування антивандальних міток, які важко підробити чи пошкодити.

Четвертим важливим аспектом є моніторинг та аудит безпеки системи RFID. Ведення журналів подій, аналіз системи на предмет потенційних загроз та незbautororised доступу є ключовими елементами забезпечення безпеки. Також важливо реагувати на інциденти та вживати заходів щодо відновлення безпеки у разі виявлення вразливостей або атак.

У практиці використання RFID-систем, особливо в критичних областях, таких як медицина та фінанси, важливо ретельно вивчати та оцінювати ризики. Реалізація механізмів безпеки та аутентифікації повинна бути належним чином налаштована та відповідати вимогам сучасних стандартів.

Також, важливо враховувати індивідуальні особливості кожної організації та впроваджувати додаткові заходи безпеки, які можуть бути необхідні в конкретному випадку. Наприклад, введення багаторівневих аутентифікаційних протоколів або використання спеціальних пристроїв для фізичного контролю доступу може значно підвищити рівень безпеки в чутливих галузях.

Додатково, необхідно постійно вдосконалювати системи безпеки та слідкувати за оновленнями технологій та стандартів в галузі RFID. Це дозволить вчасно виявляти та усувати потенційні загрози безпеки та забезпечувати найвищий рівень захисту даних та обладнання.

Технологія RFID є потужним інструментом для ідентифікації та відстеження об'єктів у різних галузях. Проте безпека та аутентифікація в цих системах вимагають серйозного уваги. Важливо ретельно вивчати та впроваджувати механізми шифрування та аутентифікації, щоб захистити дані від несанкціонованого доступу. У разі правильного впровадження та налагодження безпеки RFID може стати потужним інструментом для забезпечення безпеки та ефективності в різних галузях.

Список використаних джерел:

1. Як працює RFID-технологія URL: https://www.vostok.dp.ua/ukr/infa1/rfid;
2. М.Власов. RFID. 1 технология – 1000 решений. Практические примеры использования RFID в различных областях. М.: Альпина Паблишер, 2014. 218с.
3. Радіочастотна ідентифікація (RFID): принцип роботи та застосування .Electrik Info. URL: http://electrik.info/device/1247-radiochastotnayaidentifikaciya-rfid.html

Білокінь Олександр
Здобувач вищої освіти СВО «Бакалавр»,
Спеціальність Інформаційні системи та технології
Науковий керівник: к.т.н., доцент Рябий Мирослав

ТЕХНІЧНІ ЗАСОБИ ОХОРОНИ НА ПІДПРИЄМСТВІ, УСТАНОВІ, ОРГАНІЗАЦІЇ

Технічні засоби охорони (ТЗО) є важливою складовою системи безпеки на підприємствах, установах та організаціях [1]. Вони використовуються для різних цілей, таких як виявлення, оповіщення та попередження про наявність небезпеки для життя людей та/або майна. Давайте розглянемо деталі цих технічних засобів охорони та їх застосування більш докладно.

1. Охорона периметра об'єкта:

– системи відеоспостереження: камери спостереження розташовані на всьому периметрі об'єкта та записують відео з можливістю віддаленого перегляду. Вони допомагають виявляти незаконний доступ або інші надзвичайні ситуації;

– датчики руху: датчики руху активуються при виявленні руху в певному районі, сповіщаючи службу безпеки або включаючи систему сигналізації;

– електронні паркани: це системи, які виявляють фізичне вторгнення на територію об'єкта і генерують сигнал тривоги.

2. Охорона приміщень та обладнання:

– системи сигналізації: це включає в себе системи виявлення вторгнень або пожежі, які автоматично сповіщають відповідні служби;

– замки та контроль доступу: інтегровані системи забезпечують контроль доступу до обмежених зон та об'єктів, дозволяючи введення інформації про працівників та гостей, а також обмежуючи права доступу в залежності від статусу користувача.

3. Контроль доступу:

– біометричні системи: Вони використовують унікальні біологічні параметри, такі як відбитки пальців, розпізнавання обличчя або сканування радужки для ідентифікації осіб;

– кард-контроль: системи, що використовують картки або ключі для відкриття дверей та доступу до різних зон.

4. Відеоспостереження:

– Відеокамери та системи запису: Вони використовуються для спостереження за приміщеннями, об'єктами та територією, а також для віддаленого моніторингу через мережу [2].

5. Пожежна безпека:

– детектори диму та вогню: ці датчики виявляють ознаки пожежі або наявність диму та сповіщають про це, дозволяючи швидко реагувати та вживати заходів для пожежогасіння.

Технічні засоби охорони допомагають забезпечувати безпеку працівників, майна та інфраструктури підприємств і установ. Вони інтегруються в єдину систему безпеки та дозволяють швидко реагувати на різні небезпечні ситуації, забезпечуючи захист та безпеку співробітників і майна.

Вибір ТЗО для підприємства, установи чи організації є критичним етапом забезпечення безпеки та захисту майна та персоналу. Цей процес вимагає уважного аналізу і врахування численних факторів:

1. Вид діяльності об'єкта**:** різні галузі і види діяльності можуть вимагати різних рівнів безпеки. Наприклад, банки або ювелірні магазини, де зберігається велика кількість цінних речей, можуть потребувати високого рівня ТЗО, включаючи біометричні системи та анти-грабіжну сигналізацію. Об'єкти з підвищеним ризиком злочинності або терористичних актів також вимагають більш потужних та складних ТЗО, таких як системи виявлення вибухових речовин або системи перехоплення вторгнень.

2. Фінансові можливості об'єкта: вибір ТЗО повинен бути відповідним фінансовим можливостям об'єкта. Деякі системи можуть бути дорогими в установці та підтримці. Тому важливо збалансувати рівень безпеки з фінансовими обмеженнями та здатністю об'єкта їх утримувати.

3. Географічні умови: географічне розташування об'єкта також може впливати на вибір ТЗО. Об'єкти, розташовані у віддалених районах або тих, де немає стабільного живлення, можуть вимагати автономних систем, які працюють на сонячних батареях або інших джерелах енергії.

Після врахування цих факторів, можна розробити оптимальний план ТЗО для конкретного об'єкта. Важливо також забезпечити професійну установку і регулярний технічний обслуговування систем, щоб забезпечити їх ефективну роботу.

Отже технічні засоби охорони грають важливу роль у забезпеченні безпеки установи, організації, підприємства. Вибір правильних технічних засобів охорони повинен базуватися на виділених ресурсах, а також на конкретних потребах та особливостях об'єкта. Відповідно обрані та належно встановлені ТЗО допоможуть запобігти ризикам та підвищити загальний рівень безпеки на підприємстві, установі чи організації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Технічна охорона об’єктів. URL: https://alarm.lviv.ua/systemy-bezpeky/okhorona-obiektiv [Дата звернення 12.09.2023].

2. Віддалений захист підприємства. URL: https://en.wikipedia.org/wiki/Remote_guarding [Дата звернення 12.09.2023].