

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ДИЗАЙНУ

КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Пояснювальна записка

до кваліфікаційної роботи

магістра

(освітньо-кваліфікаційний рівень)

на тему ПОБУДОВА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
НА ОСНОВІ ПРИВАТНИХ ВІРТУАЛЬНИХ МЕРЕЖ (VPN)

BUILDING THE INFORMATION SECURITY SYSTEM BASED ON PRIVATE
VIRTUAL NETWORKS (VPN)

Виконав: студент 2 курсу, групи 6КСМ

напряму підготовки (спеціальності)

123 «Комп'ютерна інженерія»

(шифр і назва напряму підготовки, спеціальності)

Лаврук І.С.

(прізвище та ініціали)

Керівник Лена Є.В.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

Херсон – 2020 року

ХЕРСОНСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Інститут, факультет, відділення факультет інформаційних технологій та дизайну
Кафедра, циклова комісія інформаційних технологій
Освітньо-кваліфікаційний рівень магістр
Напрямок підготовки _____
Спеціальність 123 «Комп'ютерна інженерія»
(шифр і назва)
(шифр і назва)

ЗАТВЕРДЖУЮ

Завідувач кафедри, голова циклової комісії інформаційних технологій
Г.О. Райко
«__» _____ 2020 року

ЗАВДАННЯ НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Лавруку Іллі Семеновичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Побудова системи інформаційної безпеки на основі приватних віртуальних мереж (VPN)

керівник проекту (роботи) Лєна Євгеній Володимирович к.т.н., доцент

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від «01» жовтня 2020 року №536-С

2. Строк подання студентом проекту (роботи) 8 грудня 2020 р.

3. Вихідні дані до проекту (роботи) Методичні рекомендації до виконання, оформлення та захисту кваліфікаційної роботи магістра для студентів всіх форм навчання за спеціальністю 123 «Комп'ютерна інженерія»

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)

1. Аналіз потенційних погроз інформаційної безпеки підприємства

2. Характеристика технологій та заходів для забезпечення інформаційної безпеки

3. Програмно-апаратний комплекс інформаційної безпеки

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

1. Методи й завдання проектування 2. Ранжирування активів підприємства

3. Структура локальної комп'ютерної мережі 4. Технології захисту ЛОМ

5. Діалогові вікна 6. Технічна архітектура інформаційної системи

7. Програмна архітектура інформаційної системи 8. Висновки

6. Консультанти розділів проекту (роботи)

| Розділ | Прізвище, ініціали та посада | Підпис, дата |
|--------|------------------------------|--------------|
|--------|------------------------------|--------------|

| | консультанта | завдання видав | завдання прийняв |
|--|--------------|----------------|------------------|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

| № з/п | Назва етапів дипломного проекту (роботи) | Строк виконання етапів проекту (роботи) | Примітка |
|-------|---|---|----------|
| 1. | <i>Визначення комплексу завдань для забезпечення інформаційної безпеки</i> | <i>Вересень 2020</i> | |
| 2. | <i>Інженерно-технічні заходи захисту інформації</i> | <i>Вересень 2020</i> | |
| 3. | <i>Програмно-апаратні комплекси захисту інформації</i> | <i>Вересень 2020</i> | |
| 4. | <i>Реалізації системи інформаційної безпеки на підприємстві</i> | <i>Вересень 2020</i> | |
| 5. | <i>Установка комплексу програмних засобів ViPNet</i> | <i>Жовтень 2020</i> | |
| 6. | <i>Створення технічної архітектури інформаційної системи</i> | <i>Жовтень 2020</i> | |
| 7. | <i>Створення програмної архітектури інформаційної системи</i> | <i>Жовтень 2020</i> | |
| 8. | <i>Оформлення пояснювальної записки до кваліфікаційної роботи та графічної частини.</i> | <i>Листопад 2020</i> | |
| 9. | <i>Подання роботи на кафедру для затвердження</i> | <i>Грудень 2020</i> | |
| 10. | <i>Захист кваліфікаційної роботи магістра</i> | <i>Грудень 2020</i> | |
| | | | |
| | | | |
| | | | |

Студент

(підпис)

Лаврук І.С.
(прізвище та ініціали)

Керівник проекту (роботи)

(підпис)

Лена Є.В.
(прізвище та ініціали)

ЗМІСТ

| | |
|---|----|
| ВСТУП | 7 |
| 1 АНАЛІЗ ПОТЕНЦІЙНИХ ПОГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА | 10 |
| 1.1 Організаційно-функціональна структура підприємства | 10 |
| 1.2 Методика дослідження інформаційної безпеки | 11 |
| 1.3 Ідентифікація й оцінка інформаційних активів | 15 |
| 1.4 Оцінка уразливостей активів | 17 |
| 1.5 Оцінка погроз активам | 19 |
| 1.6 Оцінка існуючих і планованих засобів захисту | 21 |
| 1.7 Оцінка ризиків | 27 |
| 1.8 Визначення комплексу завдань для забезпечення інформаційної безпеки | 29 |
| 1.8.1 Погрози порушення конфіденційності даних | 30 |
| 1.8.2 Погрози порушення цілісності даних | 30 |
| 1.8.3 Погрози порушення доступності | 31 |
| 1.8.4 Погрози порушення спостереженості даних | 31 |
| 1.8.5 Погрози порушення автентичності інформації | 31 |
| 1.9 Визначення місця комплексу завдань у комплексі завдань в інформаційній системі підприємства | 32 |
| 1.10 Організація забезпечення інформаційної безпеки | 33 |
| 2 ХАРАКТЕРИСТИКА ТЕХНОЛОГІЙ ТА ЗАХОДІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | 37 |
| 2.1 Інженерно-технічні заходи захисту інформації | 37 |
| 2.2 Virtual Personal Network (VPN) | 37 |
| 2.3 Екранування комп'ютерної мережі | 40 |
| 2.4 Системи Intrusion Detection System (IDS) | 42 |
| 2.5 Криптографія | 45 |

| | |
|--|----|
| | 5 |
| 2.6 Аналіз методів захисту інформації | 46 |
| 2.7 Криптографічні методи | 47 |
| 2.7.1 Метод DES | 47 |
| 2.7.2 Метод RSA | 49 |
| 2.8 Програмно-апаратні комплекси захисту інформації | 49 |
| 2.8.1 Комплекс «Акорд 1.95» | 49 |
| 2.8.2 Система Secretnet | 50 |
| 2.9 Пропонований розв'язок для захисту інформації підприємства | 50 |
| 3 ПРОГРАМНО-АПАРАТНИЙ КОМПЛЕКС ІНФОРМАЦІЙНОЇ БЕЗПЕКИ | 52 |
| 3.1 Структура програмно-апаратного комплексу інформаційної безпеки й захисту інформації підприємства | 52 |
| 3.2 Структура програмного забезпечення ViPNet | 53 |
| 3.3 ViPNet Manager | 56 |
| 3.4 ViPNet Coordinator | 57 |
| 3.5 ViPNet Client | 59 |
| 3.6 Установка ViPNet Manager | 63 |
| 3.7 Установка ViPNet Client на робочому місці адміністратора | 64 |
| 3.8 Установка ViPNet Coordinator на сервери (координатори) мережі ViPNet | 66 |
| 3.9 Реалізації системи інформаційної безпеки на підприємстві | 69 |
| 3.10 Формування структури програми ViPNet Manager | 71 |
| 3.11 Редагування зв'язків | 77 |
| 3.12 Настроювання доступу до координатора | 78 |
| 3.13 Завдання властивостей випадкових паролів | 79 |
| 3.14 Створення наборів ключів після формування структури мережі за допомогою майстра | 81 |
| 3.15 Настроювання системи виявлення атак | 85 |
| 3.16 Установлення з'єднання між абонентським пунктом і координатором | 86 |

ВИСНОВКИ

6

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

88

89

ВСТУП

Будь-яка діяльність в області підприємництва є тісно пов'язаною із прийманням, нагромадженням, збереженням, обробкою й застосуванням різних інформаційних потоків. Цілісність існуючого світоустрою як єдиного глобального співтовариства забезпечує, в основному, інтенсивний інформаційний обмін. Зупинка глобальних інформаційно-комунікаційних потоків навіть на зовсім короткий проміжок часу здатна приводити до не менших криз, чому розриви міждержавних економічних зв'язків.

Тому, у нові ринково-конкурентних умовах з'являється велика кількість нових проблем, які зв'язані не тільки із забезпеченням цілісності й конфіденційності комерційних, фінансових або підприємницьких даних як видів інтелектуальної власності, але також і фізичних і юридичних осіб, їх майнової власності і особистої безпеки.

Інформаційна безпека являє собою комплекс заходів щодо захисту даних від неавторизованого доступу, руйнувань, модифікацій, розкриття або затримки при доступі. В інформаційну безпеку включаються заходи щодо захисту процесу створення інформації, її введення, обробки й висновку.

Ціль інформаційної безпеки полягає в тому, щоб убезпечити цінність систем, захищати і гарантувати точність і цілісність даних, а також мінімізувати наслідку, які можуть виникнути в тому випадку, коли дані будуть модифіковані або зруйновані. У рамках інформаційної безпеки потрібен облік усіх дій, у ході яких інформація створюється, зазнає модифікації, коли до неї здійснюється доступ або вона поширюється по мережі.

Актуальність проблеми

Будь-яка діяльність в області підприємництва є тісно пов'язаною із прийманням, нагромадженням, збереженням, обробкою й застосуванням різних інформаційних потоків. Цілісність існуючого світоустрою як єдиного

глобального співтовариства забезпечує, в основному, інтенсивний інформаційний обмін.

Порушення інформаційного обміну різними способами приводить до порушення нормального функціонування підприємства. Тому підвищення інформаційної безпеки підприємств і організацій є актуальним завданням і може бути забезпечена організаційними й інженерно-технічними рішеннями.

Метою даної роботи є у збільшенні рівня захисту даних в інформаційній системі підприємства.

Для досягнення мети роботи, необхідно розв'язати наступні завдання:

- досліджувати існуючу інфраструктуру й одержати вихідні дані для проектування VPN;
- проаналізувати ризики;
- на основі аналізу ризику вибрати організаційні й інженерно-технічні розв'язки для підвищення рівня інформаційної безпеки на підприємстві;
- описати процес впровадження обраних засобів захисту інформації з використанням VPN;

Об'єктом є система інформаційної безпеки на підприємстві.

Предметом дослідження є інженерно-техніческие методи и средства для повышения уровня информационной безопасности

Методологія і методи досліджень. При вирішенні зазначених завдань використовувалися методи системного аналізу, експертних оцінок, статистики, технології програмування.

Наукова новизна роботи полягає у використанні віртуальних приватних комп'ютерних мереж для підвищення інформаційної безпеки підприємства.

Структура й об'єм роботи

Кваліфікаційна робота складається з вступу, 3-х розділів, висновку й переліку посилань, викладених на 90 сторінках тексту, що включає 9 таблиць, 28 ілюстрації та перелік посилань з 27 найменувань.

Публікації

1. Лаврук І.С., Лепа Є.В. Заходи забезпечення інформаційної безпеки Сучасні комп'ютерні системи та мережі в управлінні: Матеріали III Всеукраїнської науково-практичної інтернет-конференції студентів, аспірантів та молодих вчених (30 листопада 2020 р.). - Херсон, 2020. - С.39-42.
2. Лаврук І.С., Лепа Є.В. Програмний комплекс інформаційної безпеки. Materiały XVI Międzynarodowej naukowo-praktycznej konferencji, «Wykształcenie i nauka bez granic - 2020», 07 - 15 grudnia 2020 roku, Volume 2 - Przemysł Nauka i studia. - С.33-35.