МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Рівненський фаховий коледж інформаційних технологій

Звіт

Про виконання лабораторної роботи №3

Міні-політика інформаційної безпеки.

Виконав
Студент 3 курсу групи КН-3/1
Валерій ФОРМАНЮК
23.09.2025 р.

м.Рівне

Лабораторна робота №3

Тема: Міні-політика інформаційної безпеки для мережі СТО

Мета роботи:

- Забезпечити захист даних клієнтів, фінансової інформації та стабільну роботу IT-системи мережі станцій технічного обслуговування.
- Визначити правила роботи з інформаційними активами.
- Сформувати базові вимоги до користувачів, адміністраторів та керівництва.

1. Основні активи

- База даних клієнтів (контактні дані, історія обслуговувань).
- Фінансова інформація (рахунки касові операції).
- Система обліку запчастин та замовлень.
- Корпоративна електронна пошта.
- Вебсайт СТО (запис клієнтів онлайн).

2. Категорії доступу

- **Адміністратор** - повний доступ до всіх систем і резервних копій.
- **Бухгалтер** - доступ до фінансової інформації.
- **Менеджер** - доступ до записів та замовлень клієнтів.
- **Клієнт** - доступ до власного кабінету на сайті (перегляд історії замовлень, запис онлайн).

3. Правила

- **Паролі** мінімум 8 символів, обов'язково великі та малі літери, цифри та спецсимволи. Зміна раз на 3 місяці.
- **Електронна пошта** використовувати тільки корпоративну пошту для роботи з клієнтами. Заборонено відкривати підозрілі листи.
- **Інтернет** заборонено відвідувати сайти, що можуть містити програмне ПЗ. Доступ до робочих ресурсів лише через захищене з'єднання (HTTPS, VPN).

4. Резервне копіювання

- Щоденне автоматичне копіювання бази клієнтів і замовлень на внутрішній сервер.
- Щотижневе резервне копіювання на зовнішній носій або (USB-диск) або у хмарне сховище (Google Drive / OneDrive).
- Перевірка працездатності резервних копій раз на місяць.

5. Дії у випадку виявлення інциденту

1. Негайно повідомити адміністратора.
2. Заблокувати скомпрометований акаунт або комп’ютер.
3. Відновити дані з резервної копії.
4. Провести розслідування та вжити заходів, щоб уникнути повторення інциденту.

Таблиця політики до Лабораторної роботи №3

Розділ політики	Приклад правил та вимог
Класифікація активів	База клієнтів - конфіденційна; фінансова інформація - конфіденційна; сайт СТО - відкритий ресурс.
Категорії доступу	Адміністратор повний доступ; Бухгалтер - доступ до фінансів; Менеджер - доступ до замовлень; Клієнт - доступ до особистого кабінету.
Паролі	Мінімум 8 символів; комбінація літер, цифр і спецсимволів; зміна кожні 3 місяці.
Електронна пошта	Використовувати лише корпоративну пошту; заборонено відкривати підозрілі вкладення.
Інтернет	Використовувати лише HTTPS; заборона на небезпечні сайти.
Резервне копіювання	Щоденне - на сервер; щотижневе - на USB/хмару; щомісячна перевірка відновлення.
Дії при інцидентах	Повідомлення адміністратора; блокування доступу; відновлення з резерву; розслідування.

Висновок

У лабораторній роботі №3 на прикладі мережі СТО було розроблено міні-політику інформаційної безпеки. Визначені активи (база клієнтів, фінанси, сайт), встановлені ролі користувачів, вимоги до паролів і використання мережевих ресурсів. Також передбачена процедура резервного копіювання та дії у випадку інцидентів.
Ця політика є основою для захисту даних та стабільної роботи СТО.

Відповіді на контрольні питання

1. Що таке політика інформаційної безпеки і для чого вона потрібна?

Політика інформаційної безпеки - це документ, що визначає правила та вимоги щодо захисту інформаційних активів організації. Вона потрібна для запобігання витокам даних, забезпечення цілісності та доступності інформації, а також для визначення обов’язків користувачів і адміністраторів.

2. Які основні компоненти політики.

- Класифікація інформаційних активів.
- Вимоги до паролів та автентифікації.
- Використання мережевих ресурсів (інтернет, пошта, локальна мережа).
- Резервне копіювання та контроль цілісності.
- Дії у випадку інцидентів безпеки.

3. Хто відповідає за створення і підтримку політики ІБ в організації?

Відповідальність лежить на керівництві організації (директор, завідувач), яке затверджує політику. Технічна підтримка та впровадження - за системними адміністраторами. Контроль виконання - за ІТ-відділом або уповноваженою особою з ІБ.

4. Які вимоги до паролів вважаються мінімальними для безпеки?

- Мінімальна довжина 8-12 символів.
- Використання великих і малих літер, цифр і спеціальних символів.
- Заборона використання простих паролів (“123456”, “ qwerty”).
- Регулярна зміна паролів (раз на 3 - 6 місяців).

5. Чому важливо включати в політику резервне копіювання?

Резервне копіювання гарантує відновлення даних після збоїв, вірусних атак або втрати обладнання. Без цього навіть добре захищена система може зазнати критичних втрат інформації.