

Лабораторная работа №8

Основы кибербезопасности в цифровой экономике лесного хозяйства

Цель работы: изучить основные принципы кибербезопасности и их применение в цифровых системах лесного хозяйства, научиться идентифицировать потенциальные угрозы и разрабатывать базовые меры защиты.

Задачи:

1. Познакомиться с основными видами киберугроз для информационных систем лесного хозяйства.
2. Изучить нормативные требования к защите информации в лесном секторе.
3. Проанализировать реальные кейсы кибератак на природоресурсные системы.
4. Разработать рекомендации по обеспечению безопасности для типового лесничества.

Оборудование и ПО:

- Компьютер с доступом в интернет
- Браузер для работы с онлайн-ресурсами
- Текстовый редактор для оформления отчета

Теоретическая часть (кратко)

Почему кибербезопасность важна в лесном хозяйстве?

Современное лесное хозяйство использует различные цифровые системы:

- Государственные реестры (ЛесЕГАИС, ФГИС "Лес").
- Геоинформационные системы (ГИС).
- Системы мониторинга (датчики, дроны).
- Базы данных о лесных ресурсах.

Основные угрозы:

1. **Фишинг** – кража учетных данных сотрудников.
2. **Вредоносное ПО** – атаки на компьютеры лесничеств.
3. **Утечки данных** – несанкционированный доступ к информации.
4. **Сбои в работе систем** – отказ оборудования или ПО.

Нормативная база в России:

- Федеральный закон №187-ФЗ "О безопасности критической информационной инфраструктуры"
- ГОСТы по информационной безопасности.
- Отраслевые стандарты Рослесхоза.

Практическая часть

Задание 1. Анализ уязвимостей в цифровых системах лесного хозяйства

1. Изучите следующие системы, используемые в лесном хозяйстве:
 - ЛесЕГАИС (<https://lesega.ru>).
 - Публичные ГИС-сервисы лесного мониторинга.
2. Определите потенциальные уязвимости:
 - Какие данные являются публичными?
 - Какая информация требует защиты?
 - Как организован доступ к системам?

Задание 2. Изучение реальных кейсов кибератак

1. Найдите в открытых источниках информацию о кибератаках на:
 - Системы учета природных ресурсов
 - Геоинформационные системы
 - Государственные реестры данных
2. Проанализируйте один кейс по схеме:
 - Какая система подверглась атаке?
 - Каковы были последствия?
 - Какие меры были приняты для устранения угрозы?

Задание 3. Разработка политики парольной безопасности

Создайте правила использования паролей для сотрудников лесничества:

1. Требования к сложности паролей.
2. Правила хранения и смены паролей.
3. Меры на случай компрометации учетной записи.

Задание 4. Анализ фишинговых угроз

1. Изучите примеры фишинговых писем, нацеленных на госучреждения.
2. Разработайте памятку для сотрудников по распознаванию фишинга:
 - На что обращать внимание в письмах?
 - Как проверять отправителя?
 - Какие действия предпринимать при получении подозрительного письма?

Задание 5. Оценка защиты данных в облачных сервисах

1. Изучите популярные облачные сервисы (*Яндекс.Диск, Google Drive, VK Cloud*)

2. Сравните их возможности для защиты данных:
 - Шифрование данных.
 - Двухфакторная аутентификация.
 - Резервное копирование.

Задание 6. Создание плана восстановления после сбоя

Разработайте простой план действий на случай:

1. Потери доступа к системе ЛесЕГАИС.
2. Утери данных о лесных участках.
3. Сбоя в работе системы мониторинга.

Задание 7. Сравнение антивирусных решений

Сравните антивирусные продукты для организаций:

1. *Kaspersky Endpoint Security*.
2. *Dr.Web* для рабочих станций.
3. *Microsoft Defender* для бизнеса.

Критерий	Касперский	Доктор Веб	<i>Microsoft Defender</i>
Стоимость			
Защита от фишинга			
Работа с ГОСТами			
Техническая поддержка			

Контрольные вопросы:

1. Какие три основных угрозы для информационных систем лесного хозяйства?
2. Почему государственные реестры лесов относятся к критической инфраструктуре?
3. Как сотрудники лесничества могут защититься от фишинговых атак?
4. Какие российские законы регулируют кибербезопасность?
5. Почему важно регулярно обновлять программное обеспечение?

Требования к отчету

1. **Титульный лист** (вуз, группа, ФИО)
2. **Цель и задачи работы**
3. **Результаты выполнения заданий:**
 - Анализ уязвимостей систем
 - Описание изученного кейса
 - Разработанные документы (правила, памятки, планы)
 - Сравнительная таблица
4. **Выводы и рекомендации:**
 - Какие системы лесного хозяйства наиболее уязвимы?
 - Какие меры защиты наиболее эффективны?
 - Как повысить киберграмотность сотрудников?
5. **Список использованных источников**

Критерии оценки

1. Полнота выполнения заданий.
2. Качество анализа и глубину проработки тем.
3. Практическая значимость разработанных рекомендаций.
4. Оформление отчета и четкость изложения.

Дополнительные материалы для изучения

1. Центр кибербезопасности Рослесхоза: <https://rosleshoz.gov.ru/security>
2. Роскомнадзор: рекомендации по защите персональных данных
3. ФСТЭК России: руководящие документы по защите информации
4. Киберучебник для госслужащих: <https://digital.gov.ru/cybercourse/>

Примеры кейсов для анализа

1. **Кейс 1.** Утечка данных из регионального лесного реестра (2022 г.)
 - Причина: слабые пароли сотрудников
 - Последствия: публикация данных о лесных аукционах
 - Решение: внедрение двухфакторной аутентификации
2. **Кейс 2.** Фишинговая атака на бухгалтерию лесхоза (2023 г.)
 - Метод: поддельное письмо от "Минприроды".
 - Цель: получение доступа к финансовым системам.
 - Профилактика: обучение сотрудников.

3. **Кейс 3.** Сбой в работе системы мониторинга лесных пожаров.
- Причина: устаревшее программное обеспечение.
 - Последствия: задержка в обнаружении пожаров.
 - Решение: регулярное обновление ПО.