Лабораторная работа №12

Тема: Организация безопасной работы в сети Интернет.

Цель работы: Освоить методы и средства обеспечения безопасности при работе в сети Интернет, актуальные для специалистов по газовому оборудованию (в т.ч. при удалённом мониторинге, обновлении ПО, обмене технической документацией и т.д.).

Задачи:

1. Изучить основные угрозы информационной безопасности в Интернете.
2. Освоить практические методы защиты данных и устройств.
3. Настроить безопасные параметры браузера и сетевого подключения.
4. Отработать навыки распознавания фишинговых атак и вредоносных ресурсов.
5. Разработать рекомендации по безопасной работе в Интернете для специалистов газовой отрасли.

Теоретическая часть

Основные угрозы в сети Интернет:

- **Фишинг** — попытки получения конфиденциальных данных через поддельные сайты/письма (например, подмена сайта поставщика оборудования).
- **Вредоносное ПО** (вирусы, трояны) — может нарушить работу систем управления газовым оборудованием.
- **Утечки данных** — компрометация технической документации, схем, паролей доступа.
- **Атаки типа «человек посередине» (MitM)** — перехват трафика при удалённом доступе к оборудованию.
- **DoS/DDoS-атаки** — нарушение работы корпоративных сетей и систем мониторинга.
- **Незащищённые Wi-Fi-сети** — риск перехвата данных в публичных местах.

Специфика для газовой отрасли:

- Удалённый мониторинг оборудования требует защищённых каналов связи.

- Техническая документация (схемы, настройки) — конфиденциальная информация.
- Атаки на промышленные системы (SCADA) могут привести к авариям.

Методы защиты:

- Использование **антивирусного ПО** с регулярным обновлением баз.
- Применение **VPN** для шифрования трафика при удалённом доступе.
- Настройка **брандмауэра** для блокировки подозрительных соединений.
- Двухфакторная аутентификация (2FA) для учётных записей.
- Регулярное обновление ПО и операционных систем.
- Обучение персонала правилам кибербезопасности.

Практическая часть

Задание 1. Проверка и настройка безопасности учебного ПК

- **Цель:** убедиться, что компьютер соответствует базовым требованиям безопасности.
- **Ход работы:**

1. Проверьте, установлено ли на ПК антивирусное ПО (например, Kaspersky Endpoint Security, Dr.Web).
2. Убедитесь, что базы антивируса обновлены (в интерфейсе программы найдите раздел «Обновления»).
3. Проверьте статус брандмауэра Windows:

- откройте «Панель управления» → «Система и безопасность» → «Брандмауэр Windows»;
- убедитесь, что он включён для всех сетей.

4. Зафиксируйте результаты в отчёте в виде таблицы (антивирус: установлен/не установлен, обновления: актуальны/устарели, брандмауэр: включён/выключен).

Задание 2. Безопасная работа в браузере

- **Цель:** настроить браузер для минимизации рисков при поиске технической информации.

- **Ход работы (на примере Яндекс Браузера и Microsoft Edge):**

1. Откройте браузер.
2. Перейдите в «Настройки» → «Конфиденциальность и безопасность».
3. Активируйте:

- «Улучшенная защита от фишинга и вредоносных программ»;
- «Блокировка всплывающих окон и переадресаций».

4. В разделе «Пароли» отключите опцию «Предлагать сохранение паролей».
5. Проверьте наличие HTTPS на сайтах с технической документацией (иконка замка в адресной строке).
6. Запишите 3–5 проверенных сайтов по газовому оборудованию с HTTPS.

Задание 3. Тренировка распознавания фишинга

Цель: научиться отличать безопасные ресурсы от мошеннических.

- **Ход работы:**

1. Преподаватель предоставляет скриншота/распечатки веб-страниц и писем (Смотри приложение 1).
2. Проанализируйте каждый пример по критериям:

- URL-адрес (опечатки, странные домены);
- содержание (давление, ошибки, отсутствие персонализации);
- визуальные признаки (искажённые логотипы, плохой дизайн).

Заполните таблицу: (Смотри приложение 2)

№	Ресурс/Письмо	Признаки фишинга	Вердикт (безопасен/опасен)
1	…	…	…

Задание 4. Создание и хранение паролей (без реальной регистрации)

- **Цель:** освоить принципы создания надёжных паролей и их безопасного хранения в учебных целях.
- **Ход работы:**

1. Сгенерируйте 2 пароля для гипотетического доступа к корпоративной базе данных газового оборудования:

- пароль 1: 8 символов (минимум 1 цифра, 1 заглавная буква);
- пароль 2: 12+ символов (с символами `!@#$%`).

2. Запишите их в текстовый файл «Пароли_учебные.txt».
3. Заархивируйте файл с паролем (используйте WinRAR/7-Zip, установите пароль архива — например, `Student2026!`).
4. Удалите исходный текстовый файл.
5. В отчёте укажите: длина паролей, сложность, метод хранения (архив с паролем).

Контрольные вопросы (ответы написать в отчет)

1. Какие меры безопасности реализованы на учебных ПК вашего кабинета?
2. Почему нельзя сохранять пароли на общих компьютерах?
3. Как HTTPS защищает данные при поиске технической документации?
4. Какие признаки фишинга вы обнаружили в задании 3?
5. Какие угрозы наиболее опасны для специалистов газовой отрасли при работе в Интернете?
6. Почему использование HTTPS критично для доступа к корпоративным ресурсам?
7. Как двухфакторная аутентификация повышает безопасность учётных записей?
8. В чём преимущества VPN при удалённом мониторинге оборудования?
9. Назовите 3 признака фишингового письма.

Вывод

В ходе работы освоены методы защиты данных в условиях учебного кабинета, актуальные для сферы газового оборудования. Подтверждена необходимость:

- регулярного обновления ПО на учебных ПК;
- использования HTTPS и VPN для доступа к ресурсам;
- обучения навыкам распознавания фишинга.
  Разработаны рекомендации для безопасной работы студентов и преподавателей.

Рекомендации для учебного кабинета

1. Проводить ежемесячную проверку обновлений ПО на всех ПК.
2. Использовать групповые политики Windows для запрета сохранения паролей.
3. Организовать обучающие семинары по кибербезопасности 2 раза в год.
4. Ограничить доступ к ненадёжным сайтам через настройки прокси-сервера.
5. Хранить учебные материалы только на защищённых сетевых дисках.

Список литературы

1. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности».
2. Методические рекомендации ФСТЭК России по защите учебных информационных систем.
3. Официальные руководства производителей газового оборудования (Siemens, Emerson и др.).

Форма отчёта:

- титульный лист;
- цель, задачи;
- таблицы и результаты заданий 1–4;
- ответы на контрольные вопросы;
- вывод.

Приложение 1

Письмо 1

Тема: СРОЧНО: Блокировка аккаунта поставщика оборудования!

Уважаемый пользователь,

Ваш аккаунт на портале поставщика газового оборудования **GasTech-Supply** будет заблокирован через 24 часа из-за нарушения правил использования.

Для подтверждения аккаунта и предотвращения блокировки перейдите по ссылке:

В случае игнорирования данного сообщения доступ к технической документации и заказам будет ограничен.

С уважением,
Служба поддержки GasTech-Supply

P.S. Не пересылайте это письмо — оно отправлено автоматически.

Письмо 2

Тема: Обновление лицензий ПО для мониторинга газового оборудования

Здравствуйте,

Компания **Emerson Automation** уведомляет о необходимости срочного обновления лицензий на ПО для систем мониторинга. Устаревшие версии ПО представляют угрозу безопасности промышленных объектов.

Скачайте патч безопасности по ссылке:

Файл весит 2,3 МБ. Запустите его сразу после загрузки.

Если вы не обновите ПО до 25.10.2024, система мониторинга может быть отключена автоматически.

Техническая поддержка Emerson

Контактный телефон: +7 (999) 123-45-67 (не для общих вопросов)

Письмо 3

Тема: Доступ к обновлённой документации по газовому оборудованию

Добрый день,

Информируем вас о публикации обновлённой технической документации по серии газовых котлов **Protherm Gepard**.

Что нового:

- актуализированные схемы подключения;
- обновлённые параметры настройки давления;
- рекомендации по обслуживанию в зимний период.

Документы доступны в вашем личном кабинете на официальном портале:

Логин: ваш корпоративный email
Пароль: [ваш пароль]

При возникновении вопросов обращайтесь в техническую поддержку:

Тел.: 8 (800) 100-20-30

С уважением,
Команда Protherm

Письмо 4

Тема: Уведомление о плановом техобслуживании ПО

Уважаемые пользователи,

Сообщаем о плановом обновлении программного обеспечения системы мониторинга **Siemens SCADA** версии 4.2.

Дата и время обновления: 20.10.2024 с 02:00 до 04:00 (МСК).
На этот период возможен кратковременный перерыв в работе веб-интерфейса.

Что нужно сделать:

1. Сохраните все текущие данные до 19.10.2024 23:00.
2. После обновления проверьте работоспособность системы.
3. При обнаружении ошибок сообщите в техподдержку.

Официальный источник информации:

С уважением,
Отдел технической поддержки Siemens

Письмо 5

Тема: Приглашение на вебинар «Безопасность газовых систем»

Добрый день, [Имя Отчество]!

Приглашаем вас на бесплатный вебинар от компании **Honeywell** на тему: **«Современные методы защиты промышленных газовых систем от кибератак»**.

Дата: 25.10.2024
Время: 11:00–13:00 (МСК)
Формат: онлайн (Zoom)

Программа:

- анализ актуальных угроз для газовых систем;
- демонстрация работы защищённого ПО Honeywell Safety Suite;
- ответы на вопросы.

Регистрация по ссылке:

После регистрации вы получите ссылку на подключение.

Контактное лицо: Анна Смирнова
Email:
Тел.: +7 (495) 777-88-99

С уважением,
Команда Honeywell Россия

Письмо 6

Тема: Внимание! Подозрительная активность в вашем аккаунте поставщика запча стей

Уважаемый клиент,

Система безопасности зафиксировала попытку входа в ваш аккаунт на портале **G asParts Online** с неизвестного устройства (IP: 185.211.45.192, страна: Китай).

Если это были не вы, срочно смените пароль:

Перейдите по ссылке для подтверждения личности и сброса пароля:

В противном случае аккаунт будет заблокирован в течение 12 часов для защиты в аших данных.

Не отвечайте на это письмо — оно отправлено автоматически.

Служба безопасности GasParts Online

Письмо 7

Тема: Важное уведомление: штраф за нарушение лицензионных соглашений

Здравствуйте,

На ваше имя выписан административный штраф в размере 15 000 руб. за использ ование нелицензионного ПО для управления газовым оборудованием (нарушение ст. 7.12 КоАП РФ).

Для отмены штрафа и разблокировки системы оплатите сбор 3 000 руб. через защ ищённый платёжный шлюз:

После оплаты штраф будет аннулирован автоматически. В случае неуплаты мате риалы будут переданы в правоохранительные органы.

С уважением,
Отдел лицензирования ПО

Контактный номер: +7 (999) 888-77-66

Письмо 8

Тема: Обновление прошивки контроллера газового котла Baxi Luna 3

Добрый день, уважаемый владелец оборудования Baxi!

Компания **Baxi** информирует о выпуске обновления прошивки версии 2.15 для кон троллеров серии **Luna 3**.

Что нового:

- улучшена стабильность работы при низких температурах (до −25 °C);
- оптимизирован алгоритм модуляции пламени;
- исправлены ошибки в протоколе обмена данными.

Инструкция по обновлению:

1. Скачайте файл прошивки с официального портала:

2. Подключите USB-накопитель к контроллеру.
3. Запустите обновление через меню «Сервис → Обновление ПО».

   Важно: перед обновлением сохраните текущие настройки.

   При возникновении вопросов обращайтесь:

- горячая линия Baxi: 8 (800) 500-03-03;
- email: .

  С уважением,
  Техническая поддержка Baxi Россия

  Письмо 9

  Тема: Напоминание: семинар по обслуживанию газовых котлов Viessmann

  Уважаемый [Имя Отчество],

  Напоминаем, что завтра, **22.10.2024**, состоится практический семинар: **«Техническое обслуживание конденсационных газовых котлов Viessmann Vitodens»**.

  Место: конференц-зал отеля «Парк Инн», г. Москва, ул. Тверская, д. 15.
  Время: 10:00–16:00 (МСК), с перерывом на обед.

  Программа:

- разбор типовых неисправностей;
- демонстрация замены ключевых узлов;
- отработка навыков диагностики на стенде.

  Для участников:

- раздаточные материалы;
- сертификат о прохождении обучения;
- кофе-брейк и обед.

  Регистрация обязательна. Если вы не сможете присутствовать, сообщите об этом до 21.10.2024 18:00.

  Контакты организаторов:

- координатор: Мария Иванова;

- тел.: +7 (495) 123-45-67;
- email: .

С уважением,
Учебный центр Viessmann

Письмо 10

Тема: Доступ к личному кабинету системы мониторинга «Газовая безопасность 36 5»

Здравствуйте, [Имя]!

Ваш аккаунт в системе удалённого мониторинга **«Газовая безопасность 365»** усп ешно активирован.

Данные для входа:

- логин: [ваш email];
- пароль: [временный пароль, например, GS365_Temp2024];
- ссылка на вход: .

Рекомендации после первого входа:

1. Смените временный пароль в разделе «Профиль → Безопасность».
2. Настройте уведомления о критических событиях.
3. Добавьте контакты ответственных лиц.

Функционал системы:

- онлайн-мониторинг давления газа;
- сигнализация утечек;
- архивы данных за 3 месяца.

Техническая поддержка:

- круглосуточно: 8 (800) 700-80-90;
- email: .

С уважением,
Команда «Газовая безопасность»

Приложение 2

Сравнительная таблица признаков

Признак	Фишинговые письма	Легитимные письма
Тон сообщения	Давление, угрозы («заблокируют», «штраф», «срочно»)	Информативный, нейтральный («информируем», «напоминаем», «приглашаем»)
Ссылки	Подозрительные домены (`secure-login.net`, `gosuslugi-oplata.ru`), короткие URL	Официальные домены компаний (`.ru`, `.com`), понятные пути
Персонализация	Общая («Уважаемый клиент», «Здравствуйте»)	Конкретная (имя, номер договора, модель оборудования)
Действия	Требуют немедленных действий, загрузки .exe, оплаты	Предлагают инструкции, дают время на реакцию
Контакты	Отсутствуют или поддельные номера	Полные данные поддержки (email, телефоны, адреса)
Детали	Общие фразы, ошибки, опечатки	Чёткие даты, версии ПО, технические детали

Ключевые отличия, которые помогут распознать фишинг:

- **Фишинговые:**
  - срочность и давление («заблокируют через 24 часа», «до 25.10»);
  - подозрительные ссылки (опечатки в доменах: `gasteh`, `emerson-update`);
  - отсутствие персонализации («Уважаемый пользователь»);
  - просьбы скачать исполняемые файлы (.exe) по ссылкам;
  - общие формулировки без деталей.
- **Легитимные:**
  - чёткая структура и детализация (даты, версии ПО, программы);

- официальные домены компаний (`.ru`, `.com` с правильным написанием);
- контактные данные поддержки;
- отсутствие давления — акцент на информировании;
- ссылки ведут на официальные порталы, а не на прямые загрузки .exe.