Лабораторная 3

Таблица 1

Объект защиты	Нарушение целостности	Нарушение доступности	Нарушение конфиденциальности
База данных жителей	Изменение данных о прописке, семейном положении или дате рождения	Блокировка доступа к базе, DDoS-атака на сервер	Утечка персональных данных (ФИО, адреса, паспортные данные)
Система видеонаблюдения	Внедрение ложных записей или изменение записанных видеоданных	Вывод из строя камер или серверов хранения видеозаписей	Неавторизованный доступ к видеоархивам
Система оповещения	Изменение текстов экстренных сообщений	Нарушение работы системы уведомлений через DDoS или сбои в оборудовании	Утечка информации о готовящихся уведомлениях или списках сотрудников, управляющих системой
Система ЖКХ	Подмена данных о потреблении ресурсов	Отключение серверов управления системами отопления, водоснабжения, электропитания	Доступ к персональным данным жителей через счета на оплату
База пользователей систем	Изменение учетных данных, в том числе паролей	Массовая блокировка доступа к учетным записям	Кража учетных записей пользователей
Система реагирования на ЧП	Нарушение маршрутов экстренного реагирования	Отключение системы реагирования на ЧП	Утечка информации о запланированных мероприятиях, маршрутах экстренных служб
Система управления транспортной инфраструктурой	Изменение сигналов светофоров, маршрутов общественного транспорта	Вывод из строя серверов управления, нарушение работы светофорной сети	Утечка информации о расписаниях транспорта, конфиденциальных данных пользователей
Система "Госуслуги"	Внесение изменений в документы, которые	Невозможность доступа граждан к важным государственным	Утечка данных пользователей, включая паспорта, заявления, медицинские данные

	предоставляют пользователи	услугам	
Электронные записи медицинского лечения	Подмена информации о лечении пациентов	Нарушение доступа к данным врачей и пациентов	Утечка медицинской информации пациентов
Информация об энергетической инфраструктуре	Изменение данных о работе энергосетей	Нарушение управления энергетическими сетями, отключение энергоснабжения	Утечка информации о критической инфраструктуре города

Таблица 2

Информационные ресурсы	**Наиболее серьезные последствия**	**Сценарий**
База данных жителей	Массовая утечка персональных данных, использование их для мошенничества или шантажа	1. Получение доступа к системе через фишинг. 2. Извлечение базы данных. 3. Продажа или публикация данных в открытом доступе.
Система видеонаблюдения	Компрометация безопасности города, утечка видеозаписей	1. Уязвимость в программном обеспечении камеры. 2. Захват управления системой. 3. Извлечение или подмена видеозаписей.
Система реагирования на ЧП	Срыв экстренных мероприятий, угроза жизни и здоровью людей	1. Атака на маршрутизаторы управления. 2. Изменение маршрутов реагирования. 3. Нарушение или блокировка системы связи служб.
Система управления транспортной инфраструктурой	Нарушение транспортных потоков, создание аварийных ситуаций	1. Внедрение вредоносного ПО в систему управления. 2. Изменение сигналов светофоров. 3. Нарушение расписания движения общественного транспорта.

Электронные записи медицинского лечения	Нарушение лечения пациентов, угроза жизни и здоровью	1. Получение доступа через взлом учетных записей врачей. 2. Изменение информации о лечении. 3. Прерывание медицинской помощи пациентам.
Информация об энергетической инфраструктуре	Нарушение энергоснабжения города, массовые аварии	1. Анализ открытых данных об энергосети. 2. Подбор уязвимостей в ПО управления. 3. Вывод из строя оборудования или нарушение энергопотока.
Система "Госуслуги"	Потеря доступа к государственным услугам, массовая утечка данных граждан	1. Проведение DDoS-атаки на систему. 2. Сбор данных через уязвимость API. 3. Нарушение функционирования сервисов предоставления услуг.

Таблица 3

Этап тестирования	**Описание действий**	**Ожидаемый результат**
Подготовка фишинговой кампании	Создание фальшивого электронного письма или веб-сайта, имитирующего реальный источник	Фишинговый контент выглядит максимально достоверно, чтобы не вызывать подозрений у сотрудников.
Отправка фишинговых сообщений	Рассылка фальшивых писем определенной группе сотрудников	Проверка, сколько сотрудников откроют сообщение и перейдут по ссылке.
Сбор данных об откликах сотрудников	Отслеживание переходов по ссылкам и действий, например, ввода учетных данных	Идентификация сотрудников, которые не прошли тест на фишинг.
Анализ поведения сотрудников	Анализ причин, по которым сотрудники открыли письма (недостаток знаний, невнимательность и т.д.)	Определение факторов, способствующих успешным фишинговым атакам.

Подведение итогов и обучение	Проведение разъяснительной работы и обучение сотрудников, основываясь на результатах тестирования	Сотрудники получают навыки распознавания фишинговых атак, улучшаются показатели осведомленности в области кибербезопасности.
Повторное тестирование	Проведение аналогичного тестирования через определенный промежуток времени	Проверка уровня усвоенных знаний и закрепление правильного поведения.

Таблица 4

Название должности	**Пример целевого фишингового письма**	**Эмоции от письма**
Администрация городов	"Уважаемый сотрудник, ваше обращение в поддержку по поводу обновления прав доступа одобрено. Для подтверждения перейдите по ссылке [фальшивая ссылка]."	Уверенность, срочность, желание завершить задачу
Полиция	"Внимание! Обнаружена утечка данных, связанных с вашими учетными записями. Пройдите срочно проверку безопасности по ссылке [фальшивая ссылка]."	Паника, тревога, желание устранить проблему
Службы города	"На складе доступны последние комплекты спецодежды. Чтобы выбрать комплект и зарезервировать его, перейдите по ссылке [фальшивая ссылка]."	Удивление, радость от "подарка", желание не упустить возможность
МЧС	"Срочное уведомление! Изменения в протоколах реагирования на ЧП. Ознакомьтесь с новыми инструкциями, перейдя по ссылке [фальшивая ссылка]."	Срочность, чувство долга, желание выполнить профессиональные задачи
Пользователи системы управления транспортом	"Сообщение от службы поддержки: в вашей системе выявлены уязвимости. Для их устранения загрузите патч по ссылке [фальшивая ссылка]."	Тревога, срочность, желание защитить систему
Граждане	"Вы выиграли бесплатный проездной на общественный транспорт на месяц! Для активации нажмите [фальшивая ссылка]."	Радость, желание воспользоваться "подарком"

Таблица 5

ИР для защиты	**Сценарии нарушителей**
База данных жителей	Злоумышленники используют технику *Initial Access* (Phishing: Spear Phishing Link) для получения учетных данных сотрудника, а затем

	применяют *Credential Dumping* для полного доступа к базе.
Система видеонаблюдения	Атака через *Execution* (Command and Scripting Interpreter: PowerShell) для внедрения вредоносного кода, который позволяет перехватить поток видеозаписей и отключить камеры.
Система управления транспортной инфраструктурой	Использование *Persistence* (Boot or Logon Autostart Execution: Registry Run Keys) для установки долгосрочного доступа, нарушение управления светофорами и транспортных систем.
Система "Госуслуги"	Атака через *Privilege Escalation* (Exploitation for Privilege Escalation) для получения администраторского доступа и кражи персональных данных пользователей системы.

Таблица 6

Недостатки	**Как исправить**
Оператор пульта охраны	
Использование ноутбука для несвязанных с работой задач (игра в пасьянс).	Ограничить доступ к нерабочим приложениям на рабочих устройствах, настроить контроль за действиями оператора.
Отсутствие физической защиты доступа к пульту видеонаблюдения (может быть легко украден или взломан).	Разместить оборудование в защищенном помещении с доступом по биометрии или картам сотрудников.
Комната администраторов	
Использование личных приложений (Discord) на рабочем компьютере.	Установить политику запрета использования личных приложений на рабочих устройствах, провести обучение.
Наличие стикеров с информацией на мониторе (утечка данных).	Внедрить электронные напоминания, запретить хранение информации на бумажных носителях в рабочей зоне.
АРМ системного администратора	
Устаревшее оборудование (ЭЛТ монитор, старая операционная система).	Обновить оборудование, внедрить современные ОС с регулярными обновлениями безопасности.
Наклейки со стикерами на мониторе (потенциальная утечка конфиденциальной информации).	Обеспечить использование защищенных приложений для хранения заметок и запретить бумажные носители в зоне работы.

Таблица 7

Недостатки	**Как исправить**
Пользователи устанавливают пароли вручную и могут использовать слабые или простые	Внедрить требования к сложности паролей: длина не менее 12 символов, использование

пароли.	букв, цифр и спецсимволов.
Один пароль используется во всех системах, что увеличивает риск компрометации всех систем при утечке.	Обеспечить уникальность паролей для каждой системы, внедрить менеджеры паролей для удобства сотрудников.
Пин-код к закрытой зоне меняется раз в месяц, что делает его уязвимым к запоминанию и утечкам.	Внедрить многофакторную аутентификацию (MFA) или динамические пин-коды с коротким сроком действия.
Одноразовый пароль к онлайн-банкингу можно узнать по телефону при предоставлении общедоступной информации.	Запретить выдачу паролей по телефону, использовать защищенные каналы связи для передачи паролей.
Аутентификация в серверную по отпечатку пальца недостаточно безопасна (возможны подделки отпечатков).	Дополнить биометрическую аутентификацию дополнительными факторами (пароль, токен).

Таблица 8

Элемент атаки	**Тактика по** MITRE	**Способ реализации нарушителем**	**№ техники по** MITRE	**Мера защиты**
Продажа личной информации	Exfiltration	Передача данных через зашифрованный канал	T1041	Мониторинг сетевого трафика, внедрение DLP-систем для предотвращения утечки данных.
Навязанная реклама	Impact	Внедрение рекламного ПО в системы	T1485	Использование антивирусных решений, регулярные проверки целостности ПО, контроль источников ПО.
Продажа городской информации новостным каналам	Exfiltration	Скачивание и передача данных внешним покупателям	T1567	Ограничение доступа к критическим данным, настройка логирования доступа и оповещения об аномалиях.
Получение паролей администраторов	Credential Access	Использование кейлоггеров, подмена аутентификации	T1056, T1078	Многофакторная аутентификация, регулярная смена паролей, мониторинг активности учетных записей.
Копирование данных от имени фейковой	Collection	Создание учетной записи с фейковым	T1078	Ограничение прав доступа новых учетных записей,

организации		именем		обязательное подтверждение личности администратора.

Таблица 9

№ политики (из ISO 27001)	**Название**	**Текущее состояние объекта**	**Действия для формирования политики объекта**
A.5	Политики информационной безопасности	Отсутствует утвержденная политика, регламентирующая все аспекты информационной безопасности.	Разработать, утвердить и внедрить политику информационной безопасности, довести до сотрудников и контролировать выполнение.
A.6.1	Внутренняя организация деятельности по обеспечению информационной безопасности	Отсутствует четкое распределение ролей и обязанностей в области информационной безопасности.	Определить и задокументировать роли и обязанности в области информационной безопасности, назначить ответственных лиц.
A.9	Управление доступом	Политики управления доступом не формализованы, доступ предоставляется без должного контроля.	Разработать и внедрить политику управления доступом, включая процедуры предоставления, изменения и отзыва доступа.
A.12.6.2	Ограничения на установку программного обеспечения	Пользователи могут самостоятельно устанавливать программное обеспечение, что повышает риски безопасности.	Ввести ограничения на установку ПО, разрешив установку только авторизованного ПО через утвержденные процедуры.
A.14.2.1	Политика безопасной разработки	Отсутствуют стандарты и процедуры для обеспечения безопасности в процессе разработки программного обеспечения.	Разработать и внедрить политику безопасной разработки, включающую требования по безопасности на всех этапах жизненного цикла ПО.

Таблица 10

Информационные	**Меры по защите**

ресурсы	
База данных клиентов	**Ранее примененные меры:** Шифрование данных, контроль доступа, регулярное резервное копирование. **Добавленные меры:** Внедрение политики управления доступом (A.9.1), ограничение на установку ПО (A.12.6.2), политика безопасной разработки (A.14.2.1).
Система управления проектами	**Ранее примененные меры:** Аутентификация пользователей, контроль версий документов. **Добавленные меры:** Определение ролей и обязанностей в области ИБ (A.6.1.1), политика информационной безопасности (A.5.1).
Финансовые отчеты компании	**Ранее примененные меры:** Ограничение доступа, шифрование файлов. **Добавленные меры:** Управление доступом (A.9.1), политика информационной безопасности (A.5.1), ограничения на установку ПО (A.12.6.2).
Персональные данные сотрудников	**Ранее примененные меры:** Хранение в защищенном хранилище, ограничение доступа. **Добавленные меры:** Политика управления доступом (A.9.1), определение ролей и обязанностей в области ИБ (A.6.1.1), политика безопасной разработки (A.14.2.1).
Конфиденциальная переписка	**Ранее примененные меры:** Шифрование электронной почты, использование защищенных каналов связи. **Добавленные меры:** Политика информационной безопасности (A.5.1), управление доступом (A.9.1), ограничения на установку ПО (A.12.6.2).

Таблица 11

Инф. ресурсы	Сценарии нарушителей	Обоснование достаточности мер
База данных жителей	Кража и продажа персональных данных, манипуляция данными для подрыва доверия к системе.	Шифрование данных и разграничение доступа обеспечивают защиту. Добавленные меры мониторинга угроз усиливают контроль. Однако регулярные тесты на проникновение могут повысить уровень защищенности.
Система видеонаблюдения	Подмена или удаление видеозаписей, захват контроля над системой для слежки.	Физическая защита серверных и шифрование трафика достаточны для предотвращения большинства атак. Установленные дополнительные

		меры аудита и проверок закрывают оставшиеся уязвимости.
Система управления транспортной инфраструктурой	Нарушение работы светофоров, создание транспортных коллапсов, отправка ложных данных водителям.	Фильтрация трафика и аудит действий защищают от атак. Дополнительные процессы управления инцидентами усиливают готовность к реагированию на сложные сценарии.
Электронные записи медицинского лечения	Кража данных пациентов для шантажа, подделка информации о лечении, уничтожение записей для дискредитации системы здравоохранения.	Шифрование данных и двухфакторная аутентификация создают надежную защиту. Новые меры мониторинга на соответствие законодательству обеспечивают долгосрочную устойчивость и соблюдение правовых норм.
Информация об энергетической инфраструктуре	Захват управления энергетическими объектами, выведение из строя системы, предоставление ложной информации о состоянии объектов для создания паники или дезинформации.	Охрана периметра и ограничение подключений снижают вероятность атак. Управление инцидентами помогает быстро реагировать на попытки взлома или дестабилизации системы.