МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение   
высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ им. В. И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

Кафедра компьютерной инженерии и моделирования

**ОТЧЕТ ПО ПРАКТИЧЕСКОМУ ЗАДАНИЮ №6**

Практическая работа по дисциплине

«Основы информационной безопасности»

студента 3 курса группы ИВТ-б-о-221

Гуреева Кирилла Александровича

09.03.01 «Информатика и вычислительная техника»

Симферополь 2024

**Общие сведения о заведении**

Компания "Инновационные Решения Данных" (ИРД) – это динамично развивающаяся компания, специализирующаяся на разработке и внедрении передовых решений в области анализа и обработки данных. Основная цель компании – предоставлять высококачественные услуги и продукты, помогающие клиентам принимать обоснованные решения на основе данных.

Штат компании насчитывает 120 сотрудников, из которых 40 человек – это разработчики программного обеспечения, 30 – аналитики данных, 20 – специалисты по информационной безопасности, а оставшиеся 30 – административный и вспомогательный персонал. Компания имеет несколько офисов в разных регионах России.

**Описание инфраструктуры компании**

Инфраструктура компании состоит из ЦОД на 5 серверов с хранилищами по 100 ТБ, на серверах установлен Linux Server. 300 рабочих станций с установленной Ubuntu Desktop используются разработчиками, аналитиками и административным персоналом. Существует основная корпоративная сеть, обеспечивающая высокоскоростное подключение для всех стационарных устройств. Также имеется гостевая беспроводная сеть для посетителей. Корпоративная беспроводная сеть разделена на несколько VLAN для разграничения доступа различных отделов. Для обеспечения безопасности используются межсетевые экраны нового поколения, системы обнаружения и предотвращения вторжений (IDS/IPS), а также решения для защиты от утечек данных (DLP).

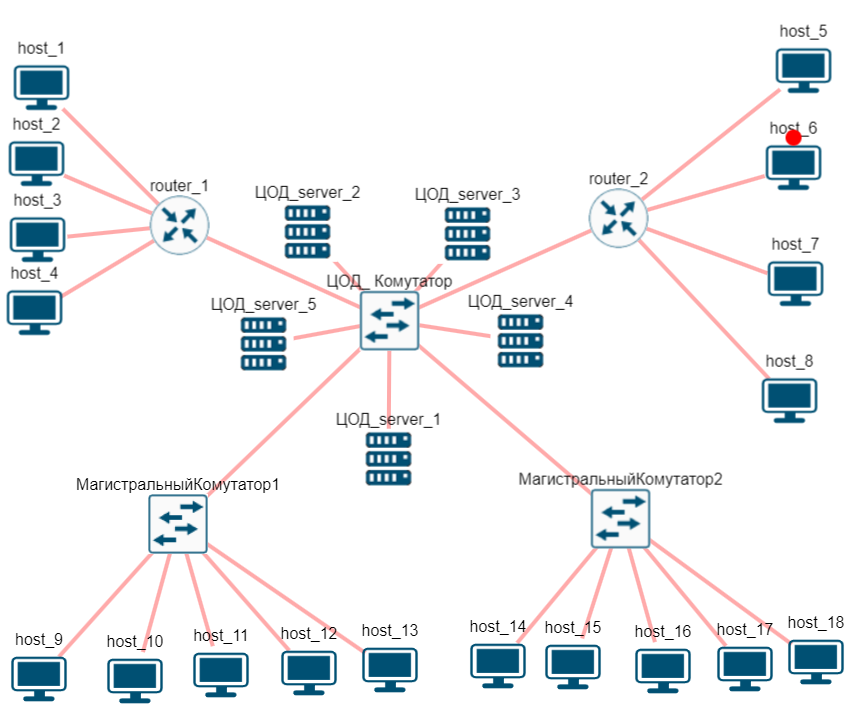


Рис. 1. Общая схема топологии сети.

**Требования к экспертам**

Для проведения оценки безопасности компании необходимы эксперты, к ним предъявляются следующие требования:

Оконченное высшее образование в сфере информационных технологий или информационной безопасности.

Подходящие направления – информационная безопасность (10.05.01), безопасность компьютерных систем (10.05.05), прикладная математика и информатика (02.03.02) со специализацией в области безопасности.

Опыт работы в сфере информационной безопасности не менее 5 лет.

Знание основных типов уязвимостей и методов их эксплуатации, а также современных методов защиты, подтвержденные сертификатами CISSP, OSCP, Security+.

Уверенные навыки работы с инструментами для анализа защищенности (например, Nessus, Burp Suite, Metasploit). Базовый набор – Nmap, Wireshark, OpenVAS.

**Анализируемые аспекты**

- защита данных, тестирование баз данных клиентов и внутренних систем, оценка политик доступа к данным, проверка наличия и анализа журналов аудита, оценка методов шифрования данных при хранении и передаче;

- защищенность сети, анализ конфигурации межсетевых экранов и правил доступа, проверка на наличие уязвимостей в сетевом оборудовании, анализ сегментации сети и контроля доступа;

- безопасность приложений, анализ безопасности веб-приложений и внутренних приложений на наличие уязвимостей (например, OWASP Top 10).

- управление доступом, оценка политик паролей, многофакторной аутентификации, ролевой модели доступа;

- реагирование на инциденты, оценка планов реагирования на инциденты, процедур восстановления после сбоев;

- проверка соответствия политик компании законодательству и нормативным актам;

- проверка физических устройств и аппаратных средств на наличие программных закладок, актуальных версий ПО, а также соответствие стандартам и нормативным документам ДИБ;

- проверка программных средств и решений на наличие вредоносного кода и соответствием стандартам и нормативным документам ДИБ.

Табл. 1. Матрица парных сравнений.

| Аспекты/Сравнение | Защита данных | Защита сети | Безопасность приложений | Управление доступом | Реагирование на инциденты | Соответствие законодательным требованиям |
| --- | --- | --- | --- | --- | --- | --- |
| Защита данных | 1 | 4 | 6 | 5 | 7 | 8 |
| Защита сети | 1/4 | 1 | 5 | 3 | 6 | 7 |
| Безопасность приложений | 1/6 | 1/5 | 1 | 1/3 | 4 | 5 |
| Управление доступом | 1/5 | 1/3 | 3 | 1 | 5 | 6 |
| Реагирование на инциденты | 1/7 | 1/6 | 1/4 | 1/5 | 1 | 3 |
| Соответствие законодательным требованиям | 1/8 | 1/7 | 1/5 | 1/6 | 1/3 | 1 |

Шаги для расчета согласованности

1. Нормализованная матрица - для каждой колонки матрицы делим каждый элемент колонки на сумму всех элементов этой колонки.

Таблица 2. Нормализованная матрица.

| Аспекты/Сравнение | Защита данных | Защита сети | Безопасность приложений | Управление доступом | Реагирование на инциденты | Соответствие законодательным требованиям |
| --- | --- | --- | --- | --- | --- | --- |
| Защита данных | 0.382 | 0.383 | 0.436 | 0.320 | 0.383 | 0.278 |
| Защита сети | 0.127 | 0.128 | 0.109 | 0.160 | 0.128 | 0.167 |
| Безопасность приложений | 0.191 | 0.255 | 0.218 | 0.240 | 0.255 | 0.222 |
| Управление доступом | 0.096 | 0.064 | 0.073 | 0.080 | 0.064 | 0.111 |
| Реагирование на инциденты | 0.127 | 0.128 | 0.109 | 0.160 | 0.128 | 0.167 |
| Соответствие законодательным требованиям | 0.076 | 0.043 | 0.055 | 0.040 | 0.043 | 0.056 |

2. Приоритетный вектор - средние значения нормализованных строк.

3. Собственное значение каждого элемента - умножаем исходную матрицу на приоритетный вектор. Этот параметр отражает насколько хорошо согласованы,

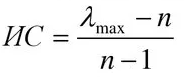
Таблица 3. — собственные значения и приоритеты в оценке факторов безопасности

|  |  |  |  |
| --- | --- | --- | --- |
| Аспект | Собственное значение | Приоритетный вектор | Результат деления (Собственное значение / Приоритет) |
| Защита данных | 2.227 | 0.364 | 6.118 |
| Защита сети | 0.827 | 0.136 | 6.081 |
| Безопасность приложений | 1.409 | 0.230 | 6.126 |
| Управление доступом | 0.489 | 0.081 | 6.037 |
| Реагирование на инциденты | 0.827 | 0.136 | 6.081 |
| Соответствие законодательным требованиям | 0.314 | 0.052 | 6.038 |

3. Собственное значение матрицы (λmax) - Среднее значение собственных значений элементов:

λmax = 6.073

4. Индекс согласованности (ИС):



(1)

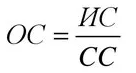
где ИС — индекс согласованности,

λmax — собственное значение матрицы,

n — количество критериев.

ИС = (6.073 - 6) / (6 - 1) = 0.073 / 5 = 0.015

5. Отношение согласованности (ОС):



(2)

где ОС — отношение согласованности,

ИС — индекс согласованности,

СС — математическое ожидание индекса согласования (для матрицы 6x6 СС = 1.24).

ОС = 0.015 / 1.24 = 0.012

Так как значение CR составляет 0.012, что значительно меньше 0.1, можно сделать вывод, что матрица является хорошо согласованной.

Негативные последствия реализации угроз безопасности информации.

1. Утечка данных.

- Несанкционированный доступ и утечка конфиденциальных данных компании, включая персональные данные клиентов, финансовые отчеты, коммерческие тайны.

- Репутационные потери, утрата доверия со стороны клиентов и партнеров, финансовые потери, юридические последствия и штрафы за нарушение законодательства о защите данных.

2. Кибератаки.

- Вредоносные действия со стороны хакеров, включая DDoS-атаки, атаки типа "человек посередине" (MitM), SQL-инъекции и XSS-атаки на веб-приложения.

- Нарушение работы критически важных бизнес-процессов, финансовые потери из-за простоя, компрометация конфиденциальной информации, необходимость восстановления систем.

3. Потеря данных.

- Утрата или повреждение важных данных из-за недостаточного резервного копирования, сбоев оборудования или программного обеспечения.

- Задержки в обслуживании клиентов, финансовые потери из-за невозможности доступа к данным, утрата важной бизнес-информации.

4. Нарушение доступности сервисов.

- Атаки, приводящие к недоступности критически важных сервисов и приложений компании для сотрудников и клиентов.

- Простой в работе, финансовые потери, недовольство клиентов, ущерб репутации.

5. Компрометация учетных записей.

- Получение несанкционированного доступа к учетным записям сотрудников с высокими привилегиями.

- Возможность доступа к конфиденциальной информации, изменение критических настроек, проведение несанкционированных операций.

**Описание модели угроз**

Классификации угроз безопасности информации для компании.

По виду защищаемой от угроз безопасности информации:

- конфиденциальная информация (персональные данные клиентов и сотрудников, финансовые данные, коммерческие тайны, интеллектуальная собственность);

- целостность данных (данные о транзакциях, конфигурационные файлы, исходный код программного обеспечения);

- доступность сервисов (веб-сайт компании, CRM-система, системы управления базами данных, электронная почта).

По видам возможных источников угроз безопасности:

- внутренний нарушитель (сотрудники компании, бывшие сотрудники с сохранившимся доступом);

- внешний нарушитель (хакеры, киберпреступники, конкуренты, использующие интернет для атак);

- стихийные бедствия и техногенные катастрофы (пожары, наводнения, отключения электроэнергии, аппаратные сбои).

По способу реализации угроз безопасности:

- несанкционированный доступ (попытки обхода механизмов аутентификации и авторизации);

- вредоносное программное обеспечение (вирусы, трояны, черви, программы-вымогатели).

- социальная инженерия (фишинг, убеждение сотрудников выдать конфиденциальную информацию);

- уязвимости программного обеспечения (использование известных и неизвестных уязвимостей в приложениях и операционных системах).

Табл. 4. Возможные цели реализации угроз

| № | Виды нарушителей | Категории | Возможные цели |
| --- | --- | --- | --- |
| 1 | Конкуренты | Внешний | Получение коммерческих тайн, нарушение работы сервисов, дискредитация компании. |
| 2 | Киберпреступники | Внешний | Получение финансовой выгоды (вымогательство, кража данных для продажи), использование ресурсов компании для вредоносных действий. |
| 3 | Хактивисты | Внешний | Проведение атак по идеологическим мотивам, привлечение внимания к определенным проблемам. |
| 4 | Недовольные сотрудники | Внутренний | Месть, получение выгоды от продажи данных, нанесение ущерба репутации компании. |
| 5 | Случайные пользователи (сотрудники) | Внутренний | Непреднамеренные действия, случайная потеря данных, заражение вредоносным ПО. |
| 6 | Бывшие сотрудники | Внешний | Месть, использование оставшихся доступов для получения информации или нанесения вреда. |

Таблица 5. Уровни возможностей нарушителей

| № | Уровень возможностей нарушителей | Возможности нарушителей по реализации угроз безопасности информации | Виды нарушителей |
| --- | --- | --- | --- |
| H1 | Нарушитель, обладающий базовыми возможностями | Использует известные уязвимости, простые скрипты и общедоступные инструменты. | Случайные пользователи (сотрудники) |
| H2 | Нарушитель, обладающий повышенными возможностями | Использует более сложные инструменты, может модифицировать скрипты, знаком с фреймворками. | Недовольные сотрудники, опытные бывшие сотрудники |
| H3 | Нарушитель, обладающий средними возможностями | Может разрабатывать собственные эксплойты, использует уязвимости нулевого дня. | Киберпреступники, некоторые хактивисты |
| H4 | Нарушитель, обладающий высокими возможностями | Имеет доступ к ресурсам государства, высококвалифицированные специалисты, скоординированные атаки. | Конкуренты (с привлечением специалистов), государственные структуры |

Таблица 6. Меры защиты от реализации угроз

| № | Уровень возможностей нарушителей | Меры защиты |
| --- | --- | --- |
| H1 | Нарушитель, обладающий базовыми возможностями | Обучение сотрудников основам информационной безопасности, своевременное обновление ПО, использование антивирусного ПО. |
| H2 | Нарушитель, обладающий повышенными возможностями | Внедрение систем обнаружения и предотвращения вторжений (IDS/IPS), усиление контроля доступа, регулярные проверки безопасности. |
| H3 | Нарушитель, обладающий средними возможностями | Проведение анализа защищенности (penetration testing), использование средств защиты веб-приложений (WAF), сегментация сети. |
| H4 | Нарушитель, обладающий высокими возможностями | Комплексный подход к безопасности, включающий все предыдущие меры, мониторинг безопасности в режиме реального времени, сотрудничество с CERT. |