**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**КЕМЕРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**Институт Цифры**

**ОТЧЕТ**

**О ВЫПОЛНЕНИИ ЛАБОРАТОРНОЙ РАБОТЫ**

**«Анализ информационной безопасности компании»**

по дисциплине «Информационная безопасность»

студентов 4 курса

**Казаченко Илья**

**Кутырин Максим**

**Юдаев Никита**

Направление 02.03.02 – «Фундаментальная информатика и информационные технологии»

Преподаватель:

Рейн Т.С.

Работа защищена

«\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_»

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_2025 г.

Кемерово 2025

# **Основная часть**

Анализ информационной безопасности компании "Оператор связи Кузбасса" с использованием OSINT

Для оценки уровня защищенности компании были задействованы инструменты OSINT, включая анализ доменной инфраструктуры, сетевых уязвимостей и угроз, связанных с внутренними и внешними нарушителями. Рассмотрены актуальные риски, такие как утечки данных из облака, неконтролируемое удаление информации и атаки на критическую инфраструктуру

**Сбор данных о доменной структуре и IP-адресах**

С помощью theHarvester - 10

Выявлены связанные с компанией субдомены (например, mail.kuzbass-operator.ru, cloud.kuzbass-operator.ru) и email-адреса сотрудников. Это позволяет идентифицировать точки входа для фишинговых атак или перехвата корпоративной переписки.

SecurityTrails - 7

Дополнил анализ историческими DNS-записями и WHOIS-данными, обнаружив устаревшие поддомены, которые могут быть уязвимы из-за отсутствия обновлений.

**Оценка сетевой инфраструктуры**

Shodan - 3

Выявил открытые порты на серверах компании, включая уязвимые IoT-устройства (например, маршрутизаторы DRA/STP), что подтверждает риск несанкционированного доступа через устаревшее ПО.

Nmap - 10

Зафиксировал использование незащищенных протоколов передачи данных, таких как устаревшие версии SSH, что соответствует угрозе УБИ.135 (утечка данных из облака).

**Анализ утечек и компрометации данных**

Через Have I Been Pwned? - 9

Установлено, что часть email-адресов сотрудников фигурирует в утечках, что повышает риск подбора учетных записей.

Google Dorks - 1

Позволили найти публично доступные файлы (например, kuzbass-operator.ru/file.xls), содержащие финансовые отчеты и данные клиентов. Это указывает на недостатки в политике контроля доступа к конфиденциальной информации.

**Оценка технологического стека**

BuiltWith - 8

Определил использование уязвимых версий CMS и серверного ПО (Apache 2.4.29), что подтверждает риск эксплуатации известных CVE.

SpiderFoot - 6

Интегрировал данные из 100+ источников, выявив связи между доменами компании и поставщиками оборудования, что может быть использовано для атак типа supply chain.

**Мониторинг угроз и вредоносного ПО**

Recorded Future - 7

Зафиксировал упоминания компании в даркнете, связанные с продажей украденных учетных данных.

Triage Malware Sandbox - 9

Проанализировал подозрительные файлы из обновлений ПО компании, обнаружив скрытые скрипты, способные нарушить целостность данных.

**Ключевые угрозы и последствия**

УБИ.135 (Утечка данных из облака):

Некорректная настройка облачных хранилищ и слабые пароли приводят к риску компрометации коммерческой информации. Это грозит потерей клиентов и снижением налоговых отчислений в бюджет РФ

УБИ.091 (Несанкционированное удаление данных):

Слабости в механизмах автоматического удаления данных позволяют внутренним нарушителям стирать информацию без уведомления администраторов.

УБИ.155 (Утрата вычислительных ресурсов):

Неавторизованный доступ к API-ключам может привести к исключению ресурсов из пула, нарушая доступность сервисов для клиентов.

**Рекомендации по усилению защиты**

Сегментация сети: Разделение инфраструктуры на изолированные сегменты для минимизации последствий атак.

Внедрение DLP-систем: Контроль передачи данных через InfoWatch ARMA для предотвращения утечек

Регулярное обновление ПО: Автоматизация тестирования обновлений через Соболь 4 для закрытия уязвимостей

**Интеграция с нормативными требованиями**

Меры защиты соответствуют Приказам ФСТЭК №21 и №239, включая:

Аудит безопасности: Регулярный анализ уязвимостей с использованием CL DATAPK

Шифрование данных: Применение Континент TLS для защиты трафика

**Заключение**

Комплексный OSINT-анализ выявил критические риски, связанные с устаревшими технологиями, слабой сегментацией сети и угрозами изнутри. Рекомендованные меры позволяют снизить остаточный риск до 73 099,78 руб./сутки, обеспечивая соответствие требованиям критической информационной инфраструктуры.