МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное

образовательное учреждение высшего образования

«КРЫМСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ

ИМЕНИ В.И. ВЕРНАДСКОГО»

ФИЗИКО-ТЕХНИЧЕСКИЙ ИНСТИТУТ

ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОЕТ №6

ПО ДИСЦИПЛИНЕ

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСТНОСТИ»

студента 3 курса

группы ИВТ-б-о-222(1)

Гоголева Виктора

Симферополь, 2024

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc185946280)

[ОБЩАЯ ИНФОРМАЦИЯ О КОМПАНИИ 4](#_Toc185946281)

[Описание инфраструктуры организации 4](#_Toc185946282)

[Веб-сайты и приложения 5](#_Toc185946283)

[Требования к экспертам 6](#_Toc185946284)

[Анализируемые аспекты 7](#_Toc185946285)

[РАСЧЕТ И ПРОВЕРКА МАТРИЦЫ СРАВНЕНИЙ 9](#_Toc185946286)

[Матрица парных сравнений 9](#_Toc185946287)

[Нормированная матрица 10](#_Toc185946288)

[Собственные значения и приоритетный вектор 11](#_Toc185946289)

[Отношение согласованности (ОС) 12](#_Toc185946290)

[АУДИТ КОМПАНИИ «АВИАБИЛЕТИКС» 13](#_Toc185946291)

[Последствия реализации атаки на предприятие 13](#_Toc185946292)

[Описание модели угроз 14](#_Toc185946293)

[Возможные источники реализации угроз 16](#_Toc185946294)

[Уровни возможностей нарушителей 17](#_Toc185946295)

[Меры защиты компании для предотвращения и профилактики атак 18](#_Toc185946296)

[ЗАКЛЮЧЕНИЕ 19](#_Toc185946297)

# **ВВЕДЕНИЕ**

В современном мире обеспечение информационной безопасности (ИБ) является критически важной задачей для предприятий и организаций. Аудит информационной безопасности позволяет выявить слабые места в системе защиты данных и разработать меры по их устранению, что помогает минимизировать риски утечек данных и кибератак. Важно, чтобы внутренние политики и процедуры компании соответствовали законодательным требованиям и государственным нормативным актам, таким как стандарты ФСТЭК.

Целью данной работы является проведение комплексного аудита информационной безопасности компании "Авиабилетикс". Для достижения этой цели были поставлены следующие задачи:

* выделить ключевые аспекты для анализа безопасности;
* построить матрицу парных сравнений для оценки важности различных аспектов безопасности;
* провести анализ возможных угроз и классифицировать их;
* разработать рекомендации и меры по улучшению информационной безопасности компании.

# **ОБЩАЯ ИНФОРМАЦИЯ О КОМПАНИИ**

Компания "Авиабилетикс" – это современная компания, специализирующаяся на продаже и бронировании авиабилетов. Основная цель компании – предоставление клиентам удобного и быстрого доступа к бронированию авиабилетов через собственный веб-сайт и мобильные приложения. "Авиабилетикс" стремится к обеспечению высококачественного сервиса и безопасности данных клиентов.

Штат компании включает 120 сотрудников, из которых 40 человек составляют административный персонал, 30 – технические специалисты и 50 - менеджеры по работе с клиентами.

Компания также имеет филиалы в нескольких крупных городах, что позволяет эффективно обслуживать клиентов по всей стране. Головной офис находится в городе Москва.

## **Описание инфраструктуры организации**

Инфраструктура компании "Авиабилетикс" состоит из высокопроизводительного центра обработки данных (ЦОД), в котором развернуто 5 серверов с хранилищами общей емкостью 100 ТБ, на серверах установлена ОС Astra Linux. Для работы сотрудников используется 150 компьютеров с установленной Astra Linux Desktop.

Для управления учетными записями сотрудников используется FreeIPA для протокола LDAP.

Для обеспечения стабильного и безопасного подключения используется проводная-локальная сеть в каждом филиале. Помимо этого, реализованы две беспроводные сети:

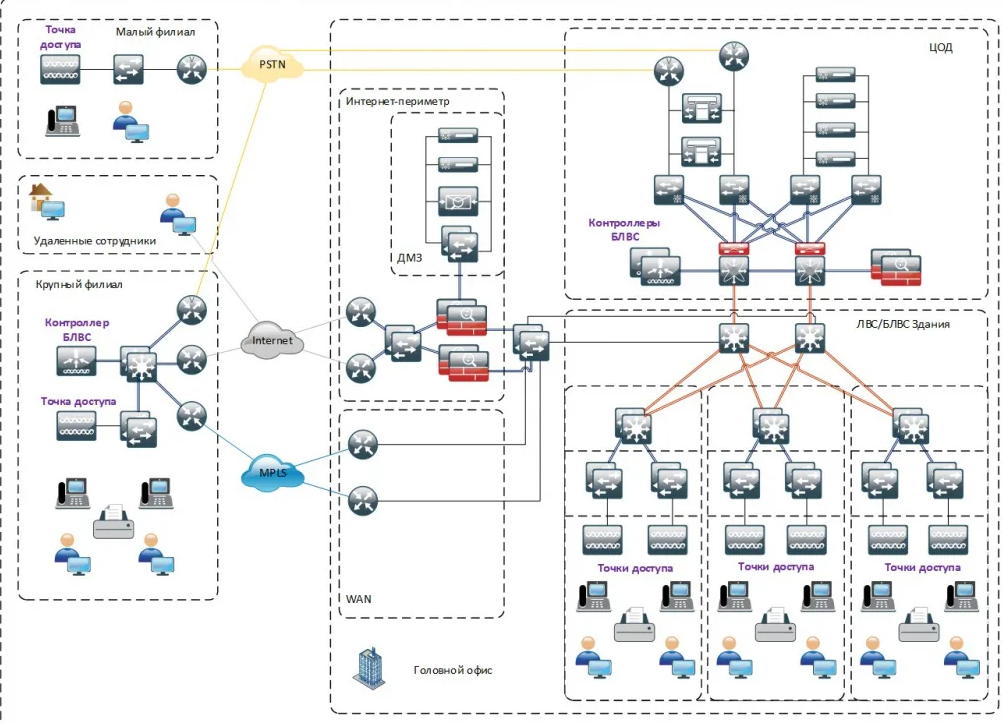
* административная беспроводная сеть: с ограниченным доступом для сотрудников, обеспечивающая безопасность данных и сетевых ресурсов;
* общедоступная беспроводная сеть: предоставляется клиентам и сотрудникам для доступа к интернету и корпоративным ресурсам.

Сотрудники подключаются по RDP соединению, предварительно используя КриптоПро NGate для подключения к VPN-шлюзу компании. Это обеспечивает высокий уровень безопасности и защищает данные от несанкционированного доступа.

Особое внимание компания уделяет безопасности данных. Так как компания работает с паспортными данными клиентов, базы данных с такой информацией выделены в отдельную область сети с повышенным уровнем защиты.

## **Веб-сайты и приложения**

Для удобства пользователей компания "Авиабилетикс" разработала веб-версию сайта и мобильные приложения для платформ Android и iOS. Веб-серверы, обслуживающие эти приложения, находятся в демилитаризованной зоне (DMZ), что обеспечивает дополнительную безопасность и изоляцию от внутренней сети компании.

Рисунок 1 – сетевая архитектура предприятия

## **Требования к экспертам**

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

* оконченное высшее образование в области ИТ или ИБ;
* опыт работы в сфере информационной безопасности не менее 2 лет с акцентом на безопасность веб-приложений и мобильных приложений;
* профессиональные сертификаты, такие как CISSP, CEH, или CISA;
* знание стандартов безопасности в авиационной индустрии, таких как PCI DSS для обработки платежей;
* глубокие знания и опыт работы с системами шифрования и защиты данных, включая асимметричное и симметричное шифрование, токенизация данных.
* навыки работы с инструментами для анализа защищенности веб-приложений и сетевых инфраструктур (например, OWASP ZAP, Kali Linux, Burpsuit, Postman).
* опыт проведения тестов на проникновение (Penetration Testing) и оценок уязвимостей в облачных средах.

## **Анализируемые аспекты**

В рамках данной работы были выделены следующие аспекты ИБ в компании «Авиабилетикс» для анализа:

* защита персональных данных клиентов: оценка методов защиты паспортных данных и других личных данных, хранящихся в базах данных. Проверка соответствия требованиям GDPR и других нормативных актов по защите данных;
* защищенность инфраструктуры: анализ программных и аппаратных продуктов, используемых при разработке/сопровождении ПО, управление доступом и аутентификация, проверка политик паролей, реализация многофакторной аутентификации (MFA) и управление ролями и правами доступа сотрудников через протокол LDAP;
* безопасность веб-приложений и мобильных приложений: Проведение тестов на проникновение для выявления уязвимостей в программных продуктах компании. Анализ на соответствие рекомендациям OWASP Top 10;
* мониторинг и управление инцидентами: оценка системы мониторинга сетевых угроз и планов реагирования на инциденты безопасности. Анализ процедур восстановления после инцидентов и их тестирования, проверка наличия систем резервного копирования и возможности отката к предыдущим версиям продуктового решения;
* соответствие нормативным требованиям и стандартам ДИБ: проверка соответствия внутренним политикам безопасности и требованиям международных стандартов (например, ISO/IEC 27001). Также сюда входит проверка физических, программных, аппаратных устройств и средств на наличие программных закладок, актуальных версий ПО, а также соответствие стандартам и нормативным документам ДИБ.

# **РАСЧЕТ И ПРОВЕРКА МАТРИЦЫ СРАВНЕНИЙ**

## **Матрица парных сравнений**

| Аспекты/Сравнение |  | Защита ПД клиентов | Защита инфраструктуры | Безопасность программных продуктов | Реагирование на инциденты | Соответствие требованиям ДИБ |
| --- | --- | --- | --- | --- | --- | --- |
| Защита ПД клиентов |  | 1 | 6 | 8 | 7 | 9 |
| Защита инфраструктуры |  | 1/6 | 1 | 4 | 3 | 5 |
| Безопасность программных продуктов |  | 1/8 | 1/4 | 1 | 1/3 | 4 |
| Реагирование на инциденты |  | 1/7 | 1/3 | 3 | 1 | 6 |
| Соответствие требованиям ДИБ |  | 1/9 | 1/5 | 1/4 | 1/6 | 1 |

Таблица 1 – матрица парных сравнений аспектов ИБ

Для оценки и ранжирования аспектов анализа компании будет использоваться матрица парных сравнений. Было выделено 5 аспектов: защита ПД клиентов, защита инфраструктуры, безопасность программных продуктов, реагирование на инциденты, соответствия требованиям ДИБ.

## **Нормированная матрица**

| Аспекты/Сравнение |  | Защита ПД клиентов | Защита инфраструктуры | Безопасность программных продуктов | Реагирование на инциденты | Соответствие требованиям ДИБ |
| --- | --- | --- | --- | --- | --- | --- |
| Защита ПД клиентов |  | 0.651 | 0.761 | 0.492 | 0.609 | 0.360 |
| Защита инфраструктуры |  | 0.109 | 0.127 | 0.246 | 0.261 | 0.20 |
| Безопасность программных продуктов |  | 0.082 | 0.032 | 0.062 | 0.029 | 0.160 |
| Реагирование на инциденты |  | 0.093 | 0.042 | 0.185 | 0.087 | 0.240 |
| Соответствие требованиям ДИБ |  | 0.072 | 0.025 | 0.015 | 0.014 | 0.040 |

Таблица 2 – матрица парных сравнений аспектов после нормирования значения

Для дальнейших вычислений следует нормировать матрицу (привести её значения в диапазон 0 – 1), для этого значение в ячейке делится на сумму всех элементов в этой колонке.

## **Собственные значения и приоритетный вектор**

|  |  |  |  |
| --- | --- | --- | --- |
| Аспект | Собственное значение | Приоритетный вектор | Результат деления (Собственное значение / Приоритет) |
| Защита ПД клиентов | 2.873 | 0.575 | 5.001 |
| Защита инфраструктуры | 1.146 | 0.189 | 6.065 |
| Безопасность программных продуктов | 0.416 | 0.073 | 5.699 |
| Реагирование на инциденты | 0,775 | 0.129 | 5.768 |
| Соответствие требованиям ДИБ | 0.271 | 0.033 | 6.007 |

Таблица 3 – таблица собственных значений аспектов и приоритетного вектора

В таблице 3 рассчитаны собственные значения аспектов и приоритетный вектор.

Приоритетный вектор – показывает относительную важную каждой категории. Вычисляется как среднее значение нормализованных строк.

Собственное значение – считается как произведение приоритетного вектора на исходную матрицу. Этот параметр отражает насколько хорошо согласованы аспекты внутри матрицы согласования.

Результат деления – среднее значение в этом столбце должны быть близки к размерности матрицы, если это так, то матрица хорошо согласована и сравнения верны.

**Собственное значение матрицы**

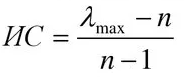
Благодаря вычислениям из таблицы 3, можно вычислить собственное значение матрицы.

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

*λmax = (5.001 + 6.065 + 5.699 + 5.768 + 6.007) / 5 = 5.411*

**Индекс согласованности (ИС)**

Далее вычислим ИС, этот параметр показывает степень согласованности матрицы парных сравнений.



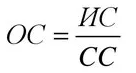
где ИС — индекс согласованности,

λmax — собственное значение матрицы,

n — количество критериев.

*ИС = (5.411 - 5) / (5 - 1) = 0.411 / 4 = 0.102*

## **Отношение согласованности (ОС)**



где ОС — отношение согласованности,

ИС — индекс согласованности,

СС — математическое ожидание индекса согласования (для 5x5 = 1.12)

*ОС = 0.102 / 1.12 = 0.091*

Так как значение CR составляет 0.091 что меньше 0.1, можно сделать

вывод, что матрица парных сравнений согласована.

# **АУДИТ КОМПАНИИ «АВИАБИЛЕТИКС»**

## **Последствия реализации атаки на предприятие**

Если на ИБ составляющую компании будет успешно реализована атака, то возможны следующие последствия:

* нарушение отказоустойчивости продуктов: вредоносные действия со стороны третьих лиц посредством DDoS-атак, SQL-инъекций, атак типа «Человек по середине» способны нарушить работоспособность и доступность решений организации;
* репутационные и финансовые риски: в следствии реализации атаки, имеется большая вероятность потери репутации, клиентской базы, акционеров и инвесторов, так же могут возникнуть судебные иски и процессы, как следствие – крупные финансовые затраты;
* потеря и утечка пользовательских данных: атаки способны привести к полной потери, или же утечки ПД и другой информации о пользователях (предпочтения в виде cookie-files, токенов авторизации, id). Важным моментом работы аудита будет акцент на наличии функционала резервного копирования и возможности отката к предыдущим версиям продукта;
* компрометированные учетных записей сотрудников: в результате применения методов социальной инженерии (фишинга, спуфинга, смишинга, вишинга, редтекстинга, байтинга) может произойти получение несанкционированного доступа к ТУЗ и УЗ сотрудников, как результат возможны: доступ к конфиденциальной информации, изменение критических настроек инфраструктуры, проведение несогласованных операций в ИС.

## **Описание модели угроз**

Классификации угроз безопасности информации для компании. В рамках работы были выделены основные классы угроз, которыми могут быть подвержены аспекты ИБ компании «Авиабилетикс».

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, резервные копии данных;
* доступность сервисов: веб-сайт компании, CRM-система, системы управления базами данных, почтовый сервис, мобильные приложения для клиентов.

По видам возможных источников угроз безопасности:

* внутренний нарушитель: cсотрудники компании, бывшие сотрудники с сохранившимся доступом, подрядчики и консультанты;
* внешний нарушитель: xакеры, киберпреступники, конкуренты, использующие интернет для атак, организованные кибергруппы;
* стихийные бедствия и техногенные катастрофы: пожары, наводнения, отключения электроэнергии, аппаратные сбои, террористические акты.

По способу реализации угроз безопасности:

* несанкционированный доступ: попытки обхода механизмов аутентификации и авторизации, использование украденных учетных данных;
* вредоносное программное обеспечение: вирусы, трояны, черви, программы-вымогатели, рекламное ПО, программные закладки;
* социальная инженерия: фишинг, убеждение сотрудников выдать конфиденциальную информацию, поддельные техподдержки;
* уязвимости программного обеспечения: использование уязвимостей в приложениях, операционных системах и сетевых устройствах;
* физический доступ: кража оборудования, доступ к защищенным зонам без разрешения.

По виду защищаемой от угроз безопасности информации:

* операционные данные: логи доступа, отчеты об ошибках, данные о производительности системы;
* общие данные: расчетные счета и реквизиты компании, квитанции о доходах/расходах;
* критические данные: ТЗ релизов, данные от ТУЗ/УЗ, архитектурные схемы сети, протоколы заседаний и совещаний, API токены, ПД клиентов.

По видам возможных источников угроз безопасности:

* инсайдерская угроза: текущие и бывшие сотрудники, имеющие глубокие знания о внутренней инфраструктуре компании;
* поставщики и партнеры: внешние организации, имеющие доступ к информационным системам компании.

По способу реализации угроз безопасности:

* злоупотребление привилегиями: несанкционированное использование административных прав для доступа к конфиденциальной информации;
* эксплуатация социальных сетей: использование публично доступной информации для проведения таргетированных атак.

## **Возможные источники реализации угроз**

| № | Виды нарушителей | Категории | Возможные цели |
| --- | --- | --- | --- |
| 1 | Работники иностранных спецслужб | Внешний | Нарушение работы транспортного обращения страны, подрыв авторитета РФ на мировой арене |
| 2 | Киберпреступники (ОПГ хакеров) | Внешний | Получение финансовой выгоды (вымогательство, кража данных для продажи, публикация данных в общий доступ) |
| 3 | Текущие(бывшие) сотрудники | Внутренний | Месть, получение выгоды от продажи данных, нанесение ущерба репутации компании |
| 4 | Рядовые сотрудники | Внутренний | Непреднамеренные действия, случайная потеря данных, заражение вредоносным ПО |
| 6 | Террористические группировки | Внешний | Совершение террористических актов, экстремистских действий в филиалах(офисах) компании |

Таблица 4 - таблица категорий нарушителей и их целей

В таблице выше показаны 4 основные категории нарушителей, определена их категория относительно сущности самой компании и определены возможные цели и умысел действий соответствующих видов.

## **Уровни возможностей нарушителей**

| № | Уровень возможностей нарушителей | Возможности нарушителей по реализации угроз безопасности информации | Виды нарушителей |
| --- | --- | --- | --- |
| 1 | Нарушитель, обладающий стандартными возможностями | Использует базовые и классические уязвимости, простые скрипты и общедоступные инструменты | Рядовые пользователи (сотрудники компании) |
| 2 | Нарушитель, обладающий привилегированными и возможностями | Знаком с архитектурой сети, инфраструктурой компании и ИС. Использует более сложные инструменты, может модифицировать скрипты, возможно имеет подельников в лице текущих сотрудников) | Недовольные сотрудники, опытные бывшие сотрудники |
| 3 | Нарушитель, обладающий повышенными возможностями | Может разрабатывать собственные эксплойты, использует уязвимости нулевого дня | Киберпреступники, кибер-организации |
| 4 | Нарушитель, обладающий наивысшими возможностями | Имеет доступ к ресурсам государства, высококвалифицированные специалисты, скоординированные атаки | Конкуренты (с привлечением специалистов), государственные структуры, иностранные агентства и службы |

Таблица 5 – уровни возможностей нарушителей

В таблице 5 представлены 4 уровня нарушителей ИБ компании «Авиабилетикс», описаны их технические возможности, и степень мастерства, для каждого уровня представлен пример вида нарушителя.

## **Меры защиты компании для предотвращения и профилактики атак**

| № | Уровень возможностей нарушителей | Меры защиты |
| --- | --- | --- |
| H1 | Нарушитель, обладающий стандартными возможностями | Курсы ИБ для сотрудников, ограничение возможностей пользователей и сотрудников ИС по ролевой модели, своевременное обновление ПО согласно инструкциям ДИБ |
| H2 | Нарушитель, обладающий привилегированными возможностями | Внедрение систем обнаружения и предотвращения вторжений (IDS/IPS), усиление контроля доступа, регулярные аудиты безопасности и проверка МСЭ. Периодическая проверка актуальных ТУЗ/УЗ и их прав доступа, реализация систем резервного копирования |
| H3 | Нарушитель, обладающий повышенными возможностями | Проведение анализа защищенности (pentest), использование средств защиты веб-приложений (WAF), сегментация сети. Выделение ключевых серверов в DMZ. Настройка firewall, реализация систем резервного копирования, ведение профилактических и аварийных работ на серверах |
| H4 | Нарушитель, обладающий наивысшими возможностями | Использование российского-лицензированного ПО и услугами импортозамещения. Комплексный подход к безопасности, покупка решений от ведущих поставщиков в государстве, настройка мониторинга и нотификации об инцидентах |

Талица 6 - Меры защиты компании для предотвращения и профилактики атак и угроз

В таблице выше показан результат аудита компании, даны практические рекомендации по мерам защиты и профилактики ИБ в целевой организации.

# **ЗАКЛЮЧЕНИЕ**

В ходе данной работы был проведен комплексный аудит информационной безопасности компании "Авиабилетикс". Были выполнены следующие этапы:

* выделение ключевых аспектов для анализа безопасности: Оценены защита персональных данных клиентов, безопасность веб-приложений и мобильных приложений, защищенность инфраструктуры, мониторинг и управление инцидентами, соответствие нормативным требованиям и стандартам ДИБ;
* построение матрицы парных сравнений: Проведен анализ важности различных аспектов безопасности с использованием матрицы парных сравнений, что позволило определить приоритеты в защите информационных систем;
* анализ возможных угроз и классификация: Выявлены ключевые угрозы, такие как утечка данных, кибератаки, потеря данных, нарушение доступности сервисов и компрометация учетных записей сотрудников. Проведена классификация угроз по видам нарушителей и способам реализации;
* разработка мер по улучшению информационной безопасности: предложены меры по защите от различных угроз и практические рекомендации по защите и профилактике ИБ в компании.

Все рекомендации и меры были разработаны с учетом требований и рекомендаций ФСТЭК. Это позволит компании "Авиабилетикс" обеспечить высокий уровень безопасности данных клиентов и устойчивость своих сервисов к различным видам угроз, что, в свою очередь, способствует укреплению доверия клиентов и партнеров, а также повышению репутации на рынке.