

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
 «ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Программное обеспечение вычислительной техники и автоматизированных систем»

|  |  |
| --- | --- |
| Заведующий кафедрой | «ПОВТ и АС» |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  (подпись) | В.В. Долгов |

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г.

**Практическая работа №1**

по лабораторно-практической работе по дисциплине “Методы кодирования и защиты информации” по кафедре «Программное обеспечение вычислительной техники и автоматизированных системы»

Обучающийся \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_Э. Ю. Волкова\_\_\_

подпись, дата

Обозначение отчета ПР.35.0000.000 Группа \_\_\_\_ВМО41\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Направление 02.03.03 Математическое обеспечение и администрирование информационных систем

Профиль Математическое обеспечение и администрирование информационных систем

Преподаватель: ст.пр. Ляхницкая Ольга Владимировна

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Дата подпись преподавателя

Ростов-на-Дону

2024

**С****одержание**

[Введение 3](#_Toc184255678)

[1.Описание компании «DataGuard». 4](#_Toc184255679)

[1.1 История и эволюция компании 4](#_Toc184255680)

[1.2 Сфера деятельности и производимая продукция 4](#_Toc184255681)

[1.3 Репутация и положение на рынке 4](#_Toc184255682)

[1.4 Форма организации 5](#_Toc184255683)

[1.5 Перечень сотрудников и их должностных обязанностей 5](#_Toc184255684)

[2.1 Внешние угрозы (хакерские атаки, шпионаж, фишинг и т.д) 6](#_Toc184255685)

[2.2 Внутренние угрозы (несанкционированный доступ, утечка информации и т.д) 7](#_Toc184255686)

[3. Меры по обеспечению безопасности 9](#_Toc184255687)

[3.1 Программно-аппаратные средства защиты. 9](#_Toc184255688)

[3.2 Организационно правовые меры. 9](#_Toc184255689)

[3.3 Политика безопасности компании 10](#_Toc184255690)

[Заключение 15](#_Toc184255691)

[Перечень используемых информационных источников 17](#_Toc184255692)

# ****Введение****

Кибербезопасность – это область, которая занимается защитой компьютерных систем, сетей и данных от угроз, связанных с цифровым пространством. В современном мире, где все больше информации хранится и передается через интернет, обеспечение безопасности становится критически важным. Вот почему кибербезопасность играет ключевую роль в защите нашей конфиденциальной информации, финансовых данных, интеллектуальной собственности и даже национальной безопасности.

В данной работе рассмотрен процесс разработки политики безопасности для фиктивной компании ООО «DataGuard», специализирующаяся на предоставлении услуг в области цифровых финансов. Основной целью работы является анализ угроз кибербезопасности, выявление уязвимостей, а также разработка мер по защите компании от потенциальных атак.

# ****1.Описание компании «DataGuard».****

## 1.1 История и эволюция компании

Компания «DataGuard» была основана в 2010 году в Москве и изначально занималась предоставлением финансовых услуг для малого и среднего бизнеса. Однако с развитием технологий и ростом объема цифровых транзакций, компания постепенно стала интегрировать передовые решения в области финансовых технологий (FinTech) и сосредоточилась на обеспечении безопасности данных своих клиентов. С 2018 года компания активно внедряет технологии блокчейн и облачные решения для хранения данных, что позволило ей завоевать широкое признание на рынке цифровых финансовых услуг.

## 1.2 Сфера деятельности и производимая продукция

Основное направление компании — предоставление платформ для онлайн-транзакций, облачного хранения финансовой информации и консультации по кибербезопасности для финансовых организаций. В число услуг входят:

* Обработка и защита онлайн-платежей.
* Управление цифровыми активами.
* Финансовое консультирование.
* Разработка безопасных приложений для финансовых операций.
* Облачное хранение данных с повышенным уровнем безопасности.

## 1.3 Репутация и положение на рынке

«DataGuard» завоевала репутацию надежного партнера в области цифровых финансов, благодаря высокому уровню защиты данных и прозрачности операций.

Компания является лидером на российском рынке FinTech-услуг и активно расширяется на международные рынки. «DataGuard» пользуется доверием у крупных банков и государственных учреждений, с которыми реализует совместные проекты по повышению финансовой безопасности.

## 1.4 Форма организации

«DataGuard» — это общество с ограниченной ответственностью (ООО) с централизованной структурой управления. Центральный офис находится в Москве, однако компания также имеет представительства в Санкт-Петербурге и за рубежом.

Организация разделена на несколько отделов: IT, отдел кибербезопасности, отдел по работе с клиентами и юридический отдел. Управление компанией осуществляет совет директоров, во главе которого стоит генеральный директор.

# 1.5 Перечень сотрудников и их должностных обязанностей

«DataGuard» имеет разнообразную команду специалистов:

Генеральный директор (CEO) – управляет стратегическим развитием компании.

Технический директор (CTO) – отвечает за технологическую инфраструктуру и безопасность систем.

Руководитель отдела кибербезопасности – планирует и реализует меры по обеспечению безопасности данных.

Инженеры по кибербезопасности – мониторят системы на предмет угроз и разрабатывают методы защиты.

Юристы – обеспечивают соответствие всех операций и технологий действующему законодательству.

Менеджеры по работе с клиентами – обеспечивают взаимодействие с клиентами и реализацию услуг.

**2**. Анализ угроз безопасности

## 2.1 Внешние угрозы (хакерские атаки, шпионаж, фишинг и т.д)

Внешние угрозы кибербезопасности – это действия злоумышленников, направленные на нарушение конфиденциальности, целостности или доступности информационных ресурсов компании «DataGuard»с использованием сетевых технологий. Среди наиболее распространенных видов внешних угроз можно выделить следующие:

* Хакерские атаки. Кибератаки, направленные на системы компании с целью кражи финансовых данных клиентов и саботажа операций.
* Фишинг. Мошеннические рассылки с целью получения конфиденциальной информации пользователей.
* DDoS-атаки. Перегрузка серверов компании с целью блокировки доступа к онлайн-сервисам.
* Шпионаж. Попытки получения корпоративной информации конкурентами через взлом сетей или через инсайдеров.

Для защиты от внешних угроз кибербезопасности компания «DataGuard»должна применять комплексный подход, включающий как технические, так и организационные меры. Среди них можно назвать следующие:

* Обновление и аудит ПО, установка антивирусных программ и файрволлов, шифрование данных и резервное копирование.
* Разработка и соблюдение политики безопасности, регулирующей правила доступа, использования и передачи информации, а также ответственность за нарушения.
* Обучение и повышение осведомленности сотрудников о киберугрозах и методах их предотвращения, а также контроль за их действиями в сети.
* Сотрудничество с правоохранительными органами, специализированными организациями и сообществами по кибербезопасности, обмен информацией и опытом по борьбе с киберпреступностью.

## 2.2 Внутренние угрозы (несанкционированный доступ, утечка информации и т.д)

Внутренние угрозы кибербезопасности – это действия сотрудников или контрагентов компании, которые могут нанести ущерб информационным ресурсам, системам или процессам компании, как по ошибке, так и намеренно. Среди наиболее частых видов внутренних угроз можно выделить следующие:

* Несанкционированный доступ. Потенциальные риски, связанные с действиями сотрудников, имеющих доступ к конфиденциальной информации.
* Утечка данных. Риски, связанные с несанкционированной передачей клиентской информации.
* Ошибка сотрудников. Ненамеренные действия сотрудников, приводящие к нарушениям работы систем безопасности.

Для защиты от внутренних угроз кибербезопасности компания «DataGuard» применяет следующие меры:

* Разграничение и контроль доступа к информации, системам и устройствам на основе ролей, полномочий и обязанностей сотрудников и контрагентов.
* Мониторинг и аудит действий пользователей в сети, регистрация и анализ всех попыток доступа, нарушений и инцидентов безопасности.
* Обучение и повышение осведомленности сотрудников и контрагентов о правилах обращения с конфиденциальной информацией, системами и устройствами, а также о последствиях их нарушения.
* Применение дисциплинарных и юридических мер в отношении нарушителей безопасности, в том числе увольнения, штрафов, исков и т.д.

# ****3. Меры по обеспечению безопасности****

## 3.1 Программно-аппаратные средства защиты.

Программно-аппаратные средства защиты – это важная часть стратегии кибербезопасности компании «DataGuard». Они позволяют защитить информацию, которая является ценным ресурсом для компании, ее клиентов и партнеров. Компания «DataGuard» использует различные виды программно-аппаратных средств защиты, в зависимости от специфики своих продуктов и услуг, а также от потребностей своих клиентов. Некоторые из них:

* Системы шифрования для защиты данных при передаче и хранении.
* Многофакторная аутентификация (MFA) для сотрудников и клиентов.
* Антивирусное ПО и системы предотвращения вторжений (IPS) для защиты от внешних угроз.
* VPN для безопасного удаленного доступа сотрудников.

## 3.2 Организационно правовые меры.

Организационно-правовые меры – это меры, которые направлены на создание и соблюдение правовых норм и стандартов в области кибербезопасности, а также на формирование организационной структуры и процедур для обеспечения безопасности информации. Они включают в себя:

* Регулярные аудиты безопасности и сертификация по стандартам ISO/IEC 27001.
* Внедрение правил доступа на основе ролей (RBAC) для разграничения прав сотрудников.
* Проведение регулярных тренингов по кибербезопасности для сотрудников.

## 3.3 Политика безопасности компании

Политика безопасности компании представляет собой документ, в котором фиксируются основные цели, принципы, правила и меры для обеспечения защиты информации внутри организации. Этот документ отражает подход компании к вопросам кибербезопасности, определяет роли и обязанности всех участников, включая сотрудников и партнеров. Политика должна соответствовать законодательным нормам, отраслевым стандартам и лучшим практикам в области информационной безопасности, а также учитывать особенности и потребности компании.

Политика безопасности компании «DataGuard» включает в себя следующие разделы:

***Предмет политики***

В компании «DataGuard» объектами защиты являются данные, включающие в себя различные виды информации: факты, концепции, алгоритмы, программы, документы, относящиеся к деятельности компании, её продуктам, услугам, клиентам, партнёрам и сотрудникам. Эти данные могут храниться в разных форматах, таких как бумажные документы, электронные файлы, аудиоматериалы, видео и графические данные.

Существуют следующие виды информации в «DataGuard»:

* Общедоступная информация — открытые данные, не содержащие коммерческой тайны или персональных сведений, доступные для свободного распространения (например, материалы сайта, пресс-релизы, клиентские отзывы).
* Внутренняя информация — данные, предназначенные для использования исключительно внутри компании, не подлежащие разглашению без специального разрешения (например, планы, стратегии, технические документы).
* Конфиденциальная информация — критически важные данные, утечка которых может нанести существенный вред компании или её сотрудникам (например, коммерческая тайна, персональные данные, финансовые отчеты).

***Классификация информации***

В компании «DataGuard» информация классифицируется по степени конфиденциальности и важности в соответствии с следующей шкалой:

* Не секретно (NS) — информация, которая может быть свободно распространена.
* Для служебного пользования (ДСП) — внутренняя информация, доступная только для сотрудников компании.
* Секретно (С) — данные, требующие высокого уровня защиты и доступа лишь по необходимости.
* Совершенно секретно (СС) — особо важные данные, которые нуждаются в максимальной защите и передаются строго по установленным правилам.

***Угрозы и риски***

В компании «DataGuard» существуют следующие угрозы и риски для информации:

* Внешние угрозы — атаки и события извне, такие как хакерские атаки, фишинг, шпионаж, вредоносные программы и физическое проникновение.
* Внутренние угрозы — ошибки сотрудников или умышленные действия, включая несанкционированный доступ, утечку информации, коррупцию и мошенничество.

***Описание позиции компании***

Компания «DataGuard» осознаёт важность информации как ключевого актива и считает её безопасность приоритетной задачей. Защита данных от угроз, обеспечение их целостности, конфиденциальности и доступности — это основа стратегии компании.

Основные принципы компании в области кибербезопасности:

* Комплексный подход — безопасность информации требует учёта множества факторов и внедрения защитных мер на разных уровнях.
* Проактивность — компания стремится предотвратить угрозы заранее, а не только реагировать на них.
* Соответствие стандартам — соблюдение всех законодательных и стандартных требований.
* Ориентация на риски — регулярная оценка рисков и принятие мер для их минимизации.
* Непрерывность работы — поддержание рабочих процессов даже в случае нарушений безопасности.
* Обучение персонала — постоянное повышение квалификации сотрудников в области кибербезопасности.
* Сотрудничество — взаимодействие с государственными и частными организациями для обмена опытом и лучшими практиками.

***Ценности компании***

В области кибербезопасности компания «DataGuard» имеет следующие ценности:

* Доверие — формирование устойчивых и доверительных отношений с клиентами и партнёрами.
* Инновации — постоянное внедрение новых технологий для улучшения безопасности.
* Качество — предоставление продуктов и услуг на высоком уровне с акцентом на надёжность защиты данных.
* Этика — соблюдение этических норм в области защиты данных и прав участников информационных отношений.

***Обязательства компании***

Компания «DataGuard» обязуется:

* Следовать законодательству и стандартам в области кибербезопасности.
* Обеспечивать безопасность продуктов и услуг для клиентов.
* Постоянно улучшать систему защиты.
* Проводить обучение и повышать осведомленность сотрудников.
* Взаимодействовать с экспертами и государственными структурами по вопросам безопасности.
* Оперативно реагировать на инциденты и восстанавливать нарушенные процессы.

***Применимость политики***

Данная политика распространяется на все виды информации в компании, а также на всех сотрудников, партнеров и клиентов. Политика применяется ко всем системам, ресурсам и процессам, связанным с обработкой данных, вне зависимости от формата или носителя информации.

Политика безопасности компании «DataGuard» не распространяется на личную информацию сотрудников, если она не связана с их профессиональной деятельностью, а также на данные, не относящиеся к работе компании.

***Роли и обязанности***

В компании «DataGuard» определены следующие роли и обязанности по обеспечению безопасности информации:

* Топ-менеджмент отвечает за разработку, внедрение и контроль исполнения политики безопасности.
* Специалисты по кибербезопасности занимаются проектированием и поддержанием системы защиты.
* Административный персонал координирует процессы, ведёт документацию и проводит аудит.
* Пользователи информации обязаны соблюдать правила безопасности, обеспечивая защиту данных.

Все сотрудники и пользователи информации должны следовать данной политике, использовать информацию исключительно в рамках своих полномочий и обеспечивать её защиту от несанкционированного доступа или утечки.

# Заключение

В данном документе был рассмотрен процесс разработки политики безопасности для вымышленной компании «DataGuard», специализирующейся на цифровых финансовых услугах и защите данных. Мы подробно описали историю развития компании, её сферу деятельности, рыночное положение, репутацию, а также организационную структуру. Кроме того, был проведен анализ угроз, с которыми сталкивается компания, и предложены соответствующие меры для защиты от этих угроз. Были изучены как программно-аппаратные средства защиты, так и организационно-правовые меры, а также политика безопасности компании.

На основе проведенного анализа можно сделать следующие выводы и рекомендации:

* Компания «DataGuard» является одним из лидеров на рынке финансовых технологий, предоставляя инновационные и надежные решения для защиты данных своих клиентов от киберугроз.
* У компании централизованная структура, что позволяет поддерживать единое видение и стратегию в вопросах кибербезопасности.
* «DataGuard» сталкивается с различными угрозами, включая хакерские атаки, шпионаж, вирусы, фишинг и другие внешние и внутренние угрозы. Для их предотвращения компания использует современные программно-аппаратные решения, такие как антивирусное ПО, фаерволы, VPN и шифрование данных.
* Помимо технических средств, компания применяет организационно-правовые меры, такие как строгие правила контроля доступа, регулярное обучение сотрудников и заключение соглашений с партнёрами для обеспечения безопасности.
* Политика безопасности компании «DataGuard» чётко определяет её цели, принципы и ответственность в области кибербезопасности. Политика регулярно пересматривается и обновляется в соответствии с текущими угрозами и изменениями в законодательстве, чтобы поддерживать высокий уровень защиты информации.

# Перечень используемых информационных источников

1. Безопасность информационных систем: учебник / под ред. В. И. Борисова. – М.: Издательский дом «Вильямс», 2002. – 512 с.
2. Макаров, А. А. Основы кибербезопасности: учебное пособие / А. А. Макаров, В. В. Петров. – СПб.: БХВ-Петербург, 2019. – 224 с.
3. Смирнов, В. А. Кибербезопасность: теория и практика / В. А. Смирнов, А. В. Смирнова // Вестник Санкт-Петербургского университета. Серия 10. Прикладная математика. Информатика. Процессы управления. – 2018. – № 4. – С. 3-15.
4. ГОСТ Р ИСО/МЭК 27001-2022. Информационные технологии. Безопасность. Системы менеджмента информационной безопасности. Требования. – М.: Стандартинформ, 2022. – 35 с.
5. Петров, В. В. Кибербезопасность в России: вызовы и решения / В. В. Петров // Информационная безопасность. – 2020. – № 2. – С. 42-49.
6. Касперский, Е. А. Киберугрозы и безопасность: мировой опыт / Е. А. Касперский. – М.: Альпина Паблишер, 2021. – 310 с.
7. Беляев, А. В. Основы информационной безопасности: учебник / А. В. Беляев. – М.: Юрайт, 2020. – 416 с.