

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Воронежский государственный технический университет»  
(ФГБОУ ВО «ВГТУ» ВГТУ)

ФАКУЛЬТЕТ Информационных технологий и компьютерной безопасности  
КАФЕДРА Систем информационной безопасности

## ОТЧЕТ ПО ПРОИЗВОДСТВЕННОЙ ПРАКТИКЕ

Обучающийся Скрипкин Максим Михайлович  
(Ф.И.О. обучающегося)

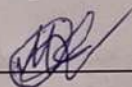
Группа КБ-201

Вид практики производственная

Тип практики Практика по получению профессиональных умений и опыта профессиональной деятельности

Наименование предприятия ООО «Техномаркет»

Обучающийся



М.М. Скрипкин

(подпись, И.О.Фамилия)

Руководитель по практической подготовке

Л.В. Парина

(подпись, И.О.Фамилия)

Оценка

отлично

## СОДЕРЖАНИЕ

ВВЕДЕНИЕ .....	3
1 Определение типа информационной системы .....	4
2 Перечень документации информационной системы .....	7
3 Формирование списка объектов и компонентов воздействия .....	11
4 Построение моделей нарушителя и угроз .....	19
5 Количественная оценка рисков .....	26
6 Составление перечня мер по противодействию выявленным угрозам .....	30
ЗАКЛЮЧЕНИЕ .....	34
СПИСОК ЛИТЕРАТУРЫ .....	35

## ВВЕДЕНИЕ

Современные условия функционирования информационных систем характеризуются высоким уровнем неопределённости и частыми изменениями. Постоянно меняется политическая ситуация, ситуация на рынках, потребность пользователей. Чтобы успевать за этим темпом, приходится применять все больше различных технологий. Каждое изменение в системе компании является риском. Возможно, только что введенная передовая технология плохо проверена и имеет ряд скрытых недочетов, которые найдутся только через несколько месяцев или несколько лет.

В современных информационных системах необходим постоянный контроль информации о применяемых технологиях и тестирование их работоспособности. Для этого компании приглашают к себе специалистов по менеджменту рисков, которые постоянно контролируют ситуацию и предлагают дополнительные защитные меры. Риск в действиях каждой компании существует постоянно. Он проявляется в различных негативных последствиях, таких как сокращение прибыли, снижении эффективности производства и экономической деятельности, простои, остановка производства. Разработкой планов по ликвидации причин и последствий действия злоумышленников также занимаются специалисты по риск-анализу. В итоге, риск-анализ как профилактика негативных последствий незаменим в каждой организации.

Цель работы: провести риск-анализ информационной системы компании разработчиков онлайн-игр «Allaud».

Задачи:

1. Определение типа информационной системы компании «Allaud»;
2. Составление перечня документации, в рамках которой функционирует данная информационная система;
3. Определение объектов и компонентов информационной системы;
4. Построение моделей нарушителя и угроз;
5. Проведение количественной оценки рисков;
6. Составление перечня мер по противодействию выявленным угрозам.

## 1 Определение типа информационной системы

Информационная система компании разработчиков онлайн-игр «Allaud» относится к типу ИСПДн (информационная система персональных данных). Эта система включает в себя сами персональные данные, которые передаются при регистрации и подписки пользователя онлайн игр, а также средства, которые используются для их обработки и защиты.

Большую часть автоматизированной обработки персональных данных регламентирует федеральный закон №152 «о персональных данных». Саму информационную систему регламентирует федеральный закон №149 «об информации, информационных технологиях и о защите информации» [1, 2].

По федеральному закону №152 «о персональных данных» эта информационная система хранит и обрабатывает в себе персональные данные игроков. Следовательно, в этом случае идёт обработка персональных данных, эту обработку сам оператор в соответствии с статьями, прописанными в законе. Уполномоченное лицо может обезличивать, уничтожать и блокировать персональные данные. Сам пользователь – игрок – в добровольном варианте предоставляет право оператору на использование, обработку и передачу третьим лицам свои персональные данные. Также в настоящем федеральном законе прописаны меры, направленные на выполнения оператором обязанностей, предусмотренным настоящим федеральным законом. Аналогично приводятся меры по обеспечению безопасности персональных данных при их обработке.

Данные пользователей в компании по разработке онлайн игр хранятся на сервере. Данный сервер будет регулироваться в соответствии с федеральным законом №149 «об информации, информационных технологиях и о защите информации».

В этом законе регламентируется управление потоками данных, информационными системами, а также информационными технологиями.

В нём представлены основные требования для использования информации, технологий, дающих возможность создания информационных систем, систем передачи информации и информационно- телекоммуникационных сетей.

Хранение на сервере осуществляется с помощью технологии RAID массива накопителей, все накопители – это физические устройства представленный в виде жёстких дисков или SSD дисков. Вся система хранения данных централизованная и имеет главный сервер обработки данных, который фиксирует потоки передаваемых данных и отправляет их на, разграниченные по регионам, серверы.

В компании по разработке онлайн игр обеспечение информационной безопасности персональных происходит с помощью средств защиты информации (СЗИ). В организации имеются такие меры, как:

1. Идентификация и аутентификация. Сюда входят идентификация и аутентификация пользователей, устройств, а также управление идентификацией и аутентификация в том числе метками, устройствами хранения и возможностью удаления в случае потери.
2. Управление доступом. В него входит управление учётными записями пользователей. Реализация методов, правил разграничения, также разделение полномочий пользователей и установка точного значения блокировки пользователя в случае истечения времени бездействия или неверно ведённого количества раз пароля.
3. Регистрация событий безопасности. В неё осуществляется определение событий безопасности, определение состава и содержания событий безопасности, а также сбор, запись и хранение информации о событии;
4. Антивирусная защита.
5. Контроль защищённости персональных данных. В нём рассматриваются: выявление уязвимостей системы, контроль установки обновлений программного обеспечения, контроль правильной работоспособности программного обеспечения.
6. Защита среды виртуализации. Она включает в себя: идентификацию и аутентификация субъектов доступа и объектов доступа, управление доступом, регистрация управлением событий безопасности в виртуальной инфраструктуре.

7. Управление конфигурацией информационной системы и системы защиты персональных данных. Она включает в себя: управление изменениями конфигураций в информационных системах, анализ потенциально планируемых изменений в системе, документирование информации об изменении [3].

Дальше определим уровень защищённости персональных данных в рассматриваемой информационной системе (классификация ИСПДн отменена с 11 марта 2013 года по приказу ФСТЭК/ФСБ/Минкомсвязи №151/786/461). Требованиями к защите ПДн при их обработке в информационных системах (Утв. Постановлением Правительства № 1119 от 01.11.2012) установлены 4 уровня защищенности персональных данных. Исходя из этих требований, для ИС компании «Allaud» определена третья группа обрабатываемых ПДн (общедоступные персональные данные) и второй уровень защищённости ПДн (2 УЗ) [4].

## 2 Перечень документации информационной системы

Для обеспечения информационной безопасности в нашей компании, мы будем использовать государственные стандарты, связанные с информационной безопасностью. Для начала определим круг подчинения организации:

1. Методический документ ФСТЭК – методика оценки угроз безопасности информации;
2. ГОСТ Р ИСО/МЭК ТО 13335-3—2007 – методы менеджмента безопасности информационной технологии;
3. ГОСТ Р ИСО/МЭК 27018 – 2020 – свод правил по защите персональных данных в публичных облаках, используемых для их обработки;
4. ГОСТ Р ИСО/МЭК 27034 – безопасность приложений;
5. ГОСТ Р ИСО/МЭК 12207 – процессы жизненного цикла программ.

Из документов ФСТЭК мы будем использовать вышеупомянутую методику определения угроз безопасности информации и объектов воздействия угроз. Также в этом документе дана методика определения источников угроз. Из приложений в этом документе будем использовать таблицы видов риска, объектов воздействия, целей реализации угроз. Чтобы определить уровень нарушителя, также воспользуемся таблицей из этого документа [5].

Следующий документ, которым мы воспользуемся, будет ГОСТ Р ИСО/МЭК ТО 13335-3—2007 – методы менеджмента безопасности информационной технологии. В этом документе мы ознакомимся с основными вариантами стратегий анализа риска. Существует базовый подход, который защищает все системы компании стандартными защитными мерами, неформальный подход, который основан на практическом опыте эксперта или группы экспертов. Третьей стратегией является детальный анализ риска, а четвертый это комбинация из первых трех стратегий. Из приложений этого документа можно взять таблицы методик анализа рисков, примеры общих уязвимостей, перечень типичных угроз, алгоритм определения активов компании [6].

Третий документ, который мы будем использовать в своей информационной системе ГОСТ Р ИСО/МЭК 27018 – 2020 – свод правил по защите персональных данных в публичных облаках, используемых для их обработки. Так как в информационной системе компании занимающейся разработкой и обслуживанием онлайн игр приходится сталкиваться с арендой и покупкой серверов, обработкой персональных данных и платежей пользователей, необходимо обеспечить безопасную работу этой части компании. В этом документе мы воспользуемся организацией деятельности по обеспечению информационной безопасности, безопасностью, связанную с персоналом при приеме на работу, во время работы и при увольнении. Также в этом документе описаны методики управления доступом, криптозащита наиболее важных и закрытых данных, защита коммуникаций, безопасность при приобретении техники и программного обеспечения, взаимоотношения с поставщиками [7].

В следующую группу документов мы выделим стандарты по обеспечению безопасности приложений. Эта группа стандартов разделена на 5 частей:

1. ГОСТ Р ИСО/МЭК 27034-1-2014 – обзор и общие понятия;
2. ГОСТ Р ИСО/МЭК 27034-2-2021 – нормативная структура организации;
3. ГОСТ Р ИСО/МЭК 27034-3-2021 – безопасность приложений;
4. ГОСТ Р ИСО/МЭК 27034-5-2020 – структуры данных протоколов и мер обеспечения безопасности приложений;
5. ГОСТ Р ИСО/МЭК 27034-6-2021 – практические примеры.

Из первого документа мы узнаем основные понятия по защите приложений. Во втором описано создание группы нормативной структуры организации. Эта группа специалистов занимается мониторингом безопасности используемых и разрабатываемых приложений, анализом и улучшением приложений. Из-за того, что в онлайн играх обрабатывается большое количество конфиденциальной информации, безопасность приложений должна постоянно контролироваться и улучшаться. Из третьего и четвертого документа мы используем этапы менеджмента приложений. Из пятого документа мы анализируем примеры, чтобы лучше реализовать защиту системы безопасности приложений. Также важно не допустить возможность взлома



пользователей и сотрудников. Эти задачи решает группа НСО. Процесс создания группы нормативной структуры организации, мониторинг, улучшения приложений и внедрение изменений можно представить в виде рисунка (см. Рис. 1) [8].



Рисунок 1 – Менеджмент НСО

Стандарт по обеспечению защиты приложений способствует реализации других стандартов в сфере информационной безопасности, а также ссылается на другие стандарты. Схему взаимодействия стандартов можно представить в виде рисунка (см. Рис. 2).



Рисунок 2 – Взаимосвязь ИСО/МЭК 27034 с другими стандартами

Изучить документы, как-либо связанные с безопасностью приложений, не будет лишним. Воспользуемся одним из таких – ГОСТ ИСО/МЭК 12207 – процессы жизненного цикла программ для защиты во время разработки приложений и их покупки. В стандарте описано, какие процессы должны происходить на этапе создания соглашений, организации технического и программного обеспечения, проектирования приложения, реализации и поддержки его поддержки. Приложения, предполагающие регистрацию и подписку, должны быть защищены и на этапе разработки, и на этапе поддержки. Атаки на плохо защищенное приложение могут привести к потере большого количества конфиденциальной информации пользователей [9].

Следует отметить, что это не окончательный список документации, используемой в компании. Мы выписали только базовый список документов. Перечень документов должен пополняться и изменяться в зависимости от деятельности компании, ее расширении и изменении, по мере исполнения уже выбранных стандартов и правил. Необходимо следить за обновлением стандартов, появлением новых документов. Также в качестве ознакомления можно прочитать документы по информационной безопасности, предназначенные для других организаций и структур (например, документы, регулирующие информационную безопасность в банковской сфере).

### 3 Формирование списка объектов и компонентов воздействия

В данной части работы перед нами ставится задача определения объектов и компонентов воздействия в рассматриваемой информационной системе.

Приведем определение объекта воздействия. Понятие определяет информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям. Совокупность объектов воздействия и их интерфейсов определяет границы процесса оценки угроз безопасности информации и разработки модели угроз безопасности информации.

Рассмотрим объекты и компоненты воздействия на исследуемую информационную систему. Для каждого объекта существуют основные и дополнительные компоненты. Определения объектов возьмём из справочника БДУ ФСТЭК [10].

Все объекты можно представить в виде рисунка (см. Рис. 3).

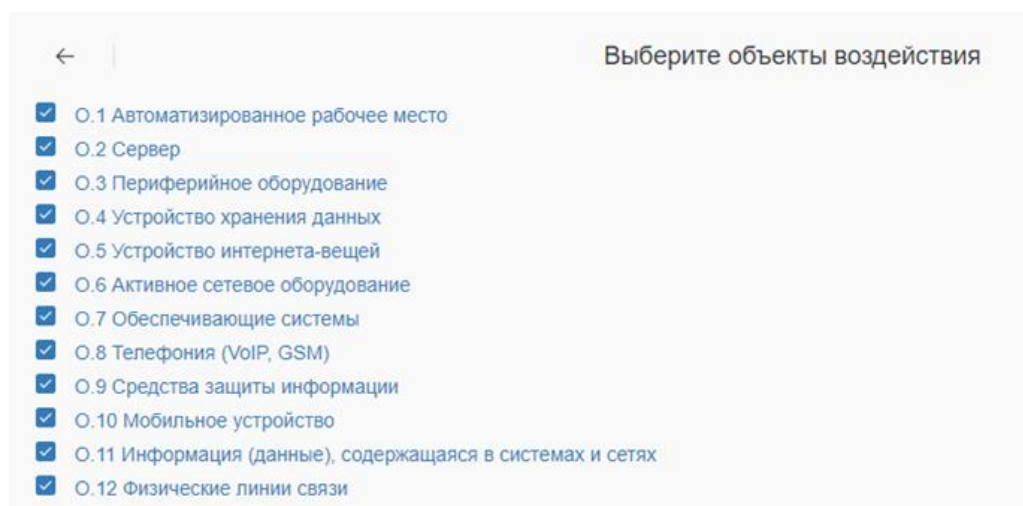


Рисунок 3 – Объекты воздействия на исследуемую ИС

1) Автоматизированное рабочее место. Оно подразумевает под собой комплекс вычислительной техники и программного обеспечения, предназначенный для автоматизации определенного вида деятельности. Ниже на рисунке приведены основные компоненты для этого объекта (см. Рис. 4).

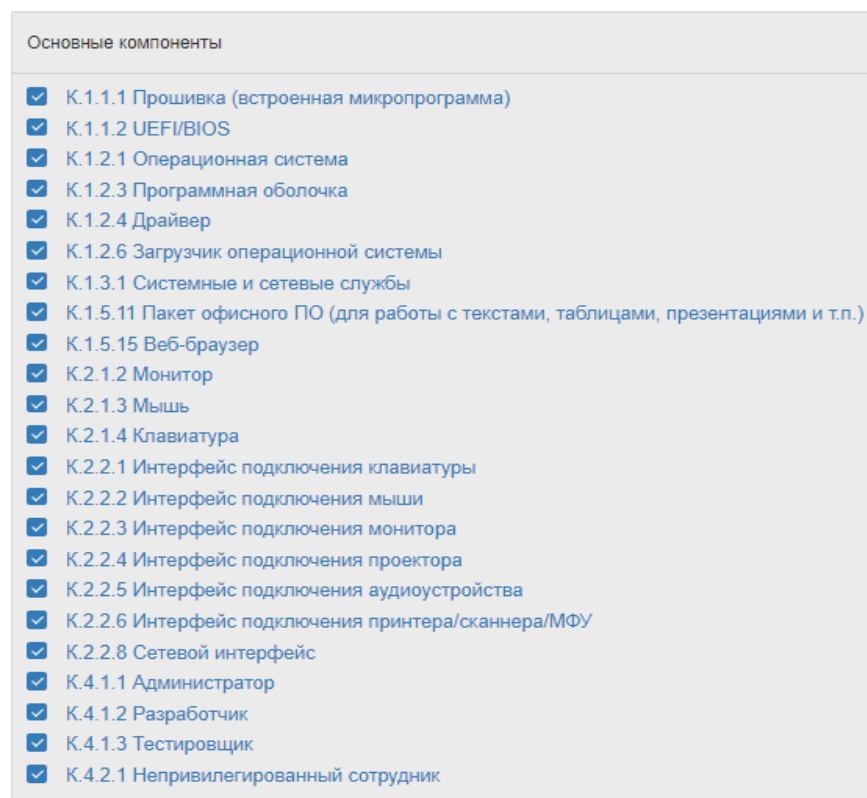


Рисунок 4 – Основные компоненты автоматизированного рабочего места

2) Сервер. Совокупность средств вычислительной техники и программных средств, предназначенная для управления, хранения, представления информации в локальной вычислительной сети для рабочих мест и других сетевых устройств (см. Рис. 5).

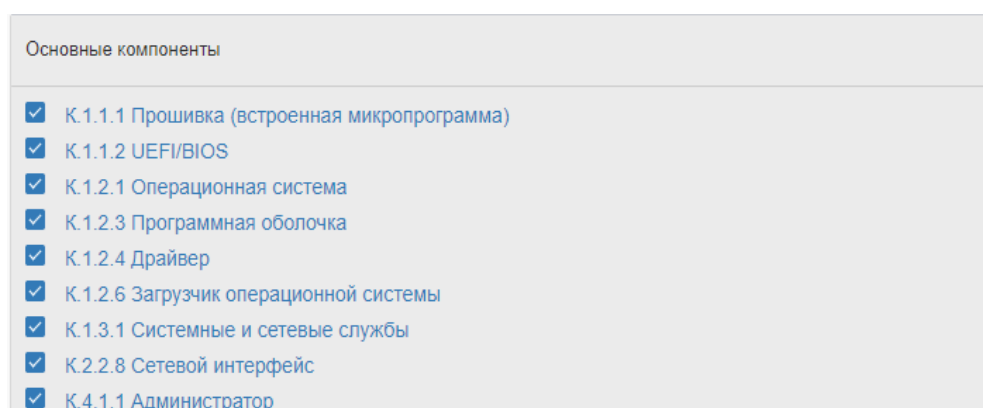


Рисунок 5 – Основные компоненты сервера

3) Периферийное оборудование. Устройства, подключаемые к автоматизированным рабочим местам, серверам или мобильным устройствам (см. Рис. 6).

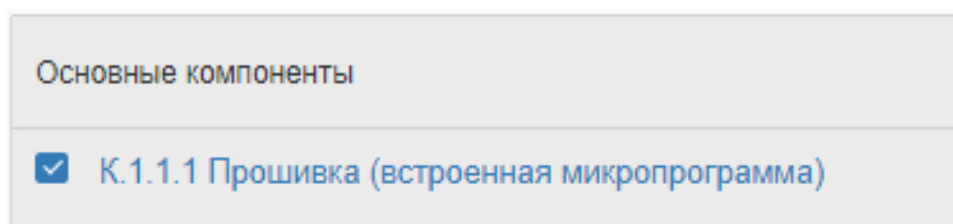


Рисунок 6 – Основные компоненты периферийного оборудования

4) Устройство хранения данных. Носитель информации, предназначенный для записи и хранения данных (см. Рис. 7).

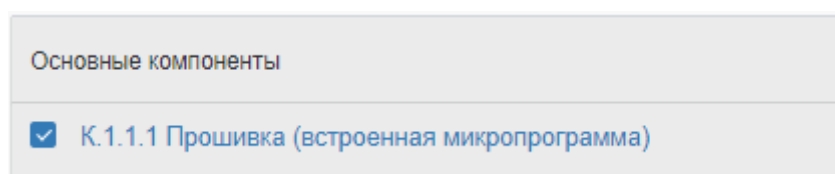


Рисунок 7 – Основные компоненты устройства хранения данных

5) Устройства интернета-вещей. Программно-техническое средство, использующее датчики и API-интерфейсы для связи и обмена данными в сети Интернет (см. Рис. 8).

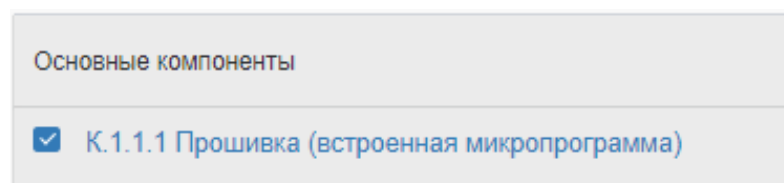


Рисунок 8 – Основные компоненты устройств интернета-вещей

6) Активное сетевое оборудование. Оборудование, содержащее электронные схемы, получающее питание от электрической сети или других источников питания и выполняющее функции преобразования, усиления и передачи сигналов, а также обрабатывающее техническую информацию, перенаправляя и распределяя потоки в соответствии с встроенными алгоритмами (см. Рис. 9).

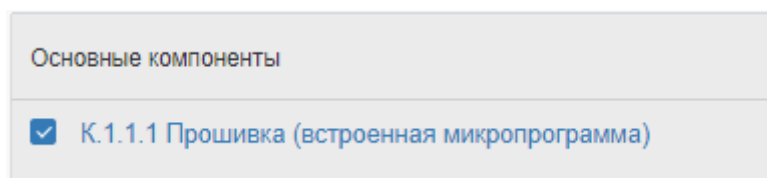


Рисунок 9 – Основные компоненты активного сетевого оборудования

7) Обеспечивающие системы. Системы, которые служат дополнением к рассматриваемой ИС на протяжении стадий ее жизненного цикла, но необязательно вносит непосредственный вклад в её функционирование (см. Рис. 10).

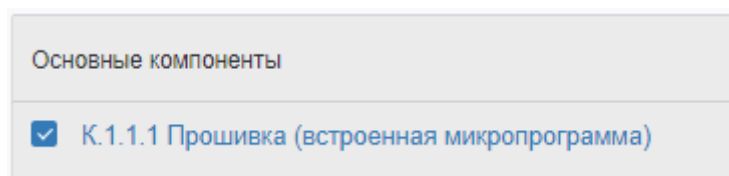


Рисунок 10 – Основные компоненты обеспечивающих систем

8) Телефония. Программно-аппаратные средства для обеспечения коммуникации посредством передачи голосовых и видеосообщений абонентам (см. Рис. 11).

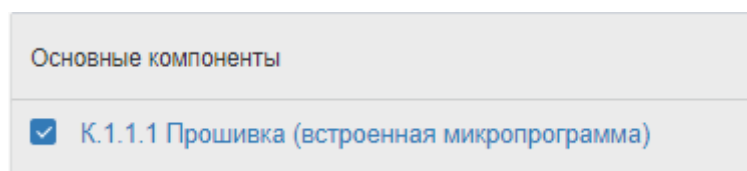


Рисунок 11 – Основные компоненты телефонии

9) Средства защиты информации. Программное или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации (см. Рис. 12).

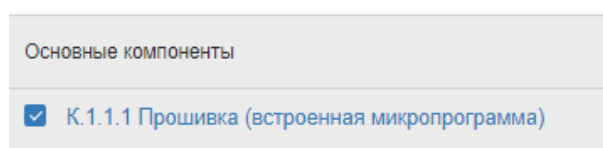


Рисунок 12 – Основные компоненты средств защиты информации

10) Мобильное устройство. Мобильный программно-технический комплекс, предназначенный для автоматизации определенного вида деятельности (см. Рис. 13).

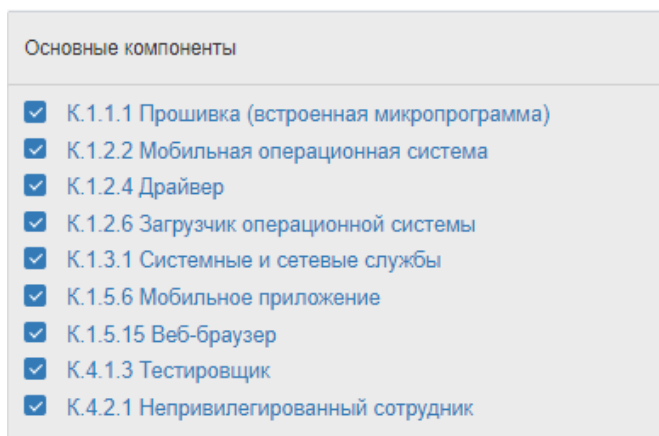


Рисунок 13 – Основные компоненты мобильного устройства

11) Информация, содержащаяся в системах и сетях. Сведения (сообщения, данные) независимо от формы их представления (см. Рис. 14).

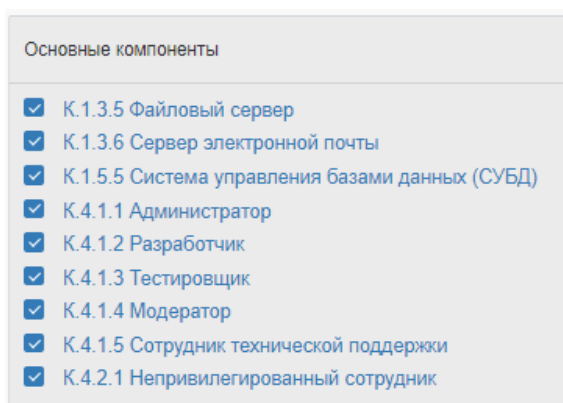


Рисунок 14 – Основные компоненты информации, содержащейся в сетях

12) Физические линии связи. Физическая среда, по которой передаются электрические информационные сигналы, аппаратура передачи данных и промежуточная аппаратура (см. Рис.15).

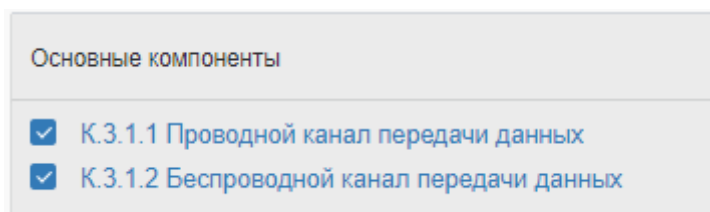


Рисунок 15 – Основные компоненты физических линий связи

Рассмотрим дополнительные компоненты информационной системы:

- К.1.2.5 Утилита (вспомогательное ПО, необходимо для выполнения широкого спектра задач);
- К.1.3.5 Файловый сервер (необходим корректного функционирования системы, позволяет множеству пользователей иметь доступ к системе хранения данных);
- К.1.3.6 Сервер электронной почты (для общения сотрудников организации посредством электронной почты, массовых рассылок и т. п.);
- К.1.4.1 ПО для разработки кода (один из важнейших компонентов для рассматриваемой организации, специализирующейся на разработке онлайн-игр);
- К.1.4.2 Средства тестирования и отладки (неотъемлемая часть процесса разработки любого ПО);
- К.1.5.1 Клиент электронной почты (для получения, написания, хранения, отправки сообщений);
- К.1.5.2 Мессенджер (необходим для удобной и быстрой коммуникации сотрудников компании);
- К.1.5.7 Скрипт автоматизации (важная часть разработки ПО, необходим для автоматизации рутинных задач);
- К.1.5.12 ПО для проектирования и моделирования (необходимо для разработки современных игр);
- К.1.6.1 Антивирусные средства (важное средство обеспечения информационной безопасности);
- К.2.4.3 Межсетевой экран (также является важным средством обеспечения ИБ, осуществляет контроль и фильтрацию сетевого трафика);
- К.1.6.4 ПО системы резервного копирования (необходимо для защиты данных от непреднамеренного повреждения и/или удаления);
- К.1.6.6 Средства анализа защищённости (для обеспечения информационной безопасности);



- К.1.6.7 Другие средства защиты информации (для обеспечения информационной безопасности);
- К.1.7.1 Веб-сайт (для организации удобного взаимодействия пользователей с информационной системой);
- К.1.7.2 Веб-клиент (для получения доступа в Интернет);
- К.1.7.3 Веб-интерфейс администрирования (необходим для управления информационной системой);
- К.2.3.1 Система хранения данных (для корректного функционирования системы);
- К.2.3.2 Съёмный машинный носитель информации (для передачи различной информации);
- К.2.4.4 Средство обнаружения (предотвращения) вторжений (важное средство обеспечения информационной безопасности);
- К.3.1.1 Проводной канал передачи данных (для корректного функционирования системы);
- К.3.1.2 Беспроводной канал передачи данных (для корректного функционирования системы);
- К.3.2.1 Протоколы аутентификации (необходимы для обеспечения информационной безопасности);
- К.3.2.2 Протоколы обмена данными (для корректного функционирования системы);
- К.4.1.5 Сотрудник технической поддержки (необходим для улучшения взаимодействия пользователей с ИС, своевременного обнаружения и устранения неполадок в ИС);
- К.4.1.2. Разработчик (занимается непосредственной разработкой коммерческих продуктов организации);
- К.4.1.3. Тестировщик (необходим для проверки качества разработанных продуктов, помогает выявить недостатки и уязвимости продукта на стадии разработки);

- К.1.5.5 Система управления базами данных (СУБД) (для корректного функционирования системы);
- К.1.6.5 Средства разграничения и управления доступом (важное средство обеспечения ИБ);
- К.1.2.2 Мобильная операционная система (необходима для пользования мобильными устройствами и разработки игр для них);
- К.1.2.4 Драйвер (необходим для функционирования всего ПО);
- К.1.3.1 Системные и сетевые службы (для реализации сетевых сервисов);
- К.1.6.2 Агент системы защиты (важное средство обеспечения ИБ);
- К.4.1.1 Администратор (необходим для поддержания функционирования ИС, выявления и исправления неполадок в её работе);
- К.1.5.11 Пакет офисного ПО (для написания и оформления отчётов, создания презентаций и т. п.).

#### 4 Построение моделей нарушителя и угроз

Защита информационной сети является ключевой задачей для реализации безопасности компании. Для этого необходимо принять решение о создании и составлении модели нарушителя и модели угроз.

Составление модели нарушителя для информационной сети необходимо для предотвращения возможности реализации проведения атак на информационную сеть. Для этого воспользуемся документом ФСТЭК «Методика моделирования угроз безопасности информации» (см. Табл. 1) [11].

Таблица 1 – Модель нарушителя

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Уровень возможностей нарушителя (потенциал)
1.	Публикация недостоверной информации на веб-ресурсах организации	Преступные группы	Базовый повышенный
2.	Использование веб-ресурсов для распространения и управления вредоносным программным обеспечением	Преступные группы	Базовый повышенный
3.	Искажение информации для получения финансовой выгоды	Преступные группы	Базовый повышенный
4.	Тестирование хакерских инструментов или апробация описанных способов осуществления атак	Физические лица	Базовый

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Уровень возможностей нарушителя (потенциал)
5.	Рассылка информационных сообщений с использованием вычислительных мощностей оператора и(или) от его имени	Преступные группы	Базовый повышенный
6.	Получение доступа к системам и сетям с целью незаконного использования вычислительных мощностей	Преступные группы	Базовый повышенный
7.	Получение доступа к системам и сетям с целью дальнейшей продажи доступа	Преступные группы	Базовый повышенный
8.	Получение преимущества за счет нарушения работоспособности систем и сетей	Конкурирующие организации	Базовый повышенный
9.	Хищение денежных средств	Преступные группы	Базовый повышенный
10.	Кража конфиденциальной информации	Преступные группы	Базовый повышенный
		Конкурирующие организации	Базовый повышенный
		Лица, привлекаемые для администрирования (управления)	Базовый повышенный

№ п/п	Возможные цели реализации угроз безопасности информации	Виды нарушителя	Уровень возможностей нарушителя (потенциал)
11.	Непреднамеренные, неосторожные или неквалифицированные действия	Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	Базовый повышенный
		Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	Базовый
		Отдельные физические лица (хакеры)	Базовый
		Пользователи (привилегированные, непривилегированные)	Базовый
		Лица, привлекаемые для ремонта, регламентного обслуживания и иных работ	Базовый повышенный
		Лица, обеспечивающие функционирование или обслуживание обеспечивающих систем, уборку, охрану	Базовый повышенный
		Пользователи (привилегированные, непривилегированные)	Базовый
		Лица, администрирования привлекаемые для (управления)	Базовый

Данная модель имеет три пункта, которые необходимы для оценки и построения модели нарушителя [11]:

1. Возможные цели реализации угроз безопасности информации: в качестве возможных целей реализации нарушителями угроз безопасности информации в информационной системе могут быть различные мотивации нарушителя для реализации атаки на информационную систему.
2. Виды нарушителя: выделяются для понимания того, кем могут быть реализованы угрозы безопасности информации в информационной системе.
3. Уровень возможностей нарушителя: демонстрирует оценку уровня возможности нарушителя по отношению к информационной системе.

Исходя из таблицы 1, максимальный потенциал возможного нарушителя – базовый повышенный. Укажем это при формировании перечня угроз на сайте БДУ (см. Рис. 16):

☒ В.1 Нарушитель, обладающий базовыми возможностями ?  
☒ В.2 Нарушитель, обладающий базовыми повышенными возможностями ?  
☐ В.3 Нарушитель, обладающий средними возможностями ?  
☐ В.4 Нарушитель, обладающий высокими возможностями ?

Рисунок 16 – Выбор уровня возможностей нарушителя

Теперь перейдем к построению модели угроз с учетом компонентов, которые могут подвергаться воздействиям (см. Табл. 2).

Таблица 2 – Модель угроз

№ УБИ	Объект	Компонент	Способ реализации	Уязвимость
УБИ.1.9.8	О.9 Средства защиты информации	К.1.6.6 Средства анализа защищенности	СП.8.5 Идентификация пользователей	Ненадежная сетевая архитектура
УБИ.2.2.22	О.2 Сервер	К.1.7.1 Веб-сайт	СП.22.3 Межсайтовый скриптинг (XSS) с запросами через сервер	Ненадежная сетевая архитектура

№ УБИ	Объект	Компонент	Способ реализации	Уязвимость
УБИ.3.3.1	О.3 Периферийное оборудование	К.1.2.4 Драйвер	СП.1.1 Эксплуатация известных уязвимостей	Недостаточная система мониторинга
УБИ.4.4.24	О.4 Устройство хранения данных	К.1.1.1 Прошивка (встроенная микропрог рамма)	СП.23.1 Подмена прошивки (микропрограммы)	Недостаточная физическая защита здания, дверей и окон
УБИ.5.10.1	О.10 Мобильное устройство	К.1.2.2 Мобильная операционн ая система	СП.1.1 Эксплуатация известных уязвимостей	Отсутствие политики по использованию мобильных устройств
УБИ.6.4.15	О.4 Устройство хранения данных	К.2.3.1 Система хранения данных	СП.15.2 Шифрование данных встроенными средствами	Неконтролируе мая загрузка и использование программных средств
УБИ.7.2.22	О.2 Сервер	К.1.7.3 Веб- интерфейс администри рования	СП.22.1 SQL- инъекция	Ненадежная сетевая архитектура
УБИ.8.3.15	О.3 Периферийно е оборудование	К.2.3.2 Съемный машинный носитель информаци и	СП.15.2 Шифрование данных встроенными средствами	Неконтролируе мая загрузка и использование программных средств
УБИ.9.11.4	О.11 Информация (данные), содержащаяся в системах и сетях	К.1.3.6 Сервер электронно й почты	СП.4.4 Внедрение вредоносного программного обеспечения через сетевое взаимодействие	Несвоевременн ое обновление базы данных антивирусов
УБИ.10.10. 13	О.10 Мобильное устройство	К.4.1.3 Тестировщи к	СП.13.1 Целенаправленная рассылка через рассылку рекламных писем (спам- сообщений)	Отсутствие осведомленнос ти о безопасности

№ УБИ	Объект	Компонент	Способ реализации	Уязвимость
УБИ.11.3.3	О.3 Периферийно е оборудование	К.2.1.6 Веб- камера	СП.3.1 Эксплуатация недостатков незащищенных протоколов передачи данных	Использование незащищенных протоколов передачи данных

Далее приведём наименования и описание угроз:

УБИ.1.9.8 – угроза утечки информации, обрабатываемой средством защиты информации, за счет сканирования сетевой инфраструктуры. Угроза заключается в возможности противоправного получения либо передачи информации.

УБИ.2.2.22 – угроза несанкционированного доступа к серверу за счет атаки на веб-приложение. Она заключается в получении доступа к информационным ресурсам, нарушающего установленные в информационной системе правила разграничения доступа.

УБИ.3.3.1 – угроза несанкционированной модификации (искажения) компонентов периферийного оборудования за счет эксплуатации уязвимостей. Заключается в изменении содержания или формы представления обрабатываемой в информационной системе информации, нарушающем установленный в информационной системе порядок обработки информации.

УБИ.4.4.24 – угроза несанкционированной подмены компонентов устройства хранения данных за счет физического воздействия. Заключается во внедрении ложного или подмене существующего компонента информационной системы и (или) обрабатываемой с его использованием информации.

УБИ.5.10.1 – угроза удаления информации, обрабатываемой мобильным устройством за счет эксплуатации уязвимостей. Заключается в несанкционированном удалении обрабатываемой в информационной системе информации.

УБИ.6.4.15 – угроза вызова отказа в обслуживании устройства хранения данных за счет шифрования данных. Заключается в недоступности информационной системы



или ее компонентов и (или) приостановлении оказания услуг или предоставления сервисов для авторизованных пользователей.

УБИ.7.2.22 – угроза ненадлежащего (нецелового) использования сервера за счет атаки на веб-приложение. Заключается в использовании вычислительных ресурсов средств вычислительной техники для осуществления сторонних, не предусмотренных технологией обработки информации, процессов.

УБИ.8.3.15 – угроза нарушения функционирования (работоспособности) периферийного оборудования за счет шифрования данных. Заключается в частичной или полной утрате работоспособности или функциональности компонента или информационной системы в целом.

УБИ.9.11.4 – угроза получения информации (данных), содержащейся в системах и сетях, из недоверенного источника за счет внедрения вредоносного программного обеспечения. Заключается в нарушении функционирования информационной системы и (или) внедрении в ее состав вредоносных программных или программно-аппаратных средств в результате получения компонентов информационной системы из недоверенных (происхождение или принадлежность которого неизвестны) или легитимных скомпрометированных источников.

УБИ.10.10.13 – угроза распространения противоправной информации через компоненты мобильного устройства за счет реализации социальной инженерии. Заключается в распространении противоправной информации с применением информационной системы или ее компонентов, а также в возможности осуществления с их использованием вредоносного воздействия на другие информационные системы.

УБИ.11.3.3 – угроза несанкционированного массового сбора информации с периферийного оборудования за счет использования недостатков архитектуры. Угроза заключается в несанкционированном сборе информации, обрабатываемой информационной системой или ее компонентами, с использованием автоматизированных средств сбора данных.

Далее проведем количественную оценку рисков, исходя из построенной модели угроз и разберем используемые меры по реализации противодействий [12].

## 5 Количественная оценка рисков

Для анализа рисков будем использовать методы оценки, представленные в ГОСТ Р ИСО/МЭК 27005-2010 [12].

Согласно примеру 3 из вышеупомянутого стандарта, для начала необходимо определить уровни угроз и уязвимостей, затем рассчитать значение степени вероятности, опираясь на таблицы из того же стандарта (см. Табл. 3).

Таблица 3 – Расчет значения степени вероятности

Угроза	Уровень угрозы	Уровень уязвимости	Значение степени вероятности
УБИ.1.9.8 «Угроза утечки информации, обрабатываемой средством защиты информации, за счет сканирования сетевой инфраструктуры»	Высокий	Средний	3
УБИ.2.2.22 «Угроза несанкционированного доступа к серверу за счет атаки на веб-приложение»	Высокий	Средний	3
УБИ.3.3.1 «Угроза несанкционированной модификации (искажения) компонентов периферийного оборудования за счет эксплуатации уязвимостей»	Низкий	Средний	1
УБИ.4.4.24 «Угроза несанкционированной подмены компонентов устройства хранения данных за счет физического воздействия»	Высокий	Средний	3
УБИ.5.10.1 «Угроза удаления информации, обрабатываемой мобильным устройством за счет эксплуатации уязвимостей»	Низкий	Низкий	0

Угроза	Уровень угрозы	Уровень уязвимости	Значение степени вероятности
УБИ.6.4.15 «Угроза вызова отказа в обслуживании устройства хранения данных за счет шифрования данных»	Высокий	Высокая	4
УБИ.7.2.22 «Угроза ненадлежащего (нецелового) использования сервера за счет атаки на веб-приложение»	Низкий	Средний	1
УБИ.8.3.15 «Угроза нарушения функционирования (работоспособности) периферийного оборудования за счет шифрования данных»	Низкий	Высокая	2
УБИ.9.11.4 «Угроза получения информации (данных), содержащейся в системах и сетях, из недоверенного источника за счет внедрения вредоносного программного обеспечения»	Высокий	Высокий	4
УБИ.10.10.13 «Угроза распространения противоправной информации через компоненты мобильного устройства за счет реализации социальной инженерии»	Низкий	Средний	1
УБИ.11.3.3 «Угроза несанкционированного массового сбора информации с периферийного оборудования за счет использования недостатков архитектуры»	Высокий	Высокий	4

Теперь определим ценность рассматриваемых объектов.

1. Объект О.2 (Сервер) имеет ценность 4, так как его бесперебойное функционирование является критически важным для работы всей ИС.

2. Объект О.3 (Периферийное оборудование) имеет ценность 2, так как является менее важным при разработке онлайн-игр, кроме того, его выход из строя влечёт за собой сравнительно небольшой ущерб.
3. Объект О.4 (Устройство хранения данных) является критически важным, так как обеспечивает хранение большого объёма информации, но в силу того, что в рассматриваемой ИС применяются технологии RAID и резервного копирования, этому объекту присваивается ценность 3.
4. Объект О.9 (Средства защиты информации) имеет ценность 4, так как является средством обеспечения ИБ в организации и в том числе обеспечивает защиту персональных данных пользователей.
5. Объект О.10 (Мобильные устройства) в основном служит для коммуникации сотрудников компании и слабо влияет на работу ИС – следовательно, имеет ценность 1.
6. Объект О.11 (Информация, содержащаяся в системах и сетях) имеет ценность 4, так как представляет собой критически важную информацию о пользователях, о компании и её разработках и т. п.

На следующем шаге подсчитаем присвоенные баллы объектам и угрозам, чтобы получить итоговые баллы величины риска (см. Табл. 4).

Таблица 4 – Оценка рисков системы безопасности

Угроза	Объект	Ценность объекта	Значение степени вероятности	Величина риска	Тип риска
УБИ.1.9.8	О.9	4	3	7	Высокий
УБИ.2.2.22	О.2	4	3	7	Высокий
УБИ.3.3.1	О.3	2	1	3	Средний
УБИ.4.4.24	О.4	3	3	6	Высокий
УБИ.5.10.1	О.10	1	0	1	Низкий
УБИ.6.4.15	О.4	3	4	7	Высокий
УБИ.7.2.22	О.2	4	1	5	Средний

Угроза	Объект	Ценность объекта	Значение степени вероятности	Величина риска	Тип риска
УБИ.8.3.15	О.3	2	2	4	Средний
УБИ.9.11.4	О.11	4	4	8	Высокий
УБИ.10.10.13	О.10	1	1	2	Низкий
УБИ.11.3.3	О.3	2	4	6	Высокий

Окончательный шаг заключается в подсчете всех итоговых баллов активов системы, чтобы получить баллы системы. Сумма величин рисков системы равна 56. Построим диаграмму оценки рисков на основе типа риска (см. Рис. 17).

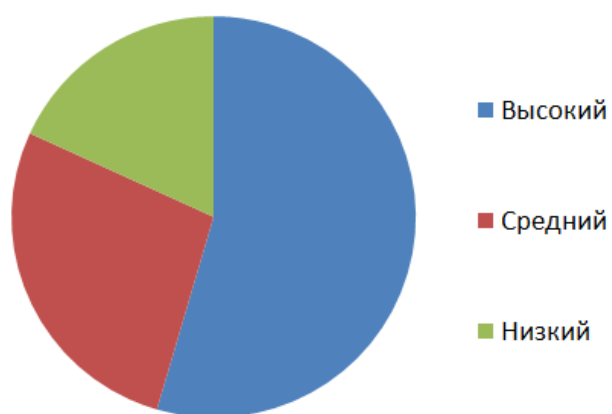


Рисунок 17 – Диаграмма оценки рисков по типам

Полученная оценка и диаграмма говорят о необходимости принятия мер противодействия угрозам [10].

## 6 Составление перечня мер по противодействию выявленным угрозам

Для каждой из ранее выявленных угроз необходимо подобрать оптимальную защитную меру, которая позволит устранить угрозу либо снизить её опасность, и обосновать данный выбор. Угрозы и соответствующие меры защиты приведены в таблице (см. Табл. 5).

Таблица 5 – Меры противодействия

Угроза	Мера противодействия
УБИ.1.9.8	ЗИС.35.1 Фильтрация сетевого трафика, в том числе между внешними сетями и внутренними, в том числе при организации сетевого обмена с сетями связи общего пользования.
УБИ.2.2.22	УПД.6.2 Блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа.
УБИ.3.3.1	АУД.2.1 Выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением.
УБИ.4.4.24	ЗТС.3.1 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены.
УБИ.5.10.1	АУД.2.4 Информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации.

Угроза	Мера противодействия
УБИ.6.4.15	ОДТ.4.1 Резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью.
УБИ.7.2.22	УПД.6.2 Блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа.
УБИ.8.3.15	ЗТС.3.1 Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, помещения и сооружения, в которых они установлены.
УБИ.9.11.4	АВЗ.4.1 Получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов).
УБИ.10.10.13	ИПО.3.1 Проведение практических занятий с персоналом по правилам безопасной работы.
УБИ.11.3.3	ЗИС.35.4 Отключение неиспользуемых сетевых протоколов компонентами инфраструктуры, хостовой операционной системы.

Для угрозы УБИ.1.9.8 «Угроза утечки информации, обрабатываемой средством защиты информации, за счет сканирования сетевой инфраструктуры» выбрана мера ЗИС.35.1 «Фильтрация сетевого трафика, в том числе между внешними сетями и внутренними, в том числе при организации сетевого обмена с сетями связи общего пользования», потому что классические варианты сканирования обнаруживаются межсетевым экраном, который применяется для фильтрации трафика.

Применение меры ЗТС.3.1 «Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены,

исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены» для угроз УБИ.4.4.24 «Угроза несанкционированной подмены компонентов устройства хранения данных за счет физического воздействия» и УБИ.8.3.15 «Угроза нарушения функционирования (работоспособности) периферийного оборудования за счет шифрования данных» исключит возможность несанкционированного физического доступа к компонентам периферийного оборудования и устройства хранения данных.

Применение меры УПД 6.2 «Блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа» по отношению к угрозам УБИ.2.2.22 «Угроза несанкционированного доступа к серверу за счет атаки на веб-приложение» и УБИ 7.2.22 «Угроза ненадлежащего (нецелового) использования сервера за счет атаки на веб-приложение» подходит, так как она сильно ограничивает возможности злоумышленника, уменьшая количество попыток получения доступа к серверу, и требует немного ресурсов для ее внедрения.

Применение меры АУД.2.1 «Выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением» по отношению к УБИ.3.3.1 «Угроза несанкционированной модификации (искажения) компонентов периферийного оборудования за счет эксплуатации уязвимостей» позволит улучшить систему мониторинга уязвимостей.

Принятие меры АУД.2.4 «Информирование должностных лиц оператора (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты



информации» к УБИ.5.10.1 «Угроза удаления информации, обрабатываемой мобильным устройством за счет эксплуатации уязвимостей» повысит информированность должностных лиц, что поможет компенсировать отсутствие политики по использованию мобильных устройств.

Мера ОДТ.4.1 «Резервное копирование информации на резервные машинные носители информации с установленной оператором периодичностью» к УБИ.6.4.15 «Угроза вызова отказа в обслуживании устройства хранения данных за счет шифрования данных» позволит избежать негативные последствия, вызванных выходом из строя устройства хранения данных.

Мера АВЗ.4.1 «Получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов)» к УБИ.9.11.4 «Угроза получения информации (данных), содержащейся в системах и сетях, из недоверенного источника за счет внедрения вредоносного программного обеспечения» позволит контролировать своевременность обновлений баз данных антивирусов.

Принятие меры ИПО.3.1 «Проведение практических занятий с персоналом по правилам безопасной работы» по отношению к УБИ.10.10.13 «Угроза распространения противоправной информации через компоненты мобильного устройства за счет реализации социальной инженерии» повысит устойчивость персонала к методам воздействия социальной инженерии.

Применение меры ЗИС.35.4 «Отключение неиспользуемых сетевых протоколов компонентами инфраструктуры, хостовой операционной системы, вычислительной сети» к УБИ.11.3.3 «Угроза несанкционированного массового сбора информации с периферийного оборудования за счет использования недостатков архитектуры» позволит снизить риск несанкционированного массового сбора информации с периферийного оборудования.

Предложенные меры противодействия помогут снизить величину риска и повысить степень защищенность рассматриваемой информационной системы, при этом их принятие не требует больших финансовых затрат компании.

## ЗАКЛЮЧЕНИЕ

В результате работы с информационной системой компании, занимающейся разработкой онлайн-игр, был определён тип информационной системы (данная система относится к классу ИСПДн, в ней содержатся и обрабатываются персональные данные пользователей), определён перечень применяемых средств защиты информации, составляющие менеджмента рисков информационной системы на основе методических документов ФСТЭК и государственных стандартов, а также был сформирован список объектов и компонентов воздействия с помощью раздела «Формирование перечня угроз» на сайте ФСТЭК.

На основе вышеупомянутого списка были построены модели нарушителя и угроз, в которых были выявлены виды нарушителя и уровни его возможностей, а для построения модели угроз были использованы объекты, определенные ранее, способы реализации и уязвимости.

Исходя из построенных моделей, была проведена количественная оценка риска согласно стандарту ГОСТ ИСО МЭК 27005-2010, по результатам которой был предложен и обоснован перечень мер противодействия выявленным угрозам.

Конечным результатом проведённой работы является комплексный анализ защищённости рассматриваемой информационной системы.

Таким образом, в рамках прохождения практики по получению профессиональных умений и опыта профессиональной деятельности были получены навыки проведения риск-анализа информационных систем, работы с нормативно-правовой документацией в области ИБ, построения моделей нарушителя и угроз и проведения количественной оценки рисков. Полученные знания и опыт будут очень полезны в дальнейшей работе в сфере ИБ.

## СПИСОК ЛИТЕРАТУРЫ

1 Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ – Электрон. дан. – Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61798/](http://www.consultant.ru/document/cons_doc_LAW_61798/)

2 Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ – Электрон. дан. – Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_61801/](http://www.consultant.ru/document/cons_doc_LAW_61801/)

3 Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» – Электрон. дан. – Режим доступа: <https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21>

4 Постановление правительства РФ от 1 ноября 2012 года №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» – Электрон. дан. – Режим доступа: <https://data-sec.ru/laws/1119-personal-data-security/>

5 Методический документ «Методика оценки угроз безопасности информации» – Электрон. дан. – Режим доступа: <https://fstec.ru/en/component/attachments/download/2919>

6 ГОСТ Р ИСО/МЭК 13335-3–2007 «Информационная технология. Методы и средства обеспечения безопасности. Методы менеджмента безопасности информационных технологий». – М.: Стандартинформ. – 2007. – 45 с.;

7 ГОСТ Р ИСО/МЭК 27018 – 2020 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по защите персональных данных (ПДн) в публичных облаках, используемых для их обработки». – М.: Стандартинформ. – 2020. – 32 с.;

8 ГОСТ Р ИСО/МЭК 27034-1-2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений». – М.: Стандартинформ. – 2014. – 72 с.;

9 ГОСТ Р ГОСТ ИСО/МЭК 12207 – 2010 «Информационная технология. Системная и программная инженерия «Процессы жизненного цикла программных средств». – М.: Стандартинформ. – 2010. – 100 с.;

10 Банк данных угроз безопасности информации Электрон. дан. – Режим доступа: <https://bdu.fstec.ru/threat-section/shaper-threats>

11 Методический документ «Методика моделирования угроз безопасности информации» – Электрон. дан. – Режим доступа: <https://fstec.ru/en/component/attachments/download/2727>

12 ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». – М.: Стандартинформ. – 2010. – 51 с.;