**Министерство науки и высшего образования РФ**

Федеральное государственное автономное образовательное учреждение высшего образования «Московский политехнический университет»

**(МОСКОВСКИЙ ПОЛИТЕХ)**

**Модель угроз информационной безопасности**

**для информационной системы биометрического**

**терминала банка “Ак Барс” модели POS**

Выполнили:

Студенты 3 курса

Группы 181-352

Захаров В.А.

Константинов Д.А.

г. Москва

2021 г.

**Обозначения и сокращения**

|  |  |
| --- | --- |
| АВПО - | антивирусное программное обеспечение |
| АРМ – | автоматизированное рабочее место |
| БД – | база данных |
| ИС – | информационная система |
| КЗ – | контролируемая зона |
| ЛВС – | локально-вычислительная сеть |
| МЭ – | межсетевой экран |
| НДВ – | не декларированные возможности |
| НСД – | несанкционированный доступ |
| ОС – | операционная система |
| ПО – | программное обеспечение |
| ППО – | прикладное программное обеспечение |
| ПТС – | программно-технические средства |
| ПЭМИН – | побочные электромагнитные излучения и наводки |
| РД – | руководящие документы |
| РСБ – | регистрация событий безопасности |
| САВЗ – | средство антивирусной защиты информации |
| СВТ – | средства вычислительной техники |
| СЗ – | система (подсистема) защиты |
| СЗИ – | средства защиты информации |
| СОВ – | система обнаружения вторжений |
| СУБД – | система управления базами данных |
| ТУ – | технические условия |
| УБ – | угрозы безопасности |
| СКЗИ – | средство криптографической защиты информации |
| POS – | Point Of Sale — точка продажи |

1. **Термины и определения**

В настоящем документе используются следующие термины и их определения:

**Автоматизированная система** – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

**Аутентификация отправителя данных** – подтверждение того, что отправитель полученных данных соответствует заявленному.

**Безопасность персональных данных** – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

**Блокирование персональных данных** – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

**Вирус (компьютерный, программный)** – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

**Вредоносная программа** – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

**Вспомогательные технические средства и системы** – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных, или в помещениях, в которых установлены информационные системы персональных данных.

**Доступ в операционную среду компьютера (информационной системы персональных данных)** – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

**Доступ к информации** – возможность получения информации и ее использования.

**Закладочное устройство** – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

**Защищаемая информация** – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации. **Идентификация** – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем

присвоенных идентификаторов.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информативный сигнал** – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные), обрабатываемая в информационной системе персональных данных.

**Информационная система персональных данных** – это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

**Информационные технологии** – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

**Источник угрозы безопасности информации** – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

**Контролируемая зона** – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

**Конфиденциальность персональных данных** – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространения без согласия субъекта персональных данных или наличия иного законного основания.

**Межсетевой экран** – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

**Нарушитель безопасности персональных данных** – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

**Недекларированные возможности** – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

**Несанкционированный доступ (несанкционированные действия)** – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.

**Носитель информации** – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

**Обработка персональных данных** – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

**Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

**Перехват (информации)** – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

**Персональные данные** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

**Побочные электромагнитные излучения и наводки** – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

**Пользователь информационной системы персональных данных** – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

**Правила разграничения доступа** – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

**Программная закладка** – скрытно внесенный в программное обеспечение функциональный объект, который при определенных условиях способен обеспечить несанкционированное программное воздействие. Программная закладка может быть реализована в виде вредоносной программы или программного кода.

**Программное (программно-математическое) воздействие** - несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

**Ресурс информационной системы** – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

**Средства вычислительной техники** – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

**Субъект доступа (субъект)** – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

**Технические средства информационной системы персональных данных** – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

**Технический канал утечки информации** – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

**Угрозы безопасности персональных данных** – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

**Уничтожение персональных данных** – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

**Утечка (защищаемой) информации по техническим каналам** – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

**Уязвимость** – некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.

**Целостность информации** – состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

1. **Общие положения**
   1. Разработка модели угроз безопасности информации, обрабатываемой в информационной системе биометрического терминала банка «Ак Барс» (далее – ИС «Ак Барс») проведена в соответствии с:

- Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

- Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных»;

- Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных постановлением Правительства Российской Федерации от 1 ноября 2012 г. №1119.

- Федеральный закон от 27 июня 2011 г. № 161-ФЗ г. Москва "О национальной платежной системе"

* 1. Модель угроз безопасности информации, обрабатываемой в ИС «Ак Барс» разработана на основании:

- Методики оценки угроз безопасности информации, утвержденной приказом заместителя директора ФСТЭК от 5 февраля 2021 г.;

- Банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю, расположенной на информационном ресурсе <http://bdu.fstec.ru/threat>;

- Книге “Персональные данные: что было, что будет, на чем сердце успокоится...” под авторством Ксении Шудровой, расположенной на информационном ресурсе http://shudrova.blogspot.com/p/blog-page\_23.html;

* 1. Модель угроз содержит данные по УБ, связанные с:

- Перехватом (съемом) информации по техническим каналам с целью их копирования или неправомерного распространения;

- Несанкционированным, в том числе случайным, доступом в систему с целью нарушения конфиденциальности (неправомерные доступ, копирование, предоставление или распространение), целостности (неправомерные уничтожение или модифицирование) или доступности (неправомерное блокирование) информации.

* 1. Моделью угроз необходимо руководствоваться на всех этапах жизненного цикла системы: при проектировании, в режиме эксплуатации, при проведении регламентных и ремонтно-профилактических работ, модернизации и выводе ее из эксплуатации.
  2. Частная модель угроз применяется при решении следующих задач:

- Анализа защищенности от угроз безопасности в ходе организации и выполнения работ по обеспечению безопасности;

- Разработки системы защиты, обеспечивающей нейтрализацию угроз с использованием методов и способов защиты;

- Проведения мероприятий, направленных на предотвращение НСД к информации и (или) модификации и блокированию действий лиц, не имеющих права доступа информации;

- Недопущения воздействия на технические средства системы, в результате которого может быть нарушено их функционирование;

- Контроля над обеспечением требований к установленному классу защищенности ИС.

* 1. Угрозы безопасности информации, содержащиеся в настоящей модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития способов и средств реализации угроз безопасности информации в ИС.
  2. Плановый пересмотр проводится с периодичностью не реже чем один раз в 3 года. По результатам анализа проводится уточнение (при необходимости) модели угроз безопасности информации.
  3. Пересмотр (переоценка) угроз безопасности информации осуществляется в случаях:

- изменения требований законодательства Российской Федерации о защите информации, нормативных правовых актов и методических документов, регла­ментирующих защиту информации;

- изменения конфигурации (состава основных компонентов) и особенностей функционирования информационной системы, следствием которых стало воз­никновение новых угроз безопасности информации;

- выявления уязвимостей, приводящих к возникновению новых угроз без­опасности информации или к повышению возможности реализации существую­щих;

- появления сведений и фактов о новых возможностях нарушителей.

* 1. Принципы модели угроз:

- Безопасность персональных данных и иной защищаемой информации при их обработке в информационных системах обеспечивается с помощью системы защиты информации в ИС «Ак Барс».

- При формировании модели угроз необходимо учитывать как угрозы, осуществление которых нарушает безопасность персональных данных и иной защищаемой информации (далее – прямая угроза), так и угрозы, создающие условия для появления прямых угроз (далее – косвенные угрозы) или косвенных угроз.

- Персональные данные обрабатываются и хранятся в информационной системе с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

- Криптосредство штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к криптосредству требований и которые образуют среду функционирования криптосредства (СФК).

- Система защиты информации ИС «Ак Барс» (в том числе и СКЗИ) не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (система защиты информации не предназначена для защиты информации от раскрытия лицами, которым предоставлено право на доступ к этой информации).

- Нарушитель может действовать на различных этапах жизненного цикла криптосредства и СФК (под этими этапами в настоящем документе понимаются разработка, производство, хранение, транспортировка, ввод в эксплуатацию, эксплуатация программных и технических средств криптосредства и СФК).

- Криптографическая защита информации может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ.

- СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований, действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ.

- Для обеспечения безопасности персональных данных при их обработке в информационных системах должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия.

- СКЗИ являются как средством защиты информации, так и объектом защиты.

**3.  Описание ИС Биотерминала «Ак Барс»**

* 1. Общие сведения об информационной системе:
* Сервер ядра ИС:
  1. ЦПУ не менее 8-х;
  2. ОЗУ не менее 8Gb;
  3. Объем жесткого диска не менее 40Gb;
  4. Ubuntu 18.04.5 LTS;
  5. Доступ в глобальную сеть интернет (на момент установки и настройки);
  6. Доступ в локальную сеть
* Сервер локальной части:
  1. ЦПУ не менее 8-х;
  2. ОЗУ не менее 8Gb;
  3. Объем жесткого диска не менее 40Gb;
  4. Ubuntu 18.04.5 LTS;
  5. Доступ в глобальную сеть интернет (на момент установки и настройки);
  6. Доступ в локальную сеть
* Терминал распознавания:
  1. Архитектура NVIDIA
  2. Ubuntu 18.04.5 LTS;
  3. Объем жесткого диска не менее 16Gb;
  4. Доступ в глобальную сеть интернет (на момент установки и настройки);
  5. Доступ в локальную сеть для связи с сервером
  6. Web камера инфракрасная
  7. Стерео камера
  8. Maxwell Процессор ARM
  9. Cortex-A57 MPCore
  10. Оперативная память - 4 Гб
  11. Синхронизированная стерео-камера 1500р
  12. ИК-камера 720р
  13. Подсветка в ИК и оптическом диапазоне
  14. Дисплей 1920\*1080 - Диагональ 13 дюймов
  15. Touch-screen дисплей
  16. Приложения и компоненты:

ИС «Ак Барс» состоит из десяти приложений и модулей, собственной разработки разделенные на 4 части:

* Сервер ядра ИС:
  1. Abdt.Face2Action. Auth – Сервис авторизации
  2. Abdt.Face2Action.Sync.Matcher – Модуль БД для сравнения эмбедингов
  3. Abdt.Face2Action.Extractor – Приложение для получение эмбедингов с фотографии
  4. Abdt.Face2Action.Server.Sync – Приложение для внесения информации о ФИО и номерах карт СКУД
  5. Abdt.Face2Action.Validator.Server – Приложение для внесения эмбедингов и внесения в БД
  6. Abdt.Face2Pass.Broker – Приложение предоставление информации о пользователе
  7. Abdt.Face2Action.Logger.Server – Приложение для внесения информации о попытках проходов
  8. Abdt.Face2Action.Journal – Приложение получения информации о попытках проходов
  9. Abdt.Face2Action.WebJournal – Веб сайт для отображения информации
* Сервер локальной части:
  1. Abdt.Face2Pass.Validator.Local – Приложение сравнения фотографии полученной с терминала и эмбединга сохраненного в БД
  2. Abdt.Face2Pass.Local.Sync – Приложение получения информации с серверной части в локальную и передачи информации о проходах
  3. Abdt.Face2Action.Extractor – Приложение для получение эмбедингов с фотографии
* Терминал распознавания:
  1. Abdt.Face2Pass.Terminal – Приложение для отображения информации о нахождении сотрудника в БД. Приложение реализовано на архитектуре AARM64 и работает на оборудовании Nvidia Jetson Nano
  2. Abdt.Face2Loyalty.Terminal – система лояльности, основанная на технологии распознавания лиц при помощи терминала INOFACE.
  3. Abdt.Face2Pay.Terminal

Для полноценного запуска системы и дальнейшей работы дополнительно будут установлены сторонние программы и компоненты:

* PostgreSQL 11 – база данных;
* Minio s3 – объектное хранилище, для хранения фотографий сотрудников с терминалов;
* Nginx – http сервер;

**4.  Возможности нарушителей (модель нарушителя)**

* 1. В качестве источников угроз несанкционированного доступа к информации при ее обработке в ИС могут выступать лица (нарушители), случайно или преднамеренно совершающие действия, следствием которых может стать нарушение одного из свойств безопасности информации (конфиденци­альности, целостности, доступности).
  2. В настоящем документ представлена лишь часть разработанный модели нарушитель, чтобы ознакомиться с действующей версия следует перейди в EXEL таблицу.
  3. Нарушители подразделяются на два типа в зависимости от возможностей доступа к информационной системе:

- внешние нарушители - лица, не имеющие права доступа к инфор­мационной системе, ее отдельным компонентам и реализующие угрозы безопас­ности информации из-за границ информационной системы;

- внутренние нарушители - лица, имеющие право постоянного или разового доступа к информационной системе или к ее отдельным компонентам.

* 1. Угрозы безопасности информации в информационной системе могут быть реализованы следующими видами нарушителей:

- специальные службы иностранных государств (блоков государств);

- внешние субъекты (физические лица);

- разработчики, производители, поставщики программных, технических и программно-технических средств;

- лица, обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.);

- пользователи информационной системы;

- системные администраторы;

- бывшие работники (пользователи).

- и тд.

* 1. Предположения о видах нарушителей и их целях (мотивации) реализации угроз безопас­ности информации приведены в таблице 1.

Таблица 1

| № вида | Вид нарушителя | Тип нарушителя | Возможные цели (мотивации) реализации УБ |
| --- | --- | --- | --- |
|  | Специальные службы иностран­ных госу­дарств (бло­ков государств) | Внешний, внутренний | Дискредитация или дестабилизация деятельности предприятия. |
|  | Внешние субъ­екты (фи­зические лица) | Внешний | Идеологические или политиче­ские мотивы. Любопытство или желание са­мореали­зации (подтверждение ста­туса). Выявление уязвимостей с це­лью их дальнейшей продажи и получения фи­нансовой выгоды. |
|  | Разработчики, про­изво­дители про­граммных, тех­нических и про­граммно-техниче­ских средств | Внешний | Внедрение дополнительных функцио­нальных возможностей в ПО или ПТС на этапе разработки. Непреднамеренные, неосто­рожные или неквалифициро­ванные действия. |
|  | Лица, обслужи­вающие ин­фра­структуру опера­тора (администра­ция, охрана, убор­щики и т.д.) | Внутренний | Непреднамеренные, неосто­рожные или неквалифицированные действия. |
|  | Пользователи ин­форма­ционной сис­темы | Внутренний | Любопытство или желание са­мореали­зации (подтверждение ста­туса). Месть за ранее совершенные дейст­вия. Непреднамеренные, неосто­рожные или неквалифициро­ванные действия. |
|  | Системные адми­нистраторы, адми­нистраторы без­опасности | Внутренний | Любопытство или желание са­мореали­зации (подтверждение ста­туса). Месть за ранее совершенные дейст­вия. Выявление уязвимостей с це­лью их дальнейшей продажи и полу­чения иной выгоды. Непреднаме­ренные, неосто­рожные или неквалифи­циро­ванные действия. |
|  | Бывшие работ­ники (пользова­тели) | Внешний | Причинение имущественного ущерба путем мошенничества или иным пре­ступным путем. Месть за ранее совер­шенные действия |

* 1. Возможности каждого вида нарушителя по реализации угроз безопасности информации характеризуются его потенциалом. Потенциал нарушителя опреде­ляется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации.

В зависимости от потенциала, требуемого для реализации угроз безопас­ности информации, нарушители подразделяются:

- на нарушителей, обладающих базовым (низким) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

- на нарушителей, обладающих базовым повышенным (средним) потенциалом нападения при реализации угроз безопасности информации в информационной системе;

- на нарушителей, обладающих высоким потенциалом нападения при реализа­ции угроз безопасности информации в информационной системе.

Потенциал нарушителей и их возможности приведены в таблице 2.

Таблица 2

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Потенциал нарушителей | Виды нарушите­лей | Возможности по реализации угроз без­опасности информации |
| 1 | Нарушители с базовым (низ­ким) по­тенци­алом | Внешние субъ­екты (физические лица),  лица, об­служи­вающие инфра­структуру опера­тора, пользова­тели информаци­онной системы,  бывшие работ­ники, | Имеют возможность получить инфор­мацию об уязвимостях отдель­ных ком­понент информационной сис­темы, опуб­ликованную в общедос­тупных ис­точниках.  Имеют возможность получить инфор­мацию о методах и средствах реализа­ции угроз безопасности инфор­мации (компьютерных атак), опубликован­ных в общедоступных источниках, и (или) самостоятельно осуществляет создание методов и средств реализа­ции атак и реализа­цию атак на информационную сис­тему |
| 2 | Нарушители с базовым повышенным (средним) по­тенциалом | Разработчики, про­изводители, поставщики про­граммных, техни­ческих и про­граммно- техниче­ских средств, ад­мини­страторы ин­фор­мационной сис­темы и адми­нист­раторы без­опасно­сти | Обладают всеми возможностями нару­шителей с базовым потенциа­лом.  Имеют осведомленность о мерах за­щиты информации, применяемых в ин­формационной системе данного типа.  Имеют возможность получить инфор­мацию об уязвимостях отдель­ных ком­понент информационной сис­темы пу­тем проведения, с исполь­зованием имеющихся в свобод­ном доступе про­граммных средств, анализа кода при­кладного программного обеспечения и отдель­ных программных компонент общесис­темного программного обеспе­чения.  Имеют доступ к сведениям о струк­турно - функциональных характеристи­ках и особенностях функ­ционирования информационной системы. |
| 3 | Нарушители с высоким по­тенциалом | Специальные службы ино­стран­ных госу­дарств (блоков государств) | Обладают всеми возможностями на­рушителей с базовым и базовым по­вышенным потенциалами.  Имеют возможность осуществлять не­санкционированный доступ из выде­ленных (ведомственных, корпора­тив­ных) сетей связи, к кото­рым возможен физический доступ (незащищенных ор­ганизационными мерами).  Имеют возможность получить дос­туп к системному и при­кладному про­грамм­ному обеспечению, телеком­му­никационному оборудова­нию и другим программно-техниче­ским средствам информационной сис­темы для преднамеренного внесе­ния в них уязвимостей или программ­ных закла­док.  Имеют хорошую осведомленность о мерах защиты информации, применяе­мых в информационной сис­теме, об ал­горитмах, аппаратных и программ­ных средствах, используе­мых в инфор­маци­онной системе. |

* 1. Угрозы безопасности информации могут быть реализованы нарушителями за счет:

- несанкционированного доступа и (или) воздействия на объекты на аппа­ратном уровне;

- несанкционированного доступа и (или) воздействия на объекты на обще­системном уровне (базовые системы ввода-вывода, операционные системы);

- несанкционированного доступа и (или) воздействия на объекты на при­кладном уровне (системы управления базами данных, браузеры, web- приложения, иные прикладные программы общего и специального назначения);

- несанкционированного доступа и (или) воздействия на объекты на сетевом уровне (сетевое оборудование, сетевые приложения, сервисы);

- несанкционированного физического доступа и (или) воздействия на линии, (каналы) связи, технические средства;

- воздействия на пользователей, админи­страторов информационной системы или обслуживающий персонал (социальная инженерия).

- при обработке, включая сбор, биометрических персональных данных на устройстве клиента-физического лица (угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения целостности (подмены, удаления) информации о степени соответствия биометрических персональных данных гражданина Российской Федерации).

- при сборе биометрических персональных данных в государственных органах, банках и иных организациях, включая сбор биометрических персональных данных и передачу собранных биометрических персональных данных между структурными подразделениями государственного органа, банка и иной организации ( угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных).

- при передаче собранных биометрических персональных данных между государственным органом, банком, иной организацией и единой биометрической системой (угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), угроза нарушения конфиденциальности (компрометации) биометрических персональных данных).

- при обработке информации о степени соответствия в банках (угроза нарушения целостности (подмены, удаления) информации о степени соответствия в банках).

- при передаче информации о степени соответствия между банком и единой биометрической системой (угроза нарушения целостности (подмены, удаления) информации о степени соответствия, угроза нарушения конфиденциальности (компрометации) информации о степени соответствия).

- при обработке, хранении, проверке биометрических персональных данных, обработке и передаче информации о степени соответствия в единой биометрической системе (угроза нарушения целостности (подмены, удаления) биометрических персональных данных, нарушения конфиденциальности (компрометации) биометрических персональных данных, нарушения достоверности биометрических персональных данных (внесения фиктивных биометрических персональных данных), нарушения целостности (подмены, удаления) информации о степени соответствия, нарушения доступности (блокирования передачи) информации о степени соответствия).

* + 1. **Возможные негативные последствия от реализации (возникновения) угроз безопасности информации**

|  |  |  |
| --- | --- | --- |
| Негативные  последствия | Объекты воздействия | Виды воздействия |
| Разглашение  персональных  данных граждан  (У1) | База данных  информационной  системы, содержащая  идентификационную  информацию граждан | Утечка идентификационной информации граждан из базы данных |
| Удаленное  автоматизированное  рабочее место (АРМ)  пользователя | Утечка идентификационной информации граждан с АРМ пользователя |
| Линия связи между  сервером основного  центра обработки  данных и сервером  резервного центра  обработки данных | Перехват информации, содержащей  идентификационную информацию граждан, передаваемой по линиям связи |
| Линия связи между  Биометрических терминалом и сервером  резервного центра  обработки данных | Перехват информации, содержащей  идентификационную информацию граждан, передаваемой по линиям связи |

**Актуальные угрозы безопасности информации**

* + 1. **Определение уровня исходной защищенности информационной системы**

Под уровнем исходной защищенности ИС понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИС, определяемый экспертным методом. Результаты анализа исходной защищенности приведены в таблице 3.

Таблица 3

| Технические и эксплуатационные характеристики ИС | Уровень защищенности | | |
| --- | --- | --- | --- |
| Высокий | Средний | Низкий |
| 1. По территориальному размещению: | | | |
| распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом; | – | – | + |
| 2. По наличию соединения с сетями общего пользования: | | | |
| ИС, имеющая одноточечный выход в сеть общего пользования; | – | – | + |
| 3. По встроенным (легальным) операциям с записями баз персональных данных: | | | |
| чтение, поиск; | – | – | + |
| запись, удаление, сортировка; | – | – | + |
| модификация, передача | – | – | + |
| 4. По разграничению доступа к персональным данным: | | | |
| ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн; | – | – | + |
| 5. По наличию соединений с другими базами персональных данных иных информационных систем: | | | |
| интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн); | – | – | + |
| 6. По уровню обобщения (обезличивания) ресурсов: | | | |
| ИC, в которой предоставляемые пользователю данные не являются обезличенными (т.е. присутствует информация, позволяющая идентифицировать субъекта персональных данных) | – | – | + |
| 7. По объему конфиденциальной информации, которая предоставляется сторонним пользователям без предварительной обработки: | | | |
| ИС, предоставляющая часть персональных данных | – | – | + |
| **Характеристики ИС по уровням, %** | **0,00** | **00,00** | **99,99** |

Интегрально по всем техническим и эксплуатационным характеристикам ИС уровень исходной защищенности определяется следующим образом:

* ИС имеет **высокий уровень исходной защищенности**, если не менее 70% характеристик ИС соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу);
* ИС имеет **средний уровень исходной защищенности**, если не выполняются условия по пункту 1 и не менее 70% характеристик ИС соответствуют уровню не ниже «средний» (берется отношение суммы положительных решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности;
* ИС имеет **низкий уровень исходной защищенности**, если не выполняются условия по пунктам 1 и 2.

При составлении перечня актуальных угроз безопасности каждому уровню исходной защищенности ставится в соответствие числовой коэффициент ***Y1***:

**0** – для высокого уровня исходной защищенности;

**5** – для среднего уровня исходной защищенности;

**10** – для низкого уровня исходной защищенности.

Таким образом, ИС «Ак Барс» имеет низкий уровень исходной защищенности (Y1 = 10), так как не выполняются условия по пунктам 1 и 2.

**Определение вероятности, возможности реализации, опасности и актуальности угроз безопасности информации**

Для оценки возможности реализации угрозы применяются два показателя: уровень исходной защищенности ИС и частота (вероятность) реализации рассматриваемой угрозы.

Под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации для данной ИС в складывающихся условиях обстановки. Используем четыре вербальных градации этого показателя:

**маловероятно** – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

**низкая вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

**средняя вероятность** – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности недостаточны;

**высокая вероятность** – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности не приняты.

Для составления перечня актуальных угроз безопасности каждой градации вероятности возникновения угрозы ставим в соответствие числовой коэффициент Y2:

**0** – для маловероятной угрозы;

**2** – для низкой вероятности угрозы;

**5** – для средней вероятности угрозы;

**10** – для высокой вероятности угрозы.

С учетом изложенного коэффициент реализуемости угрозы Y определяем соотношением:

**Y = (Y1+Y2)/20**.

По значению коэффициента реализуемости угрозы Y формируем вербальную интерпретацию реализуемости угрозы следующим образом:

если **0 ≤ Y ≤ 0.3**, то возможность реализации угрозы признается низкой;

если **0.3 < Y ≤ 0.6**, то возможность реализации угрозы признается средней;

если **0.6 < Y ≤ 0.8**, то возможность реализации угрозы признается высокой;

если **Y > 0.8**, то возможность реализации угрозы признается очень высокой.

Оценка опасности (ущерба) каждой угрозы выполняется экспертным путем, при котором определяется вербальный показатель, имеющий три значения:

**низкая опасность** – если реализация угрозы может привести к незначительным негативным последствиям;

**средняя опасность** – если реализация угрозы может привести к негативным последствиям;

**высокая опасность** – если реализация угрозы может привести к значительным негативным последствиям.

Актуальной считается угроза, которая может быть реализована в информационной системе и представляет опасность. Решение об актуальности угрозы безопасности информации принимается в соответствии с таб­лицей 4.

Таблица 4

|  |  |  |  |
| --- | --- | --- | --- |
| **Возможность реализации угрозы** | **Показатель опасности угрозы** | | |
| **Низкая** | **Средняя** | **Высокая** |
| Низкая | неактуальная | неактуальная | актуальная |
| Средняя | неактуальная | актуальная | актуальная |
| Высокая | актуальная | актуальная | актуальная |

В качестве исходных данных об угрозах безопасности информации и их характеристиках, используется банк данных угроз безопасности информации, сформированный и поддерживаемый ФСТЭК России, а также иные источники, в том числе опубликованные в общедоступных источниках информации.

Результаты определения вероятности, возможности реализации, опасности и актуальности угроз безопасности информации приведены в EXEL таблице.

* + 1. **Актуальные угрозы, способы противодействия**

В таблице 6 представлены актуальные угрозы безопасности для ИС «Ак Барс», а также способы противодействия им.

Таблица 6

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование угрозы** | **Меры по защите от угроз** | |
| **Организационные** | **Технические** |
| ***1*** | Угроза анализа криптографических алгоритмов и их реализации | Использование актуальных версий сертифицированных средств криптографической защиты информации. | Своевременная установка обновле­ний программного обеспе­чения, направленного на устране­ние выявленных уязвимостей ПО |
| ***2*** | Угроза внедрения кода или данных | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. | Своевременная установка обновле­ний программного обеспе­чения, направленного на устране­ние выявленных уязвимостей ПО |
| ***3*** | Угроза воздействия на программы с высокими привилегиями |  | ? |
| ***4*** | Угроза деструктивного изменения конфигурации/среды окружения программ |  | ? |
| ***5*** | Угроза доступа к защищаемым файлам с использованием обходного пути | Информирование пользователей о возможности реализации данной угрозы и вероятными последствиями от ее реализации. | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов |
| ***6*** | Угроза загрузки нештатной операционной системы | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. | Наличие списка разрешенных внешних периферийных устройств |
| ***7*** | Угроза изменения компонентов системы | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. | Наличие в системе функции вычисления контрольной суммы целостности и ее сопоставление с уже имеющейся в системе |
| ***8*** | Угроза искажения вводимой и выводимой на периферийные устройства информации |  | ? |
| ***9*** | Угроза использования информации идентификации/аутентификации, заданной по умолчанию | Инвентаризация и анализ установленного на серверах программного обеспечения на предмет наличия учетных записей «по умолчанию» | Блокирование встроенных учетных записей с администраторскими правами |
| ***10*** | Угроза использования механизмов авторизации для повышения привилегий |  | ? |
| ***11*** | Угроза использования слабостей протоколов сетевого/локального обмена данными |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. |
| ***12*** | Угроза неправомерного ознакомления с защищаемой информацией | Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. Использова­ние плотных штор или жа­люзи на окнах. Меры по получению доступа в по­меще­ние. Ручная блоки­ровка экрана | Автоматическая блоки­ровка эк­рана по достиже­нии заданного вре­мени не активности. |
| ***13*** | Угроза неправомерных действий в каналах связи |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. |
| ***14*** | Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети | Мониторинг состояния средств межсетевого экранирования и фильтрации сетевого трафика | Исключение средствами межсетевого экранирования доступа из внешних сетей к активному сетевому оборудованию, установка в настройках оборудования разрешения на администрирование устройств только с определенного пула адресов, принадлежащих внутренней сети организации |
| ***15*** | Угроза несанкционированного доступа к аутентификационной информации |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. |
| ***16*** | Угроза обхода некорректно настроенных механизмов аутентификации | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. | Своевременная установка обновле­ний программного обеспе­чения, направленного на устране­ние выявленных уязвимостей ПО |
| ***17*** | Угроза перехвата вводимой и выводимой на периферийные устройства информации | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. Определение перечня лиц, допу­щенных в помещение, где расположены компоненты ИС. Использова­ние плотных штор или жа­люзи на окнах. Меры по получению доступа в по­меще­ние. Ручная блоки­ровка экрана | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов. Своевременная установка обновлений программного обеспечения, направленного на устранение выявленных уязвимостей ПО |
| ***18*** | Угроза перехвата данных, передаваемых по вычислительной сети |  | Защита персональной информации путём использования шифровальных (криптографических) алгоритмов |
| ***19*** | Угроза подмены действия пользователя путём обмана | Разработка инструкции по работе в системе, доведение ее до пользователей | Минимизация прав пользователей в системе |
| ***20*** | Угроза подмены доверенного пользователя | Разработка инструкции по работе в системе, доведение ее до пользователей | Минимизация прав пользователей в системе |
| ***21*** | Угроза преодоления физической защиты | Наличие поста охраны, СКУД при входе в организацию, ключевая защита серверной |  |
| ***22*** | Угроза утраты носителей информации | Наличие поста охраны, СКУД при входе в организацию, ключевая защита серверной | Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня. |
| ***23*** | Угроза включения в проект не достоверно испытанных компонентов | Использование сертифицирован­ного программного обеспечения и средств защиты информации. Мониторинг информации об обна­ружении уязвимостей исполь­зуемого ПО и выпуске соответст­вующих исправлений. |  |
| ***24*** | Угроза наличия механизмов разработчика |  | ? |
| ***25*** | Угроза неправомерного шифрования информации |  | Регулярное полное резервное копирование данных. Глубина копирования – не более одного дня. |
| ***26*** | Угроза отказа подсистемы обеспечения температурного режима | Разработка инструкции по действиям сотрудников охраны в случае срабатывания датчика по превышению температуры в серверном помещении | Оснащение серверного помещения основным и резервным кондиционером, установка сигнального датчика и вывод тревожного сигнала на пост охраны здания организации |
| ***27*** | Угроза физического устаревания аппаратных компонентов | Полная ежеквартальная проверка состояния компонентов ИС на их работоспособность | Постоянные мониторинг и тесты аппаратных компонентов |
| ***28*** | Угроза использования уязвимых версий программного обеспечения | Постоянный мониторинг актуальности версий используемого ПО и незамедлительные обновления. |  |
| ***29*** | Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения | Согласно установленной инструкции пользования, советующие обновления происходят в специально выделенные часы работы с 3-5 часов ночи. |  |
| ***30*** |  |  |  |

* + 1. **Способы реализации (возникновения) угроз безопасности информации**