**АДМИНИСТРАЦИЯ**

**НОВОМАКАРОВСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ**

**ГРИБАНОВСКОГО МУНИЦИПАЛЬНОГО РАЙОНА
ВОРОНЕЖСКОЙ ОБЛАСТИ**

**Р А С П О Р Я Ж Е Н И Е**

от 20.08.2021 г. № 31-р

с. Новомакарово

Об утверждении Модели угроз безопасности

персональных данных при их обработке в

информационной системе персональных данных

«Автоматизация бухгалтерского учета» в

администрации Новомакаровского сельского

поселения Грибановского муниципального

района Воронежской области

 Утвердить Модель угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Автоматизация бухгалтерского учёта» в администрации Новомакаровского сельского поселения Грибановского муниципального района Воронежской области.

Глава сельского поселения С.А.Шатов

|  |
| --- |
| УТВЕРЖДАЮГлава администрацииНовомакаровского сельского поселенияГрибановского муниципального района Воронежской области*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*С.А.Шатов«20» августа 2021 года |

Модель угроз безопасности персональных данных

при их обработке в информационной системе персональных данных «Автоматизация бухгалтерского учета»

|  |
| --- |
| Ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных администрации Новомакаровского сельского поселения Грибановского муниципального района \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_С.А.Шатов«20» августа 2021 года |

Содержание

1. Общие положения…….……………………………..….………….……..3
2. Описание информационной системы персональных данных и особенностей ее функционирования…………………………………………........6
3. Возможности нарушителей по реализации угроз безопасности персональных данных……………………………………….………………………9
4. Актуальные угрозы безопасности персональных данных………...….11

Приложение № 1. Топологическая схема информационной системы персональных данных *«Автоматизация бухгалтерского учета»* с обозначением ее составных частей и сегментов.……………….……………......14

Приложение № 2. Перечень актуальных угроз безопасности персональных данных при их обработке в информационной системе персональных данных *«*Автоматизация бухгалтерского учета*»*………………………………………………………………...….…………..15

Приложение № 3. Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для информационной системы персональных данных *«Автоматизация бухгалтерского учета»*………………….……..………….......18

1. **Общие положения**

В настоящей модели угроз безопасности персональных данных при их обработке в информационной системе персональных данных «Автоматизация бухгалтерского учета» (далее – Модель угроз) в соответствии с пунктом 1 части 2 статьи 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» определены актуальные угрозы безопасности персональных данных при их обработке в информационной системе персональных данных «Автоматизация бухгалтерского учета» (далее – ИСПДн «Автоматизация бухгалтерского учета»).

Определение актуальных угроз безопасности персональных данных при их обработке в ИСПДн «Автоматизация бухгалтерского учета» проведено администрацией Новомакаровского сельского поселения (далее – Администрация) – оператором ИСПДн «Автоматизация бухгалтерского учета».

Под угрозами безопасности персональных данных понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия при их обработке в ИСПДн «Автоматизация бухгалтерского учета» (нарушение конфиденциальности, целостности и доступности обрабатываемых персональных данных). Для ИСПДн «Автоматизация бухгалтерского учета» целью защиты информации является обеспечение конфиденциальности, целостности и доступности обрабатываемых персональных данных.

В качестве источников угроз безопасности персональных данных могут выступать субъекты (физические лица, организации) или явления (техногенные аварии, стихийные бедствия, иные природные явления). При этом источники угроз могут быть следующих типов:

антропогенные источники (антропогенные угрозы);

техногенные источники (техногенные угрозы);

стихийные источники (угрозы стихийных бедствий, иных природных явлений).

Источниками антропогенных угроз безопасности персональных данных могут выступать:

лица, осуществляющие преднамеренные действия с целью доступа к персональным данным (воздействия на персональные данные), содержащимся в ИСПДн «Автоматизация бухгалтерского учета», или нарушения функционирования ИСПДн «Автоматизация бухгалтерского учета» или обслуживающей ее инфраструктуры (преднамеренные угрозы безопасности персональных данных);

лица, имеющие доступ к ИСПДн «Автоматизация бухгалтерского учета», не преднамеренные действия которых могут привести к нарушению безопасности персональных данных (непреднамеренные угрозы безопасности персональных данных).

Преднамеренные угрозы безопасности персональных данных могут быть реализованы за счет утечки персональных данных по техническим каналам (технические каналы утечки информации, обрабатываемой в технических средствах ИСПДн «Автоматизация бухгалтерского учета», технические каналы перехвата информации при ее передаче по каналам (линиям) связи, технические каналы утечки акустической (речевой) информации) либо за счет несанкционированного доступа.

Настоящая Модель угроз содержит перечень угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн «Автоматизация бухгалтерского учета», которые могут быть реализованы в ИСПДн «Автоматизация бухгалтерского учета», а также содержит совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн «Автоматизация бухгалтерского учета», в которой для обеспечения безопасности персональных данных принято решение применения средств криптографической защиты информации (далее – СКЗИ).

Настоящая Модель угроз разработана с использованием следующих документов:

Федерального закона Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

Постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении [требований](#Par27) к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановления правительства Воронежской области от 26.09.2017 № 748 «Об утверждении документов, определяющих политику в отношении обработки персональных данных в правительстве Воронежской области»;

Постановления правительства Воронежской области от 02.11.2017 № 869 «Об определении угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных правительства Воронежской области, исполнительных органов государственной власти Воронежской области и подведомственных им организаций» (далее – Базовые угрозы);

Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008;

Методики определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 14.02.2008;

Методических рекомендаций по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утвержденных руководством 8-го Центра ФСБ России 31.03.2015 № 149/7/2/6-432.

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн «Автоматизация бухгалтерского учета», определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, оценки уровня исходной защищенности ИСПДн «Автоматизация бухгалтерского учета», анализа возможных способов реализации угроз безопасности персональных данных и последствий от нарушения свойств безопасности персональных данных (конфиденциальности, целостности, доступности).

Источником данных об угрозах безопасности информации, на основе которых определяются угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн «Автоматизация бухгалтерского учета», являются Базовые угрозы. При этом Базовые угрозы подлежат адаптации, которая направлена на уточнение (уменьшение) перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в ИСПДн «Автоматизация бухгалтерского учета», и осуществляется с учетом структурно-функциональных характеристик ИСПДн «Автоматизация бухгалтерского учета», применяемых информационных технологий и особенностей функционирования (в том числе исключение угроз, которые непосредственно связаны с информационными технологиями, не используемыми в ИСПДн «Автоматизация бухгалтерского учета», или структурно-функциональными характеристиками, не свойственными ИСПДн «Автоматизация бухгалтерского учета»).

Угрозы безопасности персональных данных, актуальные при обработке персональных данных в ИСПДн «Автоматизация бухгалтерского учета», подлежат пересмотру (переоценке):

при внесении изменений в Базовые угрозы для типа информационных систем персональных данных, к которому относится ИСПДн «Автоматизация бухгалтерского учета»;

при изменении структурно-функциональных характеристик или особенностей функционирования ИСПДн «Автоматизация бухгалтерского учета», вследствие чего изменился тип, к которому относится ИСПДн «Автоматизация бухгалтерского учета»;

при применении в ИСПДн «Автоматизация бухгалтерского учета» информационных технологий, посредством которых могут формироваться новые угрозы безопасности персональных данных, исключенные из базового (предварительного) перечня угроз безопасности персональных данных для ИСПДн «Автоматизация бухгалтерского учета» в соответствии с положениями раздела 4 настоящей Модели угроз;

при повышении возможности реализации существующих угроз безопасности персональных данных;

в иных случаях по решению Администрации.

**2. Описание информационной системы персональных данных и особенностей ее функционирования**

ИСПДн «Автоматизация бухгалтерского учета» эксплуатируется в целях ведения автоматизированного бухгалтерского учета в Администрации, подготовки отчетности в ПФ РФ по персонифицированному учету и страховым взносам, отправки отчетности посредством глобальной сети Интернет в контролирующие органы в ФНС, ПФР, Росстат, ФСС, УФК.

В ИСПДн «Автоматизация бухгалтерского учета» обрабатываются иные категории персональных данных менее чем 100 000 субъектов персональных данных, которые являются как сотрудниками Администрации, так и иными лицами.

С учетом состава (категории) и объема обрабатываемых персональных данных, а также 3-го типа актуальных угроз безопасности персональных данных, определенного в разделе 4 настоящей Модели угроз, в ИСПДн «Автоматизация бухгалтерского учета» необходимо обеспечение 4-го уровня защищенности персональных данных.

ИСПДн «Автоматизация бухгалтерского учета» представляет собой:

локальную информационную систему персональных данных (комплекс АРМ, объединенных в единую информационную систему в пределах одного здания), имеющую подключение к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к сети «Интернет» (тип 4 в соответствии с пунктом 2.5 Базовых угроз);

Все технические средства ИСПДн «Автоматизация бухгалтерского учета» находятся в пределах Российской Федерации в здании Администрации по адресу: Воронежская область, Грибановский район,

с. Новомакарово, ул. Советская, д. 57. Сервер с базой персональных данных ИСПДн «Автоматизация бухгалтерского учета» располагается в помещении № 1. АРМ ИСПДн «Автоматизация бухгалтерского учета» располагаются в помещениях № 2.

Контролируемая зона здания Администрации установлена по внешнему периметру здания. При входе в здание организовано круглосуточное дежурство.

В пределах контролируемой зоны находятся технические средства, входящие в состав ИСПДн «Автоматизация бухгалтерского учета». Вне контролируемой зоны находятся линии связи, используемые для информационного обмена по сетям связи. Неконтролируемый вынос технических средств ИСПДн за пределы здания Администрации запрещен.

Поскольку ИСПДн «Автоматизация бухгалтерского учета» создана в качестве прикладного сервиса на базе общей инфраструктуры Департамента, используемой для функционирования иных информационных систем, ресурсов и сервисов, четко выраженные физические границы ИСПДн «Автоматизация бухгалтерского учета» отсутствуют. Логические границы ИСПДн «Автоматизация бухгалтерского учета» определяются техническими средствами, а также линиями связи, участвующими в обработке информации в ИСПДн «Автоматизация бухгалтерского учета». Топологическая схема ИСПДн «Автоматизация бухгалтерского учета» приведена в приложении № 1 к настоящей Модели угроз.

Помещения, в которых ведется обработка персональных данных в ИСПДн «Автоматизация бухгалтерского учета» (далее – Помещения), оснащены входными дверьми с замками. Установлен порядок доступа в Помещения, препятствующий возможности неконтролируемого проникновения или пребывания в этих Помещениях лиц, не имеющих права доступа в них. В рабочее время, в случае ухода лиц, имеющих право самостоятельного доступа в Помещение, а также в нерабочее время двери Помещения закрываются на ключ. Доступ посторонних лиц в Помещения допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные Помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным, в том числе через устройства ввода (вывода) информации, а также к носителям персональных данных.

Устройства ввода (вывода) информации из состава ИСПДн «Автоматизация бухгалтерского учета», участвующие в обработке персональных данных, располагаются в Помещениях таким образом, чтобы исключить случайный просмотр обрабатываемой информации посторонними лицами, вошедшими в Помещение, а также через двери и окна Помещения.

Ввод (вывод) персональных данных в ИСПДн «Автоматизация бухгалтерского учета» осуществляется с использованием бумажных и машинных носителей информации, в том числе съемных машинных носителей информации (оптические диски, флеш-накопители, накопители на жестких магнитных дисках, твердотельные накопители и другие) (далее – Машинные носители персональных данных).

 Режим обработки информации в ИСПДн «Автоматизация бухгалтерского учета» многопользовательский с разграничением прав доступа (набора действий, разрешенных для выполнения) пользователей. Управление (администрирование) ИСПДн «Автоматизация бухгалтерского учета», а также обслуживание технических и программных средств ИСПДн «Автоматизация бухгалтерского учета», средств защиты информации, в том числе СКЗИ и среды их функционирования, включая настройку, конфигурирование и распределение носителей ключевой информации между пользователями ИСПДн «Автоматизация бухгалтерского учета», осуществляется сотрудниками Администрации.

Сотрудники, участвующие в управлении (администрировании) ИСПДн «Автоматизация бухгалтерского учета» и ее системой защиты информации, а также обслуживающие технические и программных средств ИСПДн «Автоматизация бухгалтерского учета» являются привилегированными пользователями (ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных), которые назначаются из числа доверенных лиц. Главой Администрации назначен сотрудник, ответственный за обеспечение безопасности персональных данных в информационных системах персональных данных Администрации.

В целях обеспечения информационного взаимодействия сервер и АРМ из состава ИСПДн «Автоматизация бухгалтерского учета», имеют подключение к вычислительной сети Администрации. Для организации сетевого взаимодействия в ИСПДн «Автоматизация бухгалтерского учета» используется набор (стек) протоколов TCP/IP.

Для ключевых элементов ИСПДн «Автоматизация бухгалтерского учета» предусмотрены источники резервного электропитания. В помещении с сервером ИСПДн «Автоматизация бухгалтерского учета» имеются системы вентиляции.

Обеспечение антивирусного контроля в ИСПДн «Автоматизация бухгалтерского учета» осуществляется в соответствии с установленным порядком с применением сертифицированного средства антивирусной защиты «Kaspersy Endpoint Security 11». Антивирусное средство автоматически запускается после загрузки операционной системы на сервере или АРМ при этом антивирусный контроль осуществляется в постоянном режиме без участия пользователей ИСПДн «Автоматизация бухгалтерского учета». Обновление баз сигнатур вирусов осуществляется в автоматическом режиме.

ИСПДн «Автоматизация бухгалтерского учета» сегментирована на типовые сегменты, реализующие полную технологию обработки информации (обозначение сегментов ИСПДн «Автоматизация бухгалтерского учета» приведено в приложении № 1 к настоящей Модели угроз).

К объектам защиты в ИСПДн «Автоматизация бухгалтерского учета» относятся:

обрабатываемые персональные данные;

технические средства (в том числе средства вычислительной техники, Машинные носители персональных данных, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической и видеоинформации);

средства защиты информации, в том числе СКЗИ;

среда функционирования средств защиты информации, в том числе СКЗИ;

информация, относящаяся к защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию;

носители ключевой, парольной и аутентифицирующей информации;

документы, в которых отражена информация о мерах и средствах защиты ИСПДн «Автоматизация бухгалтерского учета»;

Помещения.

В ИСПДн «Автоматизация бухгалтерского учета» возможно наличие и (или) появление новых уязвимостей в используемом микропрограммном, общесистемном, прикладном программном обеспечении, а также в применяемых протоколах передачи данных.

ИСПДн «Автоматизация бухгалтерского учета» с учетом структурно-функциональных характеристик и условий эксплуатации, а также применяемых информационных технологий и предпринятых мер обеспечения безопасности персональных данных, приведенных в настоящем разделе, имеет средний уровень исходной защищенности.

**3.** **Возможности нарушителей по реализации угроз**

**безопасности персональных данных**

Оценка возможностей нарушителей по реализации угроз безопасности персональных данных в ИСПДн «Автоматизация бухгалтерского учета» проведена с учетом положений раздела 3 Базовых угроз.

Нарушителем является физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке в ИСПДн «Автоматизация бухгалтерского учета».

В зависимости от права разового или постоянного доступа в контролируемую зону и возможностей по доступу к обрабатываемым персональным данным и (или) к компонентам ИСПДн «Автоматизация бухгалтерского учета» рассматриваются нарушители двух типов:

внешние нарушители – лица, не имеющие права доступа к ИСПДн «Автоматизация бухгалтерского учета» или ее отдельным компонентам;

внутренние нарушители – лица, имеющие право постоянного или разового доступа к ИСПДн «Автоматизация бухгалтерского учета» или ее отдельным компонентам.

С учетом состава (категории) и объема обрабатываемых персональных данных в ИСПДн «Автоматизация бухгалтерского учета», а также целей и задач их обработки в качестве возможных целей (мотивации) реализации нарушителями угроз безопасности персональных данных в ИСПДн «Автоматизация бухгалтерского учета» могут быть:

получение выгоды путем мошенничества или иным преступным путем;

любопытство или желание самореализации;

реализация угроз безопасности персональных данных из мести;

реализация угроз безопасности персональных данных непреднамеренно из-за неосторожности или неквалифицированных действий.

Для ИСПДн «Автоматизация бухгалтерского учета», относящейся к типу 4 с заданными структурно-функциональными характеристиками и особенностями функционирования (осуществляется разграничение прав доступа пользователей), а также с учетом сделанных предположений (прогноза) о возможных целях (мотивации) реализации угроз безопасности персональных данных рассматриваются следующие виды нарушителей:

преступные группы (криминальные структуры) – внешние нарушители;

внешние субъекты (физические лица) – внешние нарушители;

лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ, – внутренние нарушители;

лица, обслуживающие инфраструктуру Администрации (охрана, уборщики и т.д.), – внутренние нарушители;

пользователи ИСПДн «Автоматизация бухгалтерского учета» – внутренние нарушители;

бывшие сотрудники (пользователи) – внешние нарушители.

Нарушители обладают следующими возможностями по реализации угроз безопасности персональных данных в ИСПДн «Автоматизация бухгалтерского учета»:

получать информацию об уязвимостях отдельных компонентов ИСПДн «Автоматизация бухгалтерского учета», опубликованную в общедоступных источниках;

получать информацию о методах и средствах реализации угроз безопасности персональных данных (компьютерных атак), опубликованных в общедоступных источниках;

самостоятельно осуществлять создание способов атак, подготовку и проведение атак на ИСПДн «Автоматизация бухгалтерского учета» только за пределами контролируемой зоны;

самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом и без физического доступа к ИСПДн «Автоматизация бухгалтерского учета» или ее отдельным компонентам, на которых реализованы меры и средства защиты информации, в том числе СКЗИ и среда их функционирования.

С учетом имеющейся совокупности предположений о целях (мотивации) и возможностях нарушителей по реализации угроз безопасности персональных данных в ИСПДн «Автоматизация бухгалтерского учета» потенциал нападения при реализации угроз безопасности персональных данных для рассматриваемых видов нарушителей будет базовый (низкий). Нарушитель с базовым (низким) потенциалом является непрофессионалом, использует стандартное оборудование, имеет ограниченные знания об ИСПДн «Автоматизация бухгалтерского учета» или совсем их не имеет, возможность доступа к ИСПДн «Автоматизация бухгалтерского учета» или ее отдельным компонентам ограничена и контролируется организационными мерами и средствами ИСПДн «Автоматизация бухгалтерского учета».

В ИСПДн «Автоматизация бухгалтерского учета» угрозы безопасности персональных данных могут быть реализованы внешними и внутренними нарушителями с базовым (низким) потенциалом следующими способами:

несанкционированный доступ и (или) воздействие на объекты защиты на аппаратном уровне (программы (микропрограммы), «прошитые» в аппаратных компонентах (чипсетах));

несанкционированный доступ и (или) воздействие на объекты защиты на общесистемном уровне (операционные системы);

несанкционированный доступ и (или) воздействие на объекты защиты на прикладном уровне (система управления базами данных, браузеры, иное прикладное программное обеспечение общего назначения);

несанкционированный доступ и (или) воздействие на объекты защиты на сетевом уровне (сетевые приложения, сервисы);

несанкционированный физический доступ и (или) воздействие на объекты защиты (каналы (линии) связи, технические средства, носители информации).

**4**. **Актуальные угрозы безопасности персональных данных**

Определение угроз безопасности персональных данных, актуальных для ИСПДн «Автоматизация бухгалтерского учета», проведено с учетом положений раздела 4 Базовых угроз.

Угрозы безопасности персональных данных являются актуальными для ИСПДн «Автоматизация бухгалтерского учета», если существует вероятность их реализации нарушителем с базовым (низким) потенциалом и такая реализация приведет к неприемлемым негативным последствиям (ущербу) от нарушения конфиденциальности, целостности или доступности обрабатываемых персональных данных.

С учетом среднего уровня исходной защищенности ИСПДн «Автоматизация бухгалтерского учета», состава (категории) и объема обрабатываемых в ИСПДн «Автоматизация бухгалтерского учета» персональных данных, а также особенностей их обработки для ИСПДн «Автоматизация бухгалтерского учета» актуальны угрозы безопасности персональных данных 3-го типа. Угрозы безопасности персональных данных 3-го типа не связаны с наличием недокументированных (недекларированных) возможностей в используемом в ИСПДн «Автоматизация бухгалтерского учета» общесистемном и прикладном программном обеспечении.

Принимая во внимание природно-климатические условия, характерные для Воронежской области в силу ее территориального положения, а также предпринятые меры обеспечения безопасности персональных данных, приведенные в разделе 2 настоящей Модели угроз, для ИСПДн «Автоматизация бухгалтерского учета» техногенные угрозы, а также угрозы стихийных бедствий и иных природных явлений неактуальны и далее будут рассматриваться только антропогенные (преднамеренные, непреднамеренные) угрозы безопасности персональных данных.

С учетом особенностей функционирования, используемых структурно-функциональных характеристик, применяемых информационных технологий, характера и способов обработки персональных данных и предпринятых мер обеспечения безопасности персональных данных, приведенных в разделе 2 настоящей Модели угроз, а также возможных негативных последствий (ущерба) от реализации преднамеренные угрозы утечки персональных данных по техническим каналам для ИСПДн «Автоматизация бухгалтерского учета» неактуальны и далее из преднамеренных угроз безопасности персональных данных будут рассматриваться только угрозы, реализуемые за счет несанкционированного доступа.

В качестве базового (предварительного) перечня угроз безопасности персональных данных для ИСПДн «Автоматизация бухгалтерского учета» рассматриваются угрозы, определенные актуальными в приложении № 1 к Базовым угрозам. При этом из базового (предварительного) перечня угроз безопасности персональных данных исключаются угрозы безопасности информации (УБИ.006, УБИ.018, УБИ.019, УБИ.030, УБИ.031, УБИ.062, УБИ.071, УБИ.074, УБИ.083, УБИ.090, УБИ.125, УБИ.126, УБИ.128, УБИ.174, УБИ.191), необходимые информационные технологии или структурно-функциональные характеристики, для формирования которых в ИСПДн «Автоматизация бухгалтерского учета» не применяются (не используются) в соответствии с разделом 2 настоящей Модели угроз. Базовый (предварительный) перечень рассматриваемых угроз безопасности персональных данных для ИСПДн «Автоматизация бухгалтерского учета» приведен в приложении № 2 к настоящей Модели угроз.

Оценка актуальности угроз безопасности персональных данных из базового (предварительного) перечня для ИСПДн «Автоматизация бухгалтерского учета» осуществляется с учетом применяемых в ИСПДн «Автоматизация бухгалтерского учета» информационных технологий, необходимых для формирования соответствующих угроз, вероятности (частоты) их реализации, возможности реализации и опасности.

Вероятность (частота) реализации угроз безопасности персональных данных определяется экспертным путем и характеризуется вероятностью их реализации для ИСПДн «Автоматизация бухгалтерского учета» с учетом реальных условий эксплуатации.

С учетом базового (низкого) потенциала возможных нарушителей и среднего уровня исходной защищенности ИСПДн «Автоматизация бухгалтерского учета» вероятность (частота) реализации угроз безопасности персональных данных для ИСПДн «Автоматизация бухгалтерского учета» оценивается не выше средней. Объективные предпосылки для реализации угроз безопасности персональных данных существуют, но принятые меры обеспечения безопасности персональных данных в ИСПДн «Автоматизация бухгалтерского учета» недостаточны.

Экспертная оценка вероятности (частоты) реализации угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн «Автоматизация бухгалтерского учета», проведена с учетом максимальных значений вероятности (частоты) реализации соответствующих угроз, указанных в приложении № 1 к Базовым угрозам, и приведена в приложении № 2 к настоящей Модели угроз.

Опасность угроз безопасности персональных данных определяется экспертным путем и характеризуется возможными негативными последствиями от их реализации для Администрации и субъектов персональных данных.

С учетом состава (категории) и объема обрабатываемых в ИСПДн «Автоматизация бухгалтерского учета» персональных данных, а также необходимости обеспечения 4-го уровня защищенности персональных данных при их обработке в ИСПДн «Автоматизация бухгалтерского учета» опасность угроз безопасности персональных данных для ИСПДн «Автоматизация бухгалтерского учета» оценивается не выше средней. В результате нарушения одного из свойств безопасности персональных данных (конфиденциальность, целостность, доступность) возможны умеренные негативные последствия для Администрации и субъектов персональных данных.

Оценка опасности угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн «Автоматизация бухгалтерского учета», получена из Базовых угроз и приведена в приложении № 2 к настоящей Модели угроз.

Оценка возможности реализации и актуальности угроз безопасности персональных данных, включенных в базовый (предварительный) перечень для ИСПДн «Автоматизация бухгалтерского учета», проведена с учетом максимальных значений возможности реализации и актуальности соответствующих угроз, указанных в приложении № 1 к Базовым угрозам, и приведена в приложении № 2 к настоящей Модели угроз.

Перечень актуальных угроз безопасности персональных данных при их обработке в ИСПДн «Автоматизация бухгалтерского учета», приведенный в приложении № 2 к настоящей Модели угроз, является идентичным для всех сегментов ИСПДн «Автоматизация бухгалтерского учета».

Совокупность предположений о возможностях, которые могут использоваться при создании способов, подготовке и проведении атак для ИСПДн «Автоматизация бухгалтерского учета» получена из Базовых угроз и приведена в приложении № 3 к настоящей Модели угроз.

Для нейтрализации атак, при создании способов, подготовке и проведении которых используются признанные актуальными для ИСПДн «Автоматизация бухгалтерского учета» возможности, указанные в приложении № 3 к настоящей Модели угроз, в соответствии с пунктом 11 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утвержденных приказом ФСБ России от 10.07.2014 № 378 в ИСПДн «Автоматизация бухгалтерского учета» необходимо применение СКЗИ класса не ниже КС2.

Приложение № 1

к модели угроз безопасности персональных данных

при их обработке в информационной системе

персональных данных «Автоматизация бухгалтерского учета»

**

Топологическая схема информационной системы персональных данных *«Автоматизация бухгалтерского учета»* с обозначением ее составных частей и сегментов

Приложение № 2

к модели угроз безопасности персональных данных

при их обработке в информационной системе

персональных данных «Автоматизация бухгалтерского учета»

Перечень актуальных угроз безопасности персональных данных при их

обработке в информационной системе персональных данных *«Автоматизация бухгалтерского учета»*

| №п/п | Идентификатор угрозы из Банка данных угроз | Наименование угрозы | Актуальность использования (применения) для построения и реализации атак | Примечание |
| --- | --- | --- | --- | --- |
|  | *УБИ.006* | *Угроза внедрения кода или данных* | *Не актуально* | *Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.008* | *Угроза восстановления аутентификационной информации* | *Актуально* | *Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.015* | *Угроза доступа к защищаемым файлам с использованием обходного пути* | *Актуально* | *Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.018* | *Угроза загрузки нештатной операционной системы* | *Не актуально* | *Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.019* | *Угроза заражения DNS-кеша* | *Не актуально* | *Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.028* | *Угроза использования альтернативных путей доступа к ресурсам* | *Актуально* | *Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.030* | *Угроза использования информации идентификации/аутентификации, заданной по умолчанию* | *Не актуально* | *Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | *УБИ.031* | *Угроза использования механизмов авторизации для повышения привилегий* | *Не актуально* | *Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы* |
|  | УБИ.034 | Угроза использования слабостей протоколов сетевого/локального обмена данными | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.041 | Угроза межсайтового скриптинга | Актуально | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.062 | Угроза некорректного использования прозрачного прокси-сервера за счет плагинов браузера | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.067 | Угроза неправомерного ознакомления с защищаемой информацией | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.069 | Угроза неправомерных действий в каналах связи | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.071 | Угроза несанкционированного восстановления удаленной защищаемой информации | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.074 | Угроза несанкционированного доступа к аутентификационной информации | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.083 | Угроза несанкционированного доступа к системе по беспроводным каналам | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.084 | Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети | *Не актуально* | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.088 | Угроза несанкционированного копирования защищаемой информации | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.089 | Угроза несанкционированного редактирования реестра | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.090 | Угроза несанкционированного создания учетной записи пользователя | *Не актуально* | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.098 | Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.099 | Угроза обнаружения хостов | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.116 | Угроза перехвата данных, передаваемых по вычислительной сети | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.125 | Угроза подключения к беспроводной сети в обход процедуры аутентификации | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.126 | Угроза подмены беспроводного клиента или точки доступа | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.128 | Угроза подмены доверенного пользователя | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.156 | Угроза утраты носителей информации | Актуально | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность |
|  | УБИ.159 | Угроза «форсированного веб-браузинга» | Актуально | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.167 | Угроза заражения компьютера при посещении неблагонадежных сайтов | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.168 | Угроза «кражи» учетной записи доступа к сетевым сервисам | Актуально | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.172 | Угроза распространения «почтовых червей» | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.174 | Угроза «фарминга» | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.175 | Угроза «фишинга» | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.178 | Угроза несанкционированного использования системных и сетевых утилит | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.191 | Угроза внедрения вредоносного кода в дистрибутив программного обеспечения | *Не актуально* | Низкая вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |
|  | УБИ.192 | Угроза использования уязвимых версий программного обеспечения | Актуально | Средняя вероятность реализации угрозы. Средняя возможность реализации угрозы. Средняя опасность угрозы |

Приложение № 3

к модели угроз безопасности персональных данных

при их обработке в информационной системе

персональных данных «Автоматизация бухгалтерского учета»

Совокупность предположений о возможностях, которые могут использоваться при создании способов,

подготовке и проведении атак для информационной системы персональных данных *«Автоматизация бухгалтерского учета»*

| №п/п | Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы) | Актуальность использования (применения) для построения и реализации атак | Обоснование отсутствия |
| --- | --- | --- | --- |
| 1.1. | Проведение атаки при нахождении в пределах контролируемой зоны | Актуально |  |
| 1.2. | Проведение атак на этапе эксплуатации СКЗИ на следующие объекты:документацию на СКЗИ и компоненты среды функционирования;помещения, в которых находятся компоненты ИСПДн *«Автоматизация бухгалтерского учета»*, на которых реализованы СКЗИ и среда функционирования | Неактуально | Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн *«Автоматизация бухгалтерского учета»* назначаются из числа доверенных лиц.Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн *«Автоматизация бухгалтерского учета»*. Указанные помещения оснащены входными дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн *«Автоматизация бухгалтерского учета»* допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты.Установлен порядок, обеспечивающий сохранность документации на СКЗИ, машинных носителей информации с комплектами восстановления СКЗИ, носителей ключевой, парольной и аутентифицирующей информации. Документация на СКЗИ и указанные носители хранятся только в сейфах или закрываемых на ключ шкафах (ящиках) в условиях, препятствующих свободному доступу к ним посторонних лиц |
| 1.3. | Получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:сведений о физических мерах защиты объектов, в которых размещены ресурсы ИСПДн *«Автоматизация бухгалтерского учета»*;сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы ИСПДн *«Автоматизация бухгалтерского учета»*;сведений о мерах по разграничению доступа в помещения, в которых находятся компоненты ИСПДн *«Автоматизация бухгалтерского учета»*, на которых реализованы СКЗИ и среда функционирования | Актуально |  |
| 1.4. | Использование штатных средств ИСПДн *«Автоматизация бухгалтерского учета»*, в которой используется СКЗИ, ограниченное реализованными в ИСПДн *«Автоматизация бухгалтерского учета»* мерами, направленными на предотвращение и пресечение несанкционированных действий | Актуально |  |
| 2.1. | Физический доступ к компонентам ИСПДн *«Автоматизация бухгалтерского учета»*, на которых реализованы СКЗИ и среда функционирования | Неактуально | Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн *«Автоматизация бухгалтерского учета»* назначаются из числа доверенных лиц.Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн *«Автоматизация бухгалтерского учета»*. Указанные помещения оснащены входными дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн *«Автоматизация бухгалтерского учета»* допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты |
| 2.2. | Возможность располагать или воздействовать на аппаратные компоненты СКЗИ и среду функционирования, ограниченная мерами, реализованными в ИСПДн *«Автоматизация бухгалтерского учета»*, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий | Неактуально | Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы.Проводятся работы по подбору сотрудников, привилегированные пользователи ИСПДн *«Автоматизация бухгалтерского учета»* назначаются из числа доверенных лиц.Обеспечивается контролируемый доступ (контролируемая зона) в административные здания и (или) помещения с компонентами ИСПДн *«Автоматизация бухгалтерского учета»*. Указанные помещения оснащены входными дверьми с замками, установлен порядок доступа в эти помещения, препятствующий возможности неконтролируемого проникновения или пребывания лиц, не имеющих права доступа в них. В рабочее время в случае ухода лиц, имеющих право самостоятельного доступа в указанные помещения, а также в нерабочее время двери этих помещений закрываются на ключ. Доступ посторонних лиц в помещения с компонентами ИСПДн *«Автоматизация бухгалтерского учета»* допускается только в присутствии лиц, имеющих право самостоятельного доступа в данные помещения на время, ограниченное служебной необходимостью. При этом предпринимаются меры, исключающие возможность доступа посторонних лиц к обрабатываемым персональным данным и другим объектам защиты.Осуществляется разграничение, регистрация и учет доступа пользователей ИСПДн *«Автоматизация бухгалтерского учета»* к объектам защиты с использованием организационных мер и средств ИСПДн *«Автоматизация бухгалтерского учета»*. Правами управления (администрирования) ИСПДн *«Автоматизация бухгалтерского учета»* обладают только привилегированные пользователи |
| 3.1. | Создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих функционирование СКЗИ и среды функционирования, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного программного обеспечения | Неактуально | Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности.Высокая стоимость и сложность подготовки реализации возможности.Для ИСПДн *«Автоматизация бухгалтерского учета»* актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом общесистемном и прикладном программном обеспечении |
| 3.2. | Проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализованными в ИСПДн *«Автоматизация бухгалтерского учета»*, в которой используется СКЗИ, направленными на предотвращение и пресечение несанкционированных действий | Неактуально | Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности.Высокая стоимость и сложность подготовки реализации возможности |
| 3.3. | Проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и среду функционирования, в том числе с использованием исходных текстов входящего в среды функционирования прикладного программного обеспечения, непосредственно использующего вызовы программных функций СКЗИ | Неактуально | Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности.Высокая стоимость и сложность подготовки реализации возможности |
| 4.1. | Создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей общесистемного программного обеспечения | Неактуально | Не осуществляется обработка сведений, которые могут представлять интерес для реализации возможности.Высокая стоимость и сложность подготовки реализации возможности.Для ИСПДн *«Автоматизация бухгалтерского учета»* актуальны угрозы безопасности персональных данных третьего типа, не связанные с наличием недокументированных (недекларированных) возможностей в используемом общесистемном и прикладном программном обеспечении |
| 4.2. | Возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты среды функционирования СКЗИ | Неактуально | Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности.Отсутствует в наличии конструкторская документация на аппаратные и программные компоненты среды функционирования СКЗИ |
| 4.3. | Возможность располагать или воздействовать на любые компоненты СКЗИ и среды функционирования | Неактуально | Не осуществляется обработка сведений, которые могут представлять интерес (мотивацию) для реализации возможности.Базового (низкого) потенциала нарушителя недостаточно для реализации угрозы |