УТВЕРЖДЕНА
приказом {Название Организации}
от «___» _____20__г. № ___

Политика информационной безопасности в {Название Организации}

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - Политика) утверждается руководителем {Название Организации} и определяет мероприятия, процедуры и правила по защите информации в информационных системах {Название Организации}.

1.2. Положения настоящей Политики распространяются на следующие информационные системы {Название Организации}:

- ГИС «ИС»;
- ИСПДн «Бухгалтерия и кадры»;
- ИС «Делопроизводство».

1.3. Положения настоящей Политики обязательны к исполнению для всех пользователей указанных в п. 1.2 информационных систем (далее - Пользователи), а также для администраторов безопасности и системных администраторов (далее - Администраторы).

1.4. В соответствии с указом Президента Российской Федерации № 188 от 6 марта 1997 года к сведениям конфиденциального характера (защищаемой информации) в {Название Организации} относятся:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее) {оставить нужное};
- служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна) {только для госов};
- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

1.5. Целями настоящей Политики являются:

- обеспечение конфиденциальности, целостности, доступности защищаемой информации;
- предотвращение утечек защищаемой информации;

- мониторинг событий безопасности и реагирование на инциденты безопасности;
- нейтрализация актуальных угроз безопасности информации;
- выполнение требований действующего законодательства по защите информации.

1.6. В настоящей Политике используются термины и определения, установленные законодательством Российской Федерации об информации, информационных технологиях и о защите информации, а также термины и определения, установленные национальными стандартами в области защиты информации.

1.7. Настоящая Политика разработана с учетом положений следующих законодательных и нормативно-правовых актов:

- Федеральный закон № 149-ФЗ от 27 июля 2006 года «Об информации, информатизации и защите информации»;
- Федеральный закон № 152-ФЗ от 27 июля 2006 года «О персональных данных»;
- «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утвержденные Постановлением Правительства РФ № 1119 от 1 ноября 2012 года;
- «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», утвержденные приказом ФСТЭК России № 17 от 11 февраля 2013 года;
- «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденный приказом ФСТЭК России № 21 от 18 февраля 2013 года;
- методический документ «Меры защиты информации в государственных информационных системах», утвержденный ФСТЭК России 11 февраля 2014 года;
- «Состав и содержание 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», утверждённые приказом ФСБ России № 378 от 10.07.2014;
- «Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», утвержденное приказом ФСБ от 9 февраля 2005 №66;
- «Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом ФАПСИ от 13 июня 2001 №152.

2. ТЕХНОЛОГИЧЕСКИЕ ПРОЦЕССЫ ОБРАБОТКИ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

2.1. В данном разделе настоящей Политики описаны технологические процессы обработки различных видов защищаемой информации в информационных системах {Название Организации}. Администраторы и Пользователи,

допущенные к обработке той или иной защищаемой информации, обязаны производить обработку этой информации в соответствии с соответствующими описаниями технологических процессов обработки информации, приведенных в данном разделе.

2.2. Технологический процесс обработки персональных данных сотрудников {Название Организации}:

{описать техпроцесс}

2.3. Технологический процесс обработки персональных данных соискателей на вакантные должности в {Название Организации}:

{описать техпроцесс}

2.4. Технологический процесс обработки персональных данных клиентов на вакантные должности в {Название Организации}:

{описать техпроцесс}

3. ПРАВИЛА И ПРОЦЕДУРЫ ИДЕНТИФИКАЦИИ И АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ ГИС, ПОЛИТИКА РАЗГРАНИЧЕНИЯ ДОСТУПА К РЕСУРСАМ ГИС

3.1. С целью соблюдения принципа персональной ответственности за свои действия каждому сотруднику {Название Организации}, допущенному к работе с ресурсами ГИС «Бухгалтерия и кадры» присваивается уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать в ГИС.

3.2. Под учетной записью Пользователя понимается учетная запись для доступа к информационной системе в домене Active Directory. Если применяется дополнительное разграничение доступа, например в 1С, дописать это.

3.3. Использование одного и того же имени пользователя несколькими пользователями (или группового имени для нескольких пользователей) в ГИС запрещено.

3.4. Для администратора безопасности ГИС, для системных администраторов ГИС, для удаленных пользователей (пользователей работающих с ресурсами ГИС через внешние телекоммуникационные сети, но являющихся сотрудниками {Название Организации}), для внешних пользователей ГИС (пользователей, не являющихся сотрудниками ГИС) предусмотрена двухфакторная аутентификация в ГИС. (для ГИС К1: Для всех пользователей ГИС (в том числе для внешних пользователей и удаленных пользователей) предусмотрена двухфакторная аутентификация) Двухфакторная аутентификация подразумевает под собой обязательное выполнение двух факторов: предъявление физического электронного ключа eToken PRO Java 72K (JaCarta, RuToken и тд), и ввод пароля (пин-кода) доступа к памяти электронного ключа. Электронные ключи и пароли доступа выдаются Администратором в соответствии с теми же требованиями и правилами, установленными для выдачи учетных записей и паролей к ним в данном разделе настоящей Политики. Идентификация электронного ключа и считывание аутентификационной информации с него осуществляется с помощью механизмов средства защиты информации от несанкционированного доступа (далее - СЗИ от НСД) {Название СЗИ от НСД}.

3.5. Процедура регистрации (создания учетной записи и выдачи при необходимости электронного ключа) пользователя ГИС для сотрудника {Название Организации}, и предоставления ему (или изменения его) прав доступа к ресурсам ГИС инициируется заявкой руководителя подразделения, в котором работает этот сотрудник. Форма заявки приведена в Приложении № 1 к настоящей Политике. В заявке указывается:

- содержание запрашиваемых изменений (регистрация нового пользователя ГИС, удаление учетной записи пользователя, расширение или сужение полномочий и прав доступа к ресурсам ГИС ранее зарегистрированного пользователя);
- должность (с полным наименованием подразделения), фамилия, имя и отчество сотрудника;
- полномочия, которых необходимо лишить пользователя или которые необходимо добавить пользователю (путем указания решаемых пользователем задач в ГИС);
- заявку визирует администратор безопасности, утверждая тем самым возможность допуска (изменения прав доступа) данного сотрудника к необходимым для решения им указанных задач ресурсам ГИС.

3.6. Администратор перед визированием заявки осуществляет верификацию пользователя (подтверждает его личность), а также уточняет его должностные и функциональные обязанности и сопоставляет их с технологическими процессами обработки информации, описанным в разделе 2 настоящей Политики. Допуск Пользователей к обработке информации в ГИС производится на основании завизированной Администратором заявки, составленной по форме, приведенной в Приложении № 1 к настоящей Политике. При визировании очередной заявки Администратор осуществляет актуализацию следующих документов:

- положение о разграничении прав доступа в ГИС (при необходимости, Приложение № 2 к настоящей Политике);
- Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС «Бухгалтерия и кадры» (Приложение № 3 к настоящей Политике).

3.7. После визирования заявки Администратор определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная, учетная запись приложения, временная, гостевая) и производит необходимые настройки СЗИ от НСД и формирует учетную запись, персональный идентификатор и первичный пароль. Дает ознакомиться с инструкцией Пользователя ГИС под роспись, сообщает пользователю идентификационные данные и допускает к работе в ГИС. После допуска к работе в ГИС, Пользователь самостоятельно формирует пароль доступа к своей учетной записи в соответствии с требованиями раздела 3 Инструкции Пользователя ГИС.

3.8. {К1} В ГИС «Бухгалтерия и кадры» для учетных записей Пользователей, процессов, приложений, гостевых и временных учетных записей разрешен только один параллельный сеанс доступа к ресурсам ГИС. Для привилегированных учетных записей (администратор безопасности и системные администраторы) разрешено не более двух параллельных сеансов доступа к ресурсам ГИС с разных устройств. Настройка разрешения параллельных сеансов доступа к ресурсам ГИС осуществляется Администратором путем указания соответствующих параметров в {Название СЗИ от НСД}. Контроль и отображение числа активных одновременных

(параллельных) сеансов доступа для каждой учетной записи осуществляется во вкладке «Сессии» сервера безопасности Dallas Lock 8.0-K.

3.9. По окончании внесения изменений в списки пользователей в заявке делается отметка о выполнении задания. Исполненная заявка хранится у Администратора и может быть использована для восстановления полномочий пользователей после сбоев в работе ГИС, а также для контроля правомерности наличия у конкретного пользователя прав доступа к тем или иным ресурсам ГИС при разборе инцидентов безопасности.

3.10. Для проведения временных работ в ГИС сотрудниками сторонних организаций предусмотрена гостевая временная учетная запись «Guest». Данная учетная запись отключена и активируется (наделяется необходимыми полномочиями) только при необходимости. Все работы от имени такой учетной записи проводятся только под контролем Администратора.

3.11. В качестве модели разграничения доступа к ресурсам ГИС выбрана ролевая модель. Пользователям назначается роль в разграничительной системе ГИС в зависимости от выполняемых должностных обязанностей и задач и, соответственно, в зависимости от необходимости по доступу к тем или иным ресурсам ГИС. Обязанности и задачи пользователей определяются исходя из технологических процессов обработки информации, описанных в разделе 2 настоящей Политики. Описание всех возможных ролей в ГИС приведено в Приложении № 2 к настоящей Политике. Помимо учетных записей Пользователей доступ к системе получают различные системные службы и процессы.

3.12. Перечень лиц, их должностей, а также служб и процессов, допущенных к работе с ресурсами ГИС и сопоставляемые им роли приведены в Приложении № 3 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.13. Перечень помещений, в которых разрешена работа с ресурсами ГИС, расположены технические средства ГИС, а также перечень лиц, допущенных в эти помещения приведен в Приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня.

3.14. {К2+} Перечень устройств (стационарных, мобильных, портативных), используемых в ГИС приведен в приложении № 4 к настоящей Политике. Администратор обеспечивает оперативное обновление и актуальность данного перечня. Идентификация и аутентификация устройств в ГИС осуществляется по совокупности имени или ID устройства, IP-адреса {убрать, если динамика} и MAC-адреса. Идентификация и аутентификация устройств осуществляется с помощью механизмов СЗИ от НСД {Название СЗИ от НСД}. В случае выявления посторонних устройств, Администратор оперативно блокирует доступ неустановленного устройства к ГИС и созывает ГРИИБ, которая в свою очередь устанавливает причины и последствия такого инцидента.

3.15. Идентификация и аутентификация на сетевом оборудовании (коммутаторы, маршрутизаторы, точки доступа и т. д.) разрешена только администраторам безопасности, системным администраторам и сотрудникам сторонней организации, производящим работы в сети {Название Организации} на договорной основе под контролем Администратора. При вводе в эксплуатацию сетевого оборудования на нем обязательно меняются идентификационные и аутентификационные данные, установленные производителем устройства по

умолчанию. Новые идентификационные данные на сетевых устройствах должны соответствовать установленной парольной политике.

3.16. Пользователям запрещены любые действия в ГИС до прохождения процедуры идентификации и аутентификации в системе. Администратору разрешается ряд действий до прохождения идентификации и аутентификации в ГИС в ряде случаев. Условия, при которых разрешаются такие действия и перечень разрешенных действий для Администратора до прохождения процедуры идентификации и аутентификации в ГИС перечислены в пункте 5.9 инструкции Администратора.

4. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ ПОТОКАМИ

4.1. {Описать}

5. ПРАВИЛА И ПРОЦЕДУРЫ УПРАВЛЕНИЯ УСТАНОВКОЙ (ИНСТАЛЯЦИЕЙ) КОМПОНЕНТОВ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

5.1. В ГИС «Бухгалтерия и кадры» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

5.2. Перечень разрешенного программного обеспечения в ГИС «Бухгалтерия и кадры» определен в Приложении № 7 к настоящей Политике.

5.3. Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС «Бухгалтерия и кадры».

5.4. Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

5.5. Администратор ежемесячно с помощью инструмента XSpider 7.8.24 проводит проверку соответствия состава программного обеспечения в ГИС «Бухгалтерия и кадры» списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

5.6. {К1} На серверной части ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

5.7. {К1} На АРМ Пользователей ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

5.8. {К1} На АРМ Администратора ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

6. ЗАЩИТА МАШИННЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ, КОНТРОЛЬ ИНТЕРФЕЙСОВ ВВОДА-ВЫВОДА, ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ ИНФОРМАЦИИ

6.1. {Описать}

7. РЕГЛАМЕНТАЦИЯ И КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ БЕСПРОВОДНОГО ДОСТУПА И ЗАЩИТА БЕСПРОВОДНЫХ СОЕДИНЕНИЙ {Удалить раздел, если нет беспроводных соединений}

7.1. {Описать}

8. УПРАВЛЕНИЕ ВЗАИМОДЕЙСТВИЕМ С ИНФОРМАЦИОННЫМИ СИСТЕМАМИ СТОРОННИХ ОРГАНИЗАЦИЙ (ВНЕШНИМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ) {Удалить раздел, если нет такого взаимодействия}

8.1. {Описать}

9. ПРАВИЛА И ПРОЦЕДУРЫ ОБЕСПЕЧЕНИЯ ДОВЕРЕННОЙ ЗАГРУЗКИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНО ТЕХНИКИ {К2+}

9.1. В {Название Организации} в качестве средства доверенной загрузки технических средств применяется {Название МДЗ}. {Убрать, если применяются компенсирующие меры}

9.2. Для работы с ресурсами ГИС «Бухгалтерия и кадры» выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).

9.3. Администратор контролирует работоспособность {Название МДЗ} в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяются компенсирующие меры}

9.4. В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из ГИС на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры {Убрать, если применяются компенсирующие меры}:

- опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
- устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
- устанавливается усиленный визуальный контроль за техническим средством.

9.5. В проектной документации на систему защиты информации в ГИС «Бухгалтерия и кадры» обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств ГИС. {Убрать, если применяется МДЗ}

9.6. В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств. Данная мера обеспечивает контроль доступа злоумышленника к интерфейсам ввода-вывода, позволяющим осуществить недоверенную загрузку. {Убрать, если применяется МДЗ}

9.7. В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется установка пароля администратора на вход в BIOS/UEFI и отключение возможности вызова источника загрузки во время загрузки технического средства. Данная мера позволяет блокировать на программном уровне изменение источника загрузки при срыве пломбы с интерфейса ввода-вывода. {Убрать, если применяется МДЗ}

9.8. В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется усиленный визуальный контроль за техническими средствами ГИС. Данная мера позволяет своевременно детектировать факты нарушения пломб технического средства, выявлять факты несанкционированного доступа и принимать меры реагирования. {Убрать, если применяется МДЗ}

9.9. Администратор контролирует выполнение компенсирующих мер в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяется МДЗ}

10. ПРАВИЛА И ПРОЦЕДУРЫ ПРИМЕНЕНИЯ УДАЛЕННОГО ДОСТУПА {Убрать раздел, если нет удаленного доступа}

10.1. {Описать}

11. ПРАВИЛА И ПРОЦЕДУРЫ ОБНАРУЖЕНИЯ (ПРЕДОТВРАЩЕНИЯ) ВТОРЖЕНИЙ {К2+}

11.1. {Описать}

12. ПРАВИЛА И ПРОЦЕДУРЫ ВЫЯВЛЕНИЯ, АНАЛИЗА И УСТРАНЕНИЯ УЯЗВИМОСТЕЙ

12.1. В {Название Организации} в качестве средства выявления уязвимостей используется сертифицированный сканер уязвимостей {название сканера}.

12.2. Администратор не реже одного раза в месяц проводит полное сканирование системы на выявление уязвимостей. В случае поступления информации из новостных источников об уязвимостях в операционных системах и/или прикладном программном обеспечении применяемых в ГИС «Бухгалтерия и кадры» производится внеплановое обновление базы данных сканера уязвимостей и полное сканирование информационной системы.

12.3. Администратор изучает отчеты по результатам сканирования и принимает решение о немедленном устранении выявленных уязвимостей, либо о включении мероприятий по устранению выявленных уязвимостей в план мероприятий по защите информации, в случае если выявленные уязвимости не являются критичными, или если есть возможность сделать невозможным их эксплуатацию потенциальным злоумышленником (например, путем отключения отдельных АРМ и/или сегментов сети от Интернет). При необходимости, для адекватного реагирования на вновь выявленные угрозы может созываться ГРИИБ.

12.4. Критичность уязвимостей может быть установлена как на основании рейтинга уязвимости по шкале CVSS, так и на основании оценки рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности».

12.5. При выявлении уязвимостей, Администратор анализирует системные журналы и журналы средств защиты информации, на предмет выявления эксплуатации выявленной уязвимости в информационной системе и последствий такой эксплуатации.

12.6. В случае невозможности оперативного устранения критичной уязвимости, Администратор уведомляет об этом руководителя {Название Организации}.

13. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ УСТАНОВКИ ОБНОВЛЕНИЙ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

13.1. {Описать}

14. ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ СОСТАВА ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

14.1. Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС «Бухгалтерия и кадры» фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

14.2. В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «Бухгалтерия и кадры» или удаления существующих компонентов, на основании акта ввода в

эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

14.3. Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

14.4. Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «Бухгалтерия и кадры» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

14.5. В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

14.6. Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководителю {Название Организации}, который принимает решение об организации самостоятельной сертификации использующегося СрЗИ, либо об обновлении использующегося СрЗИ до актуальной версии, либо о замене использующегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

15. {К2+} ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ЦЕЛОСТНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

15.1. {Описать}

16. ПРАВИЛА И ПРОЦЕДУРЫ РЕЗЕРВИРОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, БАЗ ДАННЫХ, СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ ВОССТАНОВЛЕНИЯ ПРИ ВОЗНИКНОВЕНИИ НЕШТАТНЫХ СИТУАЦИЙ

16.1. Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС «Бухгалтерия и кадры» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.

16.2. {К2+} Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ГИС «Бухгалтерия и кадры».

16.3. Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «Бухгалтерия и кадры».

16.4. Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

16.5. Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками {Название Организации}, имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;
  - обработка информации на незащищенных технических средствах обработки информации;
  - опубликование информации в открытой печати и других средствах массовой информации;
  - передача носителя информации лицу, не имеющему права доступа к ней;
  - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  - несанкционированное изменение информации;
  - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
  - несанкционированное подключение технических средств к средствам и системам ГИС «Бухгалтерия и кадры»;
  - использование закладочных устройств;
  - использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «Бухгалтерия и кадры»;
  - использование злоумышленником уязвимостей программного обеспечения ГИС;
  - использование злоумышленником программных закладок;
  - заражение ГИС злоумышленником программными вирусами;
  - хищение носителей информации;
  - нарушение функционирования технических средств обработки информации;
  - блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ГИС;
- дефекты, сбои, отказы программного обеспечения ГИС;
- сбои, отказы и аварии систем обеспечения ГИС;
- природные явления, стихийные бедствия:
  - термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
  - механические факторы (повреждения зданий, землетрясения и т. д.);
  - электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

16.6. В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

16.7. Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.

16.8. С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

16.9. Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

16.10. В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

16.11. В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- **в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация**

технических средств, носителей информации и носителей с резервными копиями.

17. {K2+} ПРАВИЛА ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ И ЗАЩИТЫ ОТ СПАМА

17.1. {Описать}

18. {K2+} ПРАВИЛА И ПРОЦЕДУРЫ КОНТРОЛЯ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ МОБИЛЬНОГО КОДА

18.1. {Описать}

Приложение № 1 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

ЗАЯВКА
на внесение изменений в списки пользователей и наделение пользователей полномочиями доступа к ресурсам ГИС

Прошу зарегистрировать пользователя (исключить из списка пользователей, изменить полномочия пользователя) ГИС
(нужное подчеркнуть)

_____
(должность с указанием подразделения)

_____
(фамилия имя и отчество сотрудника)

предоставив ему полномочия, необходимые (лишив его полномочий, необходимых)
(нужное подчеркнуть)

для решения задач:

_____
(список задач согласно формуляров задач)

_____

_____

_____

_____

_____

Начальник _____
(наименование заказывающего подразделения)

«___» _____ 20__ г. _____ _____
(подпись) (фамилия)

Согласовано Администратор безопасности

«___» _____ 20__ г. _____ _____
(подпись) (фамилия)

ЗАДАНИЕ
на внесение изменений в списки пользователей ГИС

Администратору безопасности информации

_____
(фамилия и инициалы исполнителя)

Произвести изменения в списках пользователей

Руководитель {Название Организации}

_____ {ФИО руководителя}

«___» _____ 20__ г.

Обратная сторона заявки

Присвоено **имя** _____ (персональный идентификатор) и предоставлены полномочия, необходимые для решения следующих задач:

Наименование задач

Администратор безопасности {ФИО Администратора}

Имя учетной записи, персональный идентификатор и начальное значение пароля получил, о порядке смены пароля при первом входе в систему проинструктирован, с инструкцией Пользователя ГИС ознакомлен

Пользователь

_____
(подпись, фамилия)

«___» _____ 20__ года

Приложение № 2 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Положение о разграничении прав доступа в ГИС «Бухгалтерия и кадры»

Исходя из характера и режима обработки защищаемой информации в ГИС «Бухгалтерия и кадры» определяется следующий перечень групп Пользователей, служб и процессов, участвующих в обработке защищаемой информации. Перечень ролей и описание параметров доступа к ресурсам ГИС приведен в таблице.

Роль	Описание параметров доступа к ресурсам ГИС для данной роли

Приложение № 3 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Перечень лиц, должностей, служб и процессов, допущенных к работе с ресурсами ГИС «Бухгалтерия и кадры»

Настоящий Перечень устанавливает перечень лиц, должностей и процессов, допущенных к работе с ресурсами ГИС «Бухгалтерия и кадры». Для каждого элемента списка в таблице обязательно указываются ФИО (Имя службы или процесса для неодушевленных субъектов доступа), должность (только для одушевленных субъектов доступа), имя присвоенной учетной записи и роль (в соответствии с Положением о разграничении прав доступа в ГИС). Тип и серийный номер выданного идентификатора указываются только при выдаче пользователю электронного ключа. Роспись о получении электронного ключа ставится только при выдаче пользователю такого ключа.

В настоящем Перечне не отражены вопросы, связанные с использованием средств криптографической защиты информации (СКЗИ). Перечни пользователей СКЗИ, а также иные учетный данные, связанные с СКЗИ приведены в других журналах и перечнях.

№ п/п	ФИО сотрудника / Имя службы или процесса	Должность	Имя присвоенной учетной записи	Роль	Выдан эл. ключ	Роспись о получении эл. ключа
1.						
2.						
3.						
4.						
5.						
6.						
7.						

Приложение № 4 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Перечень помещений, в которых разрешена работа с ресурсами ГИС «Бухгалтерия и кадры», в которых размещены технические средства ГИС, а также перечень лиц, допущенных в эти помещения

№ п/п	Название/номер помещения	Техническое средство ГИС						Сотрудники, допущенные в помещение	
		Тип	Модель	Учетный № (серийный, инвентарный)	Сетевое имя	IP-адрес	MAC-адрес	ФИО	Должность
1.	Серверная	Сервер	HP xxxxxx	S/N: xxxxxxx	1c-server	192.168.0.1	xx:xx:xx:xx:xx	Иванов Иван Иванович	Специалист по защите информации
		Коммутатор	Cisco ASA xxxx	Инв.: xxxxxx	-	192.168.0.100	xx:xx:xx:xx:xx	Петров Петр Петрович	Системный администратор
		СХД	HP xxxxxx	S/N: xxxxxxx	backup-server	192.168.0.101	xx:xx:xx:xx:xx		
2.	Бухгалтерия	Компьютер	HP xxxxxx	Инв.: xxxxxx	buh1	DHCP	xx:xx:xx:xx:xx	Сидорова Ольга Ивановна	Бухгалтер
		Ноутбук	Acer xxxxxxxx	S/N: xxxxxxx	buh2	DHCP	xx:xx:xx:xx:xx		
3.									
4.									
5.									
6.									
7.									
8.									
9.									
10.									
11.									

Приложение № 6 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Список разрешающих правил взаимодействия с внешними телекоммуникационными сетями в ГИС «Бухгалтерия и кадры» {если применяется политика «Запретить все, кроме явно разрешенного»}

№ п/п	IP/URL ресурса или подсеть	Обоснование разрешения	Правило	Время действия правила	Учетные записи, устройства, процессы, для которых действует правило
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					
11.					
12.					
13.					
14.					

Приложение № 7 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Список разрешенного программного обеспечения в ГИС «Бухгалтерия и кадры»

№ п/п	Наименование ПО	Тип ПО	Цель применения ПО в ГИС	Место установки компонентов ПО
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Приложение № 8 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Список прикладного программного обеспечения ГИС «Бухгалтерия и кадры», доступного пользователям внешней информационной системы Система 1

№ п/п	Наименование ПО	Тип ПО	Цель допуска к ПО внешних пользователей	Пользователи внешних систем, допущенный к работе с ПО
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				
11.				
12.				
13.				
14.				
15.				

Приложение № 9 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Список пользователей ГИС «Бухгалтерия и кадры» и внешних пользователей, которым в соответствии с должностными обязанностями предоставлен удаленный доступ к системе

№ п/п	ФИО	Является ли сотрудником организации	Ресурсы, к которым предоставляется удаленный доступ	Обязанности, в связи с которыми предоставляется удаленный доступ или основание для предоставления удаленного доступа	Учетная запись, от имени которой предоставляется удаленный доступ	Время, на которое предоставляется удаленный доступ
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						

Приложение № 10 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

Порядок резервирования информационных ресурсов в ГИС «Бухгалтерия и кадры»

№ п/п	Наименование информационного ресурса	Место размещения ресурса в системе	Вид резервного копирования	Ответственный за резервное копирование	Место хранения резервной копии	Частота резервного копирования
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						

Приложение № 11 к Политике информационной безопасности в {Название Организации}, утвержденной приказом от «___» _____20__г. № ___

План обеспечения непрерывности функционирования ГИС «Бухгалтерия и кадры»

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
1.	Разглашение защищаемой информации сотрудниками, имеющими легальные права доступа к ней		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
2.	Обнаружение несанкционированно скопированной или измененной конфиденциальной информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
3.	Несанкционированное копирование или изменение конфиденциальной информации в текущий момент времени со стороны лиц имеющих право доступа к ней		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	1 день
4.	Обнаружение подключения технических средств к средствам и системам объекта информатизации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	3 часа
5.	Подключение технических средств к средствам и системам ГИС в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	Сразу после получения информации об инциденте	3 часа
6.	Обнаружение закладочных устройств		Администратору сразу после обнаружения	Администратору не позднее 8 часов после	Сразу после получения информации об	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
			инцидента	инцидента	инциденте	
7.	Установка закладочных устройств злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
8.	Маскировка под зарегистрированного пользователя внешним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
9.	Маскировка под зарегистрированного пользователя внутренним злоумышленником или обнаружением факта маскировки		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
10.	Использование дефектов программного обеспечения ОИ внешним нарушителем в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
11.	Использование программных закладок внешним нарушителем в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
12.	Использование программных закладок внутренним злоумышленником или обнаружение факта использования		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
13.	Обнаружение программных вирусов		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	10 минут в рабочее время (1 час в нерабочее)	12 часов
14.	Хищение носителя защищаемой информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 сутки	3 дня

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
15.	Нарушение функционирования ТС обработки информации в текущий момент времени злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
16.	Обнаружение нарушения функционирования ТС обработки информации произведенного злоумышленником	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	10 минут в рабочее время (1 час в нерабочее)	1 день
17.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внешним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	7 дней
18.	Блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку внутренним злоумышленником в текущий момент времени		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
19.	Обнаружение произошедшего факта блокировки доступа к защищаемой информации		Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	20 минут в рабочее время (1 час в нерабочее)	1 день
20.	Ошибки пользователей системы при		Администратору	Администратору	2 часа в рабочее	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие утерю или повреждение защищаемой информации		сразу после обнаружения инцидента	не позднее 8 часов после инцидента	время (12 часов в нерабочее)	
21.	Ошибки пользователей системы при эксплуатации ТС, программных средств, средств и систем защиты информации, повлекшие нарушение работоспособности ТС и ПО	Нарушена работа одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	20 минут	2 дня
		Нарушена работа группы пользователей	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	20 минут	1 день
22.	Дефекты, сбои, отказы, аварии ТС, программных средств и систем ГИС	Сбой ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору сразу после обнаружения инцидента	1 час	2 дня
		Отказ ТС и систем ГИС, затронувший работу группы пользователей	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час в рабочее время (8 часов в нерабочее)	1 день
		Отказ ТС и систем ГИС, затронувший работу одного пользователя	Администратору сразу после обнаружения инцидента	Администратору в первый рабочий день после инцидента	1 час	2 дня
		Авария ТС и систем ГИС	Администратору сразу после обнаружения инцидента	Администратору не позднее 8 часов после инцидента	1 час	1 день
23.	Сбои, отказы и аварии систем обеспечения ГИС	Сбой систем обеспечения ГИС	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после	1 час	1 день

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
				инцидента		
		Отказ систем обеспечения ГИС, затронувший работу группы пользователей	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение и Администратору сразу после обнаружения инцидента	1 час	1 день
		Отказ систем обеспечения ГИС, затронувший работу одного пользователя	Ответственному за материально-техническое обеспечение сразу после инцидента	Ответственному за материально-техническое обеспечение в первый рабочий день после инцидента	1 час	2 дня
		Авария систем обеспечения ГИС	Ответственному за материально-техническое обеспечение, Администратору сразу после обнаружения инцидента	Ответственному за материально-техническое обеспечение, Администратору не позднее 8 часов после инцидента	1 час	1 день
24.	Природные явления, стихийные бедствия, несущие угрозу жизни человека		Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	Руководителю, заместителям руководителя, которые оповещают всех своих сотрудников сразу после получения информации	10 минут	30 минут
25.	Природные явления, стихийные		Руководителю,	Руководителю,	10 минут	1 час

№ п/п	Тип нештатной ситуации	Критерии нештатной ситуации	Кому и в какие сроки докладывается в рабочее время	Кому и в какие сроки докладывается в нерабочее время	Срок реализации неотложных действий	Срок реализации всех необходимых мероприятий
	бедствия, не несущие угрозу жизни человека		заместителям Руководителя, Администратору	заместителям Руководителя, Администратору		