ПРИКАЗ

«___» _____ 20__ г. №_____

О назначении ответственного за организацию обработки персональных данных и администратора безопасности в ГИС «Бухгалтерия и кадры»

В целях исполнения Федерального закона от 27.07.2006 N 152-ФЗ «О персональных данных», Приказа ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»,

ПРИКАЗЫВАЮ:

1. Ответственным за организацию обработки персональных данных в {Название Организации} назначить {должность, ФИО}.
2. Ответственному за организацию обработки персональных данных обеспечить автоматизированную обработку персональных данных на объектах информатизации, удовлетворяющих действующему законодательству.
3. Утвердить прилагаемую инструкцию ответственного за организацию обработки персональных данных.
4. Ответственному за организацию обработки персональных данных руководствоваться инструкцией ответственному за организацию обработки персональных данных.
5. Ответственному за организацию обработки персональных данных обеспечить неавтоматизированную обработку персональных данных в соответствии с действующим законодательством.
6. Ответственному за организацию обработки персональных данных в {Название Организации} разработать следующие документы: {перечень}.
7. Администратором безопасности информации в ГИС «Бухгалтерия и кадры» назначить {должность, ФИО}.
8. Утвердить прилагаемую инструкцию администратора безопасности.
9. Администратору безопасности в своей работе руководствоваться инструкцией администратора безопасности ГИС «Бухгалтерия и кадры».
10. Администратору безопасности организовать проведение работ по защите информации в соответствии с руководящими документами ФСТЭК России и ФСБ России.
11. Администратору безопасности разработать следующие документы: {перечень}.
12. Допуск к обработке персональных данных осуществлять в соответствии с положениями о разграничении прав доступа к персональным данным (Приложение № 2 к Политике информационной безопасности в {Название Организации}).
13. Лицам, допущенным к обработке персональных данных при неавтоматизированной их обработке и хранении руководствоваться документом «Правила обработки персональных данных без использования средств автоматизации».

14.Лицам, допущенным к обработке персональных данных при автоматизированной их обработке и хранении руководствоваться следующими документами:

- политика информационной безопасности;
- инструкция пользователя ГИС.

15.Осуществлять регистрацию обращений субъектов персональных данных в Журнале учета обращений субъектов персональных данных о выполнении их законных прав.

16. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель _____ {И. О. Фамилия}
{Название Организации}

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

Инструкция администратора безопасности в ГИС «Бухгалтерия и кадры» {Название Организации}

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Администратор безопасности в ГИС «Бухгалтерия и кадры» (далее – Администратор) назначается приказом руководителя {Название Организации} и отвечает за обеспечение конфиденциальности, целостности и доступности персональных данных (далее – ПДн) {и другой конфиденциальной информации} в процессе ее обработки в ГИС «Бухгалтерия и кадры».

1.2. Администратор обязан поддерживать в актуальном состоянии свои знания законодательных, нормативно-правовых актов Российской Федерации и методических материалов в сфере обработки и защиты ПДн.

1.3. В своей деятельности Администратор руководствуется настоящей Инструкцией, Положением об обработке и защите персональных данных, Политикой информационной безопасности и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

1.4. Администратор безопасности подчиняется напрямую Руководителю и имеет право требовать от пользователей ГИС выполнения указаний и инструкций, связанных с защитой информации.

1.5. Настоящая инструкция 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;

- «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. ФУНКЦИИ И ОБЯЗАННОСТИ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ В ГИС «БУХГАЛТЕРИЯ И КАДРЫ»

2.1. Изучение особенностей бизнес-процессов и технологических процессов обработки информации в {Название Организации} с целью принятия решения о необходимости защиты информации в ГИС и классификации ГИС, либо поиск специализированных организаций, производящих на договорной основе такой анализ. В случае привлечения сторонних организаций, Администратор обязан контролировать процесс сбора информации о ГИС сотрудниками сторонней организации. По окончании аналитических работ Администратор обязан ознакомиться с их результатами и подписать отчетные документы, либо составить мотивированный отказ в подписании таких документов и отправить их на доработку сторонней организации.

2.2. Определение актуальных угроз безопасности информации и разработка документа «Модель угроз безопасности ГИС», либо привлечение на договорной основе сторонних организаций для таких работ.

2.3. Периодический пересмотр актуальных угроз безопасности информации в следующих случаях:

- ежегодный плановый пересмотр актуальных угроз безопасности информации;
- появление в общедоступных источниках информации о новых угрозах и уязвимостях, имеющих предпосылки в ГИС;
- существенное изменение условий функционирования ГИС, внедрение новых технологий;
- изменение нормативной документации, касающейся моделирования угроз безопасности информации;
- в результате инцидента безопасности.

2.4. Разработка проектной документации на систему защиты информации в ГИС (Техническое задание, Технический проект), либо привлечение на договорной основе сторонних организаций для таких работ.

2.5. Участие в подготовке технических заданий для конкурсов и аукционов, связанных с закупкой технических средств, программного обеспечения или средств защиты информации для ГИС.

2.6. Участие в реализации проекта по защите информации в ГИС (тестирование системы защиты информации, внедрение системы защиты информации, аттестация ГИС по требованиям к защите информации, ввод в действие аттестованной ГИС).

2.7. Выработка предложений руководителю {Название Организации} по совершенствованию системы защиты информации в ГИС.

2.8. Ведение учета применяемых в ГИС средств защиты информации (в том числе криптосредств), эксплуатационной и технической документации к ним.

2.9. Знание состава, структуры, назначения и выполняемых задач ГИС, а также состава информационных технологий и технических средств, позволяющих осуществлять обработку ПДн и иной конфиденциальной информации.

2.10. Обеспечение передачи конфиденциальной информации и персональных данных через сети связи общего пользования в зашифрованном виде.

2.11. Разработка плана мероприятий по обеспечению безопасности защищаемой информации в ГИС и по защите периметра информационной системы. Принятие мер по выполнению мероприятий по обеспечению безопасности защищаемой информации в ГИС и непосредственное участие в проведении таких мероприятий. Актуализация плана мероприятий по мере необходимости.

2.12. Осуществление контроля неизменности состояния аттестованной ГИС (расположение и состав технических средств, состав программного обеспечения, физическое и логическое строение сети). В случае планирования изменения условий функционирования ГИС, Администратор должен связаться с аттестующим органом и получить указания к дальнейшим действиям.

2.13. Осуществление контроля физической сохранности и целостности технических средств ГИС, а также контроль сохранности и целостности опечатывающих пломб на технических средствах ГИС (в том числе и программно-аппаратных средствах защиты информации). Контроль неизменности состава технических средств в ГИС.

2.14. Организация учета съемных носителей информации. Настройка соответствующих программных механизмов средств защиты информации для запрета неучтенных съемных носителей. Ведение журнала учета съемных носителей.

2.15. Организация учета иных машинных носителей информации.

2.16. Проведение инструктажей сотрудников, работающих с защищаемой информацией в ГИС (далее – Пользователи ГИС), по темам: правила работы в ГИС, защита информации в ГИС, положения законодательства в сфере защиты информации и персональных данных, новые угрозы в сфере защиты информации. Повышение осведомленности всех сотрудников {Название Организации} в вопросах информационной безопасности.

2.17. Организация первоначального доступа пользователям ГИС к ресурсам информационный системы в соответствии с утвержденным положением о разграничении прав доступа в ГИС. Блокировка учетных записей, изменение полномочий пользователей и добавление новых пользователей ГИС в соответствии с Инструкцией о внесении изменений в списки пользователей и наделению их полномочиями доступа к ресурсам ГИС, утвержденной в {Название Организации}.

2.18. Осуществление резервного копирования защищаемой в соответствии разделом 11 настоящей Инструкции.

2.19. Реализация горячего резервирования ключевых узлов ГИС (межсетевых экранов, серверов баз данных, сервера AD, криптошлюзов, коммутаторов, маршрутизаторов).

2.20. Организация резервных каналов связи и контроль обеспечения провайдером заявленных характеристик канала связи.

2.21. Осуществление контроля целостности программного обеспечения (в том числе и средств защиты информации). Периодически (не реже одного раза в месяц) сверять рассчитанные контрольные суммы ключевых системных и исполняемых файлов ПО и СЗИ с эталонными значениями.

2.22. Периодическое тестирование функций системы защиты от НСД согласно плану мероприятий по обеспечению безопасности информации, либо при изменении программной среды или полномочий Пользователей ГИС.

2.23. Участие в составе группы реагирования на инциденты информационной безопасности в расследованиях причин инцидентов безопасности, внесение по результатам таких расследований предложений по совершенствованию системы безопасности. По мере возможности, Администратор должен восстанавливать ущерб, нанесенный информационной системе во время инцидента безопасности, а также восстанавливать ПДн и конфиденциальную информацию, модифицированную или уничтоженную в результате такого инцидента.

2.24. Контроль выполнения Пользователями ГИС требований Инструкции пользователя ГИС, а также других установленных требований для обеспечения безопасности ПДн и иной конфиденциальной информации.

2.25. В случае получения от Пользователей ГИС информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа, Администратор незамедлительно принимает все необходимые меры для обеспечения безопасности ПДн и иной конфиденциальной информации в пределах своих полномочий.

2.26. Обеспечение отсутствия на АРМ Пользователей ГИС средств разработки и отладки программного обеспечения. Контроль за отключением на АРМ Пользователей и невозможностью самостоятельного включения пользователем технологий мобильного кода (JavaScript, Adobe Flash, макросы MS Office и т. д.), кроме случаев, когда использование таких технологий необходимо для выполнения служебных (должностных) обязанностей.

2.27. Выявление уязвимостей ГИС посредством периодического сканирования системы сертифицированным сканером безопасности. Принятие решений на основании итогов каждого сканирования.

2.28. Контроль обновлений системного, прикладного программного обеспечения и средств защиты информации (в том числе обновлений антивирусных баз, сигнатур сценариев вторжений, информации об уязвимостях).

2.29. Контроль сотрудников сторонних организаций, производящих ремонт/обслуживание технических средств ГИС или настройку/установку программного обеспечения ГИС.

2.30. Обеспечение функционирования и поддержания работоспособности в ГИС:

- системы защиты информации от несанкционированного доступа;
- системы межсетевого экранирования;
- системы обнаружения и предотвращения вторжений;

- системы криптографической защиты информации;
- системы антивирусной защиты.

2.31. Обеспечение непрерывности процессов в ГИС. В случае нарушения работоспособности технических средств и программного обеспечения ГИС, в том числе средств защиты ГИС, Администратор принимает меры по их своевременному восстановлению и выявлению причин, приведших к нарушению работоспособности.

2.32. Своевременное информирование Ответственного за организацию обработки ПДн о выявленных нарушениях требований по обеспечению безопасности ПДн и попытках несанкционированного доступа к ГИС.

3. ПРАВА АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ГИС

Администратор имеет право:

3.1. Знакомиться с нормативными актами {Название Организации}, регламентирующими процессы обработки и защиты ПДн и иной конфиденциальной информации.

3.2. Вносить предложения руководителю {Название Организации} по совершенствованию существующей системы защиты информации.

3.3. Требовать от Пользователей ГИС соблюдения требований Инструкции пользователя ГИС и иных нормативно-правовых и организационно-распорядительных документов по обеспечению безопасности ПДн и иной конфиденциальной информации.

3.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения безопасности ПДн и иной конфиденциальной информации.

3.5. Требовать прекращения работы в ГИС, как в целом, так и отдельных Пользователей ГИС, в случае выявления нарушений требований по обеспечению безопасности ПДн или в связи с нарушением функционирования ГИС.

3.6. Обращаться за необходимыми разъяснениями по вопросам обработки и обеспечения безопасности ПДн к Ответственному за организацию обработки ПДн.

4. РАБОЧЕЕ МЕСТО АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ГИС И ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ СИСТЕМОЙ ЗАЩИТЫ ИНФОРМАЦИИ

4.1. Одним из ключевых элементов системы защиты информации в ГИС «Бухгалтерия и кадры» является АРМ Администратора.

4.2. АРМ Администратора устанавливается таким образом, чтобы исключался как преднамеренный, так и непреднамеренный несанкционированный доступ к техническим средствам АРМ Администратора.

4.3. На АРМ Администратора устанавливаются средства централизованного управления: антивирусной защитой ГИС, средствами обнаружения вторжений в ГИС, средством защиты информации от несанкционированного доступа в ГИС. Также на АРМ Администратора устанавливается сканер уязвимостей.

4.4. Администратор осуществляет централизованное управление политиками безопасности в ГИС, обновлениями средств защиты информации, обновлениями антивирусных баз и сигнатур, конфигурацией информационной системы. Также Администратор централизованно осуществляет периодическое сканирование уязвимостей ГИС.

4.5. Администратор изучает журналы безопасности средств защиты информации на предмет выявления инцидентов безопасности.

4.6. Рабочее место администратора является объектом защиты и защищается согласно требованиям к тому же классу, по которому классифицирована ГИС в целом.

5. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦАНИРОВАННОГО ДОСТУПА {НАЗВАНИЕ СЗИ ОТ НСД}

5.1. Администратор участвует в развертывании средства защиты информации от несанкционированного доступа (далее – СЗИ от НСД) в ГИС и осуществляет управление и централизованный мониторинг этого средства с рабочего места Администратора.

5.2. Администратор производит настройку подсистемы регистрации, идентификации и аутентификации в СЗИ от НСД {Название СЗИ от НСД} согласно утвержденному Положению о разграничении доступа. Идентификации и аутентификации подлежат как пользователи, так и учетные записи служб, приложений, программных процессов.

5.3. Удаленные (внешние) пользователи проходят идентификацию и аутентификацию. Администратор обеспечивает наличие минимального количества точек входа удаленных пользователей в ГИС. Администратор производит мониторинг подключений и действий внешних пользователей в ГИС. Администратор обеспечивает отсутствие у внешних пользователей привилегированных (административных) прав доступа в ГИС. Администратор обеспечивает доступ внешних (удаленных) пользователей к ГИС по защищенным каналам связи. Администратор предоставляет возможность удаленного доступа в ГИС только тем пользователям, которым такой доступ необходим в силу исполнения ими служебных обязанностей. Удаленный доступ запрещается от имени учетных записей с повышенными полномочиями (системные администраторы, администраторы безопасности и т. д.).

5.4. Удаленные (внешние) пользователи проходят двухфакторную аутентификацию при установлении сеанса связи с ГИС. Администратор обеспечивает удаленных пользователей электронными ключами, а также проводит их инструктаж по правилам обращения с электронными ключами и по правилам двухфакторной аутентификации в ГИС.

5.5. Администратор осуществляет контроль использования в ГИС мобильных технических средств (ноутбуки, нетбуки, планшеты, смартфоны и иные устройства). В случае использования мобильных устройств удаленными пользователями для доступа в ГИС, Администратор принимает меры, предусмотренные частью 5.3 данной Инструкции. Учет мобильных технических средств ГИС производится Администратором в Журнале учета портативных устройств, имеющих встроенные носители информации.

5.6. Технические средства (мобильные и стационарные) также проходят идентификацию и аутентификацию в ГИС. Идентификация и аутентификация устройств производится посредством информационного обмена по специализированным сетевым протоколам (ARP, SNMP, NetBIOS и др.). В качестве идентификаторов устройств могут выступать: логические имена, идентификационные номера, IP-адреса, MAC-адреса или комбинация этих параметров. Администратор определяет правила идентификации и аутентификации устройств в ГИС, конфигурирует протоколы и настраивает в средствах защиты информации соответствующие правила. Администратор принимает меры для предупреждения таких атак на ГИС как MAC-flooding, MAC-spoofing, ARP-spoofing, ARP-poisoning и других.

5.7. Администратор осуществляет учет машинных носителей информации, как стационарных (жесткие диски АРМ и серверов, SSD-накопители и т. д.), так и съемных (флеш-накопители, съемные жесткие диски, карты памяти, память мобильных устройств и т. д.). Каждому носителю присваивается идентификационный номер. Для стационарных машинных носителей информации фиксируется местонахождение носителя (АРМ, кабинет), в случае замены или утилизации стационарного или съемного машинного носителя принимаются меры по гарантированному уничтожению информации на носителе или самого носителя с соответствующей пометкой в Журнале учета машинных носителей информации. Съемные машинные носители информации выдаются пользователям под роспись в Журнале учета приема/выдачи съемных машинных носителей информации. Дата сдачи машинного носителя также фиксируется в Журнале. Администратор средствами СЗИ от НСД {Название СЗИ от НСД} реализует запрет использования неучтенных машинных носителей в ГИС.

5.8. Администратор осуществляет управление учетными записями с помощью встроенных механизмов ОС и с помощью механизмов СЗИ от НСД {Название СЗИ от НСД}. В процессе управления учетными записями Администратор производит следующие действия:

- определяет тип учетной записи (внутренний пользователь, внешний пользователь, системная учетная запись, учетная запись приложения, гостевая учетная запись, временная учетная запись и т. д.);
- объединение учетных записей в группы (при необходимости);
- проводит верификацию пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя;
- проводит анализ необходимости тех или иных полномочий в системе для учетных записей служб и приложений;
- производит заведение, активацию, блокирование и уничтожение учетных записей пользователей;
- проводит пересмотр и, при необходимости, корректировку учетных записей пользователей либо в процессе периодического мероприятия, либо в связи с изменением должностных обязанностей того или иного пользователя;
- уничтожает временные учетные записи пользователей, предоставленные для однократного (или ограниченного по времени) выполнения задач в ГИС, и учетные записи уволенных сотрудников;
- осуществляет настройку прав доступа пользователей к ресурсам ГИС средствами СЗИ от НСД {Название СЗИ от НСД} в соответствии с утвержденным Положением о разграничении доступа;
- средствами СЗИ от НСД {Название СЗИ от НСД} настраивает автоматическое блокирование неактивных (неиспользуемых) учетных

записей пользователей после периода времени неиспользования более 90 дней. {для ГИС К1 – 45 дней}

5.9. Администратор запрещает средствами СЗИ от НСД {Название СЗИ от НСД} любые действия пользователя в ГИС до прохождения процедур идентификации и аутентификации, в том числе ограничивает доступ к настройкам BIOS/UEFI. Администратору информационной безопасности до идентификации и аутентификации разрешаются следующие действия с целью диагностики проблем на элементах ГИС и восстановления работоспособности элементов ГИС:

- загрузка операционной системы в безопасном режиме;
- восстановление операционной системы с последней работоспособной конфигурацией;
- изменение параметров BIOS/UEFI;
- загрузка с внешнего носителя с целью восстановления или переустановки операционной системы, восстановления работоспособности средств защиты информации, сканирования жесткого диска на вирусы, сканирования оперативной памяти или жесткого диска с целью выявления проблем и других действий восстановительного или диагностического характера.

5.10. Администратор является ответственным за хранение, выдачу, инициализацию средств аутентификации (аппаратных ключей, учетных записей, первичных паролей). Администратор с помощью механизмов СЗИ от НСД {Название СЗИ от НСД} определяет парольную политику и требования к сложности паролей. Администратор выдает пользователю пароль для первоначального входа в ГИС. СЗИ от НСД требует от пользователя сменить пароль при первом же входе в систему. Плановая смена пароля производится пользователем самостоятельно. Смена пароля Администратором допускается в случаях компрометации пароля пользователя или при подозрении на его компрометацию, в этом случае система также должна запросить смену пароля пользователем при первом входе в ГИС после смены пароля Администратором. Администратор не должен и не обязан знать пароли пользователей ГИС. В ГИС средствами СЗИ от НСД {Название СЗИ от НСД} устанавливаются следующие требования к паролям:

- минимальная длина пароля составляет 8 символов, пароль должен содержать буквы английского алфавита верхнего и нижнего регистров, как минимум одну цифру и один спецсимвол;
- при смене пароля, новый пароль должен отличаться минимум на два символа от предыдущего;
- максимальное время действия пароля – 90 дней;
- минимальное время действия пароля – 10 дней;
- запрещается использование пользователями пяти последних использованных паролей при создании новых паролей;
- при восьми неудачных попытках входа учетная запись блокируется не менее, чем на 10 минут.

5.11. Администратор с помощью механизмов СЗИ от НСД {Название СЗИ от НСД} устанавливает временной промежуток в 15 минут {5 минут для К1} в качестве допустимого времени бездействия пользователя. После истечения указанного времени происходит блокировка сеанса пользователя.

5.12. Администратор контролирует наличие и работоспособность средств доверенной загрузки.

5.13. Администратор средствами СЗИ от НСД {Название СЗИ от НСД} запрещает пользователям самостоятельную установку любого программного обеспечения. В {Название организации} утверждается перечень разрешенного к установке в ГИС программного обеспечения. Перечень разрешенного к установке программного обеспечения определяется исходя из целей и задач, решаемых с помощью ГИС. Перечень разрешенного к установке в ГИС программного обеспечения подлежит периодическому пересмотру. Установка разрешенного программного обеспечения производится либо Администратором лично, либо в присутствии Администратора и под контролем Администратора.

5.14. Механизмами СЗИ от НСД {Название СЗИ от НСД} Администратор устанавливает правила использования интерфейсов ввода/вывода технических средств ГИС. СЗИ от НСД настраивается таким образом, чтобы пользователь ГИС получал доступ к использованию только тех интерфейсов ввода/вывода, которые необходимы ему для выполнения служебных обязанностей.

5.15. Администратор настраивает в СЗИ от НСД {Название СЗИ от НСД} контроль целостности программного обеспечения. Администратор осуществляет расчет эталонной контрольной суммы и перерасчет при обновлении (санкционированном изменении) программного обеспечения. Администратор принимает меры реагирования при нарушении целостности программного обеспечения.

6. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СРЕДСТВ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ И СРЕДСТВ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ, ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ

6.1. {Описать аналогично СЗИ от НСД}

7. ОБСЛУЖИВАНИЕ СРЕДСТВ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

7.1. Общие правила работы с криптосредствами описаны в утвержденной Инструкции по обеспечению безопасности эксплуатации СКЗИ. В данном разделе описана часть, касающаяся функций и обязанностей Администратора.

7.2. Исходя из требований к защите информации и актуальных угроз безопасности информации в ГИС, Администратор определяет необходимость использования средств криптографической защиты информации (далее – СКЗИ) в системе защиты информации ГИС.

7.3. Администратор обеспечивает соответствие работы с СКЗИ технической и эксплуатационной документации к ним.

7.4. Администратор осуществляет поэкземплярный учет СКЗИ, технической и эксплуатационной документации к ним в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ГИС.

7.5. Администратор контролирует передачу СКЗИ, ключевой информации, технической и эксплуатационной документации пользователям ГИС. Факт передачи отражается в Журнале поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов в ГИС.

7.6. Администратор обеспечивает хранение дистрибутивов СКЗИ, эксплуатационную и техническую документацию к ним, ключевую информацию в шкафах (сейфах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

7.7. Администратор обеспечивает раздельное хранение действующих и резервных ключевых документов, предназначенных для применения в случае компрометации действующих ключевых документов.

7.8. Администратор производит инструктаж пользователей перед работой с СКЗИ. Отметка о проведении инструктажа проставляется в Журнале учета инструктажей по информационной безопасности в ГИС.

7.9. Администратор составляет и поддерживает в актуальном состоянии список лиц, допущенных к работе с СКЗИ.

7.10. Администратор осуществляет проверку готовности СКЗИ к использованию в ходе проведения проверок согласно Плану мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ГИС. Факт проверки отражается в Журнале учета мероприятий по контролю обеспечения защиты информации в ГИС. Результат проверки отражается в Журнале периодического тестирования средств защиты информации в ГИС. Проверка каждого СКЗИ проводится не реже одного раза в месяц.

7.11. Администратор инструктирует пользователей о порядке хранения ключевой информации и осуществляет контроль соблюдения пользователями правил хранения такой информации.

7.12. Администратор принимает участие в составе группы реагирования на инциденты информационной безопасности в расследовании случаев попыток посторонних лиц получить сведения об используемых СКЗИ, случаев компрометации или при подозрении на компрометацию ключевой информации, случаев утраты дистрибутивов СКЗИ, ключевой информации, ключевых носителей, технической и эксплуатационной документации к СКЗИ, ключей от помещений и хранилищ СКЗИ. В случае компрометации ключевой информации, Администратор немедленно выводит ее из эксплуатации.

7.13. Администратор в составе комиссии по уничтожению принимает участие в уничтожении ключевой информации и ключевых документов. Уничтожение ключевой информации производится путем физического уничтожения ключевого носителя или путем гарантированного затирания ключевой информации.

8. НАСТРОЙКА И ОБСЛУЖИВАНИЕ СИСТЕМЫ АНТИВИРУСНОЙ ЗАЩИТЫ

8.1. {Описать аналогично СЗИ от НСД}

9. РЕГИСТРАЦИЯ И УЧЕТ СОБЫТИЙ БЕЗОПАСНОСТИ

9.1. Под системой регистрации и учета событий безопасности в ГИС понимается совокупность средств централизованного управления всех СЗИ в ГИС.

9.2. Система регистрации и учета событий безопасности, а также информация, хранящаяся в электронных журналах регистрации событий сами по себе являются объектами защиты. Администратор принимает меры по защите этой

информации в соответствии с техническим заданием на систему защиты информации и эскизным проектом системы защиты информации. Доступ к записям системы регистрации и учета событий безопасности разрешен только Администратору.

9.3. Администратор периодически изучает записи системы регистрации и учета событий безопасности и в случае обнаружения инцидентов безопасности информации созывает группу реагирования на инциденты информационной безопасности, которая в свою очередь действует согласно соответствующим инструкциям.

9.4. В ГИС реализуется регистрация событий безопасности в виртуальной инфраструктуре. Администратор участвует в настройке системы регистрации событий безопасности в виртуальной инфраструктуре и изучает журналы событий с определенной периодичностью. Регистрации подлежат следующие события: {убрать если ГИС К4 или нет виртуализации}

- запуск (завершение) работы компонентов виртуальной инфраструктуры;
- доступ субъектов доступа к компонентам виртуальной инфраструктуры;
- изменения в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения;
- изменения правил разграничения доступа к компонентам виртуальной инфраструктуры.

10. ВЫЯВЛЕНИЕ, АНАЛИЗ И УСТРАНЕНИЕ УЯЗВИМОСТЕЙ

10.1. {Описать исходя из исходных данных}

11. ПРАВИЛА РЕЗЕРВИРОВАНИЯ И ВОССТАНОВЛЕНИЯ ИНФОРМАЦИИ, ТЕХНИЧЕСКИХ СРЕДСТВ, ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

11.1. {Описать исходя из исходных данных}

12. ОБСЛУЖИВАНИЕ СИСТЕМЫ ЗАЩИТЫ ВИРТУАЛЬНОЙ СРЕДЫ

12.1. {Описать исходя из исходных данных}

13. ДЕЙСТВИЯ АДМИНИСТРАТОРА ПРИ РЕМОНТЕ ТЕХНИЧЕСКИХ СРЕДСТВ, ОБСЛУЖИВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И УТИЛИЗАЦИИ НОСИТЕЛЕЙ ИНФОРМАЦИИ

13.1. Администратор присутствует в процессе установки, обновления, настройки программного обеспечения в ГИС (в том числе и средств защиты информации) сотрудниками сторонних организаций.

13.2. Администратор присутствует в процессе ремонта технических средств ГИС сотрудниками сторонних организаций на территории {Название организации}. Администратор обеспечивает гарантированное затирание данных с носителей информации, либо демонтаж носителей информации (в том числе и оперативной памяти) с технических средств в случае необходимости отправки технических средств для ремонта на территорию сторонних организаций.

13.3. Администратор обеспечивает гарантированное затирание данных на машинных носителях информации при утилизации технических средств, либо

принимает участие в физическом уничтожении машинных носителей информации в составе комиссии по уничтожению.

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

Инструкция ответственного за организацию обработки персональных данных в {Название Организации}

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Ответственный за организацию обработки персональных данных в {Название Организации} (далее – Ответственный) назначается приказом руководителя {Название Организации} (далее – Учреждение) и отвечает за организацию, обеспечение своевременного и квалифицированного выполнения сотрудниками Учреждения законодательства Российской Федерации о персональных данных (далее – ПДн), в том числе требований к обработке и защите ПДн.

1.2. Ответственный должен знать законодательные и иные нормативные правовые акты Российской Федерации, методические материалы в сфере обработки и защиты ПДн. Ответственный поддерживает в актуальном состоянии свои знания в сфере действующего законодательства и законодательных инициатив, связанных с защитой персональных данных.

1.3. В своей деятельности Ответственный руководствуется Положением об обработке и защите персональных данных, настоящей Инструкцией и действующим законодательством в сфере защиты персональных данных и конфиденциальной информации.

2. ОСНОВНЫЕ ФУНКЦИИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1. Ответственный изучает все стороны деятельности Учреждения и вырабатывает рекомендации по организации обработки ПДн при решении следующих основных вопросов:

- организация доступа к ПДн и учет сотрудников Учреждения, допущенных к обработке ПДн, как в программных комплексах, входящих в состав ГИС, так и на бумажных носителях;
- контроль за поддержанием в актуальном состоянии действующих локальных нормативных актов, журналов и форм учета по работе с ПДн;
- контроль за обеспечением соответствия проводимых работ в части обработки ПДн технике безопасности, правилам и нормам охраны труда;
- организация работы по заключению договоров на работы по защите ПДн;
- контроль изменений в процессах обработки ПДн и, в случае необходимости, отправка информации об этих изменениях в уполномоченный территориальный орган по защите прав субъектов персональных данных (Роскомнадзор) с целью актуализации уведомления {Название Организации} в реестре операторов ПДн;
- рассмотрение предложений по совершенствованию действующей системы защиты ПДн, предоставленных Администратором, назначаемым приказом руководителя {Название Организации};

- осуществление в пределах своей компетенции иных функций в соответствии с целями и задачами Учреждения.

3. ОСНОВНЫЕ ОБЯЗАННОСТИ ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Знать цели обработки ПДн в Учреждении и перечень обрабатываемых ПДн.

3.2. Соблюдать требования нормативных актов Учреждения, устанавливающих порядок работы с ПДн.

3.3. Обеспечивать доведение до сведения сотрудников Учреждения законодательства Российской Федерации о ПДн, нормативных актов по вопросам обработки ПДн, требований к защите ПДн.

3.4. Осуществлять внутренний контроль за соблюдением сотрудниками Учреждения законодательства Российской Федерации о ПДн, в том числе требований к защите ПДн.

3.5. Контролировать ведение документации, предусмотренной нормативными актами Учреждения в части обеспечения безопасности ПДн.

3.6. Обеспечивать доработку локальных нормативных документов по защите ПДн Учреждения в случае такой необходимости или при поступлении такого требования от регулирующего органа.

3.7. Участвовать в расследовании нарушений по вопросам защиты ПДн, имевших место, разрабатывать предложения по устранению недостатков и предупреждению подобного рода нарушений.

3.8. Обеспечивать организацию проведения занятий со специалистами Учреждения по организационным вопросам обработки ПДн (проводить инструктаж сотрудников, осуществляющих обработку ПДн и имеющих доступ к ПДн, обрабатываемым в Учреждении).

3.9. Обеспечивать организацию приема и обработки обращений и запросов субъектов ПДн или их представителей по вопросам обработки ПДн и (или) осуществлять контроль за приемом и обработкой таких обращений и запросов согласно п.3 ч.4 ст.22.1 Федерального закона от 27.07.06 № 152-ФЗ «О персональных данных».

4. ПРАВА ОТВЕТСТВЕННОГО ЗА ОРГАНИЗАЦИЮ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1. Знакомиться с документами и материалами, необходимыми для выполнения возложенных на него задач.

4.2. Проводить проверки соблюдения режима обеспечения безопасности ПДн в структурных и (или) территориальных подразделениях Учреждения (при их наличии) в соответствии с утвержденным приказом руководителя {Название Организации} планом мероприятий по обеспечению безопасности защищаемой информации, выполнению требований законодательства по защите информации, а также по контролю уровня защищенности и выполнения мер по защите информации в ГИС «Бухгалтерия и кадры».

4.3. Требовать от сотрудников Учреждения соблюдения требований нормативно-правовых и организационно-распорядительных документов по вопросам обработки ПДн.

4.4. Инициировать проведение служебных расследований по фактам нарушения установленных требований обработки ПДн.

4.5. Требовать от сотрудников Учреждения письменных объяснений при проведении служебных расследований по вопросам нарушений требований по обработке и защите ПДн.

4.6. Вносить предложения руководителю {Название Организации} об отстранении от выполнения служебных обязанностей сотрудников, систематически нарушающих требования по обработке и защите ПДн.

4.7. Давать сотрудникам Учреждения обязательные для выполнения указания по обработке и защите ПДн, определяемые законодательством Российской Федерации и локальными нормативными актами Учреждения.

4.8. Привлекать в установленном порядке специалистов Учреждения, имеющих непосредственное отношение к рассматриваемым проблемам, для более детального изучения отдельных вопросов, возникающих в процессе работы.