МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА ТУЛЬСКОЙ ОБЛАСТИ

ПРИКАЗ

10.03.2017 **№ 8-осн.**

Об утверждении документов, регламентирующих защиту персональных данных в министерстве сельского хозяйства Тульской области.

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», постановлением Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», нормативными и методическими документами ФСТЭК России и ФСБ России, на основании подпункта 5 пункта 7 Положения о министерстве сельского хозяйства Тульской области, п р и к а з ы в а ю:

1. Утвердить Политику министерства сельского хозяйства Тульской области в отношении обработки персональных данных (приложение № 1).
2. Утвердить инструкцию ответственного за организацию обработки персональных данных в министерстве сельского хозяйства Тульской области (приложение № 2).
3. Утвердить инструкцию пользователя информационных систем персональных данных и автоматизированных систем в министерстве сельского хозяйства Тульской области (приложение № 3).
4. Утвердить положение об обеспечение безопасности персональных данных в министерстве сельского хозяйства Тульской области (приложение № 4).
5. Утвердить инструкцию пользователя средств криптографической защиты информации в министерстве сельского хозяйства Тульской области (приложение № 5).

6. Утвердить инструкцию по порядку использования и организации работы со средствами криптографической защиты информации в министерстве сельского хозяйства Тульской области (приложение № 6).

7. Признать утратившим силу приказ министерства сельского хозяйства Тульской области от 05.05.2016 № 35 «Об утверждении документов, регламентирующих защиту персональных данных в министерстве сельского хозяйства Тульской области».

8. Политику министерства сельского хозяйства Тульской области в отношении обработки персональных данных разместить на официальном сайте министерства не позднее 10 рабочих дней с момента подписания.

9. Контроль за исполнением приказа оставляю за собой.

Заместитель председателя правительства Тульской области - министр сельского хозяйства Тульской области **Д.В. Миляев**

Приложение № 1
к приказу министерства сельского
хозяйства Тульской области
от 10.03.2017 № 8-осн.

Политика
министерства сельского хозяйства Тульской области
в отношении обработки персональных данных

1. Общие положения

1.1. Настоящая Политика министерства сельского хозяйства Тульской области в отношении обработки персональных данных (далее - Политика) разработана в соответствии с требованиями Федерального закона от 27.07.2006 №152-ФЗ «О персональных данных» в министерстве сельского хозяйства Тульской области (далее – министерство).

1.2. Политика определяет цели, принципы обработки и реализуемые требования к защите персональных данных в министерстве.

1.3. Персональные данные являются информацией ограниченного доступа и подлежат защите в соответствии с законодательством Российской Федерации.

2. Основные понятия

2.1. В настоящей Политике используются следующие основные понятия:

2.1.1. Субъектами персональных данных министерства являются: государственные гражданские служащие, работники министерства, претенденты на замещение должностей и их близкие родственники, физические лица, состоящие в Общественном совете при министерстве, лица, состоящие в договорных и (или) иных гражданских-правовых отношениях с министерством, представители организаций, крестьянских (фермерских) хозяйств, сельскохозяйственных потребительских кооперативов, индивидуальные предприниматели и граждане, ведущие лично подсобное хозяйство, обратившихся в министерство, граждане РФ направившие обращение в адрес министерства, граждане РФ достигшие наивысших результатов трудовой деятельности в организациях АПК Тульской области.

2.1.2. Персональные данные - любая информация, относящаяся прямо или косвенно к определенному, или определяемому физическому лицу (субъекту персональных данных).

2.1.3. Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

2.1.4. Конфиденциальность персональных данных – обязанность оператора и иных лиц, получивших доступ к персональным данным, не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

3. Принципы и цели обработки персональных данных

3.1. Министерство в своей деятельности по обработке персональных данных руководствуется следующими принципами:

3.1.1. Обработка персональных данных осуществляется на законной и справедливой основе.

3.1.2. Цели обработки персональных данных соответствуют полномочиям министерства.

3.1.3. Содержание и объем обрабатываемых персональных данных соответствуют целям обработки персональных данных.

3.1.4. Достоверность персональных данных, их актуальность и достаточность для целей обработки, недопустимость обработки избыточных по отношению к целям сбора персональных данных.

3.1.5. Ограничение обработки персональных данных при достижении конкретных и законных целей, запрет обработки персональных данных, несовместимых с целями сбора персональных данных.

3.1.6. Запрет объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

3.1.7. Осуществление хранения персональных данных в форме, позволяющей определить субъект персональных данных, не дольше, чем это требуют цели обработки персональных данных, если срок хранения персональных данных не установлен действующим законодательством.

3.1.8. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижению целей обработки или в случае утраты необходимости в достижении этих целей, если иное не предусмотрено действующим законодательством.

3.2. Обработка персональных данных работников министерства осуществляется в целях обеспечения соблюдения Конституции Российской Федерации, федеральных законов и иных нормативных правовых актов Российской Федерации, содействия им в прохождении службы, в обучении и должностном росте, обеспечения их личной безопасности и членов их семей, а также в целях обеспечения сохранности принадлежащего им имущества и имущества государственного органа, учета результатов исполнения ими должностных обязанностей.

3.3. Обработка персональных данных граждан, не являющихся работниками министерства, осуществляется с целью реализации закрепленных за министерством полномочий.

4. Перечень мер по обеспечению безопасности персональных данных при их обработке

4.1. Министерство при обработке персональных данных принимает все необходимые правовые, организационные и технические меры для их защиты от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении них. Обеспечение безопасности персональных данных достигается, в частности, следующими способами:

4.1.1. Назначением ответственного за организацию обработки персональных данных.

4.1.2. Утверждением локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений.

4.1.3. Осуществлением внутреннего контроля соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных.

4.1.4. Ознакомлением работников министерства, непосредственно осуществляющих обработку персональных данных, с требованиями законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, локальными актами в отношении обработки персональных данных, и обучением указанных работников.

4.1.5. Выполнением требований, установленных Постановлением Правительства Российской Федерации от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» при обработке персональных данных, осуществляемой без использования средств автоматизации.

4.1.6. Применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации.

4.1.7. Учетом машинных носителей персональных данных.

4.1.8. Выявлением фактов несанкционированного доступа к персональным данным и принятием мер.

4.1.9. Восстановлением персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

4.1.10. Установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых в информационной системе персональных данных.

4.2. Работники министерства, виновные в нарушении порядка обращения с персональными данными, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с законодательством Российской Федерации.

Приложение № 2
к приказу министерства сельского
хозяйства Тульской области
от 10.03.2017 № 8-осн.

ИНСТРУКЦИЯ
ответственного за организацию обработки персональных данных в министерстве сельского хозяйства Тульской области

1. Инструкция ответственного за организацию обработки персональных данных в министерстве сельского хозяйства Тульской области (далее – инструкция) разработана в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 02 мая 2006 года № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации», Постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановлением правительства Тульской области от 29.04.2014 № 213 «О мерах по реализации отдельных положений Федерального закона «О персональных данных», другими нормативными правовыми актами в области персональных данных.

2. Инструкция определяет ответственность, права и обязанности лица, назначенного ответственным за организацию обработки персональных данных в министерстве сельского хозяйства Тульской области (далее – министерство).

3. Ответственный за организацию обработки персональных данных в министерстве отвечает за:

соблюдение в министерстве требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

своевременность и качество проводимых им работ и мероприятий;

нарушение требований настоящей инструкции.

4. В обязанности ответственного за организацию обработки персональных данных в министерстве входит:

осуществление внутреннего контроля за соблюдением в министерстве требований законодательства Российской Федерации в области персональных данных, в том числе требований к защите персональных данных;

доведение до сведения работников и государственных гражданских служащих (далее – служащие, работники) министерства положений законодательства Российской Федерации в области персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

организация приема и обработки обращений и запросов субъектов персональных данных или их представителей, а также осуществление контроля за приемом и обработкой таких обращений и запросов;

информирование руководителя министерства о фактах нарушения порядка обращения с персональными данными, о попытках несанкционированного доступа к ним.

5. Ответственный за организацию обработки персональных данных в министерстве имеет право:

в установленном порядке осуществлять контроль соответствия обработки персональных данных требованиям законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

участвует в разработке документов министерства, регламентирующих обработку и защиту персональных данных;

участвует в рассмотрении вопросов и проведении расследований по фактам нарушений в сфере обработки и защиты персональных данных, информирует об этом руководителя министерства;

запрашивает и получает в установленном порядке информацию от служащих (работников) аппарата, органов исполнительной власти Тульской области, органов местного самоуправления, юридических лиц, необходимую для решения вопросов, входящих в их компетенцию;

в установленном порядке привлекает к реализации мер, направленных на выполнение требований законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных, служащих (работников) аппарата, органов исполнительной власти Тульской области, юридических лиц независимо от их организационно-правовой формы;

принимает меры по приостановлению или прекращению обработки персональных данных, осуществляемой с нарушением требований законодательства Российской Федерации в сфере персональных данных;

вносит руководителю министерства предложения о совершенствовании правового, технического и организационного регулирования обработки и обеспечения безопасности персональных данных в аппарате;

в установленном порядке вносит представление о применении к служащим (работникам) министерства мер взыскания.

Приложение № 3
к приказу министерства сельского
хозяйства Тульской области
от 10.03.2017 № 8-осн.

ИНСТРУКЦИЯ
пользователя информационных систем персональных данных и автоматизированных систем в министерстве сельского хозяйства Тульской области

1. Пользователями информационных систем персональных данных (далее – ИСПДн) и автоматизированных систем (далее – АС) министерства сельского хозяйства Тульской области (далее – министерство) являются государственные гражданские служащие и работники министерства, в установленном порядке допущенные к работе в ИСПДн и АС.

2. Настоящая инструкция определяет обязанности, права и ответственность пользователей, допущенных к работе в ИСПДн и АС, в области обеспечения безопасности конфиденциальной информации, в том числе персональных данных (далее – ПДн).

3. При эксплуатации ИСПДн и АС пользователь обязан:

а) соблюдать конфиденциальность при работе с информацией в ИСПДн и АС;

б) руководствоваться требованиями настоящей инструкции, а также следующих документов:

«Инструкция по применению машинных носителей информации в органах исполнительной власти, подразделениях аппарата правительства Тульской области и в подведомственных им учреждениях», утвержденная приказом комитета Тульской области по инновациям и информатизации от 29 апреля 2013 года № 33, в части, его касающейся;

«Инструкция по авторизации пользователей в информационных системах органов исполнительной власти Тульской области и аппарата правительства Тульской области», утвержденная приказом министерства по информатизации, связи и вопросам открытого управления Тульской области от 20.02.2015 № 12-осн, в части, его касающейся;

«Политика антивирусной защиты информации в органах исполнительной власти Тульской области, аппарате правительства Тульской области, подведомственных учреждениях Тульской области», утвержденная приказом министерства по информатизации, связи и вопросам открытого управления Тульской области от 04.05.2016 № 58-осн, в части, его касающейся;

«Требования к перечню и порядку использования программного обеспечения в аппарате правительства Тульской области, органах исполнительной власти Тульской области и их подведомственных учреждениях», утвержденные приказом министерства по информатизации, связи и вопросам открытого управления Тульской области от 15.08.2016 № 94-осн, в части, его касающейся;

в) помнить свои личные пароли и идентификаторы;

г) руководствоваться требованиями инструкций по эксплуатации установленных средств вычислительной техники и средств защиты информации (далее – СЗИ);

д) блокировать ввод-вывод информации на своем автоматизированном рабочем месте ИСПДн и АС (далее – АРМ) перед оставлением своего рабочего места (перерыва в работе) или выключать АРМ;

е) блокировать вывод информации на монитор АРМ при выходе в течение рабочего дня из помещения, в котором размещается ИСПДн и АС.

4. При эксплуатации ИСПДн и АС пользователю запрещается:

а) самостоятельно подключать к АРМ нештатные устройства;

б) самостоятельно вносить изменения в состав, конфигурацию и размещение АРМ;

в) самостоятельно вносить изменения в состав, конфигурацию и настройку программного обеспечения, установленного в АРМ;

г) самостоятельно вносить изменения в размещение, состав и настройку СЗИ;

д) сообщать устно, письменно или иным способом другим лицам пароли, передавать личные идентификаторы, ключевые дискеты и другие реквизиты доступа к ресурсам ИСПДн и АС.

5. Пользователь ИСПДн и АС имеет право:

а) обращаться к ответственному за обеспечение безопасности ПДн в министерстве по вопросам защиты обрабатываемой в ИСПДн и АС информации и эксплуатации установленных СЗИ;

б) обращаться в службу технической поддержки с просьбой об оказании технической и методической помощи по использованию установленных программных и технических средств ИСПДн и АС;

в) обращаться к ответственному за организацию обработки ПДн в министерстве по вопросам, связанным с выполнением требований законодательства России в сфере ПДн.

6. Пользователь несет персональную ответственность за соблюдение требований законодательства Российской Федерации и локальных актов министерства, определяющих порядок обработки и защиты конфиденциальной информации, в том числе ПДн.

Приложение № 4
к приказу министерства сельского
хозяйства Тульской области
от 10.03.2017 № 8-осн.

ПОЛОЖЕНИЕ
об обеспечении безопасности персональных данных в министерстве сельского хозяйства Тульской области

г. Тула
2017 год

Содержание

Сокращения, условные обозначения, термины

АРМ	– автоматизированное рабочее место
БД	– база данных
ИБ	– информационная безопасность
ИС	– информационные системы
ИСПДн	– информационные системы персональных данных
ЛВС	– локальная вычислительная сеть
МЭ	– межсетевое экранирование
НСД	– несанкционированный доступ
ОС	– операционная система
ПДн	– персональные данные
ПО	– программное обеспечение
ПЭМИН	– побочные электромагнитные излучения и наводки
СЗПДн	– система защиты персональных данных
СКЗИ	– средства криптографической защиты информации
СУБД	– система управления базами данных
ФСТЭК России	– Федеральная служба по техническому и экспортному контролю Российской Федерации
ФСБ России	– Федеральная служба безопасности Российской Федерации

Введение

Настоящее Положение определяет состав мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн министерства сельского хозяйства Тульской области (далее Министерство), а также порядок их реализации и контроля эффективности.

Требования Положения распространяются на все отделы Министерства, а также на юридические лица и индивидуальных предпринимателей, осуществляющих сопровождение, обслуживание и обеспечение функционирования ИСПДн Министерства (далее обслуживающие организации).

Данное Положение разработано в соответствии со следующими нормативными документами:

- Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;
- Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- постановлением Правительства Российской Федерации от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами»;
- приказом ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- иными нормативными правовыми актами Российской Федерации, правовыми и методическими документами ФСТЭК России и ФСБ России.

1. Цель и область применения

Цель Положения – определение состава, порядка организации и проведения мероприятий по защите информации, содержащей персональные данные, обрабатываемые в Министерстве, для предотвращения ущерба в результате разглашения, утраты, утечки, искажения и уничтожения персональных данных, их незаконного использования и иных несанкционированных действий, приводящих к нарушениям работы ИСПДн Министерства.

Требования настоящего Положения обязательны для всех подразделений Министерства и распространяются на:

- ИСПДн Министерства;
- информационно-телекоммуникационную сеть;
- съемные машинные носители ПДн (далее носители ПДн);
- помещения, в которых ведется обработка ПДн;
- государственных гражданских служащих и работников Министерства, замещающих должности, не отнесенные к должностям государственной гражданской службы, (далее служащие и работники), органы исполнительной власти Тульской области, взаимодействующих с Министерством в процессе обработки ПДн, обслуживающие организации.

Новые документы, регламентирующие защиту персональных данных в Министерстве, должны разрабатываться с учетом настоящего Положения и не противоречить ему.

2. Состав мероприятий по обеспечению безопасности ПДн

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках существующей СЗПДн.

2.1. Организационные мероприятия по обеспечению безопасности ПДн

Организационные мероприятия по обеспечению безопасности ПДн включают в себя:

- распределение ответственности за реализацию мероприятий по обеспечению безопасности ПДн и контроль их эффективности. Разработка инструкций, регламентирующих функции и обязанности лиц, обеспечивающих безопасность ПДн в ИСПДн;
- определение перечня служащих и работников Министерства, участвующих в обработке ПДн или получивших к ним доступ. Определение необходимых правил доступа служащих и работников Министерства к ПДн;
- определение правил обработки ПДн в ИСПДн. Определение правил использования носителей ПДн;
- мероприятия по обеспечению физической безопасности ИСПДн;
- контроль за выполнением мероприятий по обеспечению безопасности ПДн;
- оказание консультаций служащим и работникам Министерства, обрабатывающим ПДн, а также лицам, ответственным за обеспечение безопасности ПДн.

2.2. Технические мероприятия по обеспечению безопасности ПДн

Технические мероприятия по обеспечению безопасности ПДн включают в себя:

- определение перечней ПДн, ИСПДн, носителей ПДн и технологии обработки ПДн;
- определение уровня защищенности ПДн для выявления базового набора мер по обеспечению безопасности ПДн;
- разработку частной модели угроз для выявления дополнительных мер по обеспечению безопасности ПДн с целью нейтрализации актуальных угроз;
- разработку и внедрение СЗПДн;
- периодические проверки функционирования и корректности настроек компонентов СЗПДн, аудит событий, генерируемых СЗИ;
- обработку инцидентов безопасности;
- регистрацию изменений в ИСПДн и СЗПДн, оценку их влияния на безопасность ПДн;

- восстановление ИСПДн и ПДн в случае возникновения обстоятельств, повлекших потерю данных или сбои в работе ИСПДн;
- оценку эффективности СЗПДн.

3. Порядок реализации мероприятий по обеспечению безопасности ПДн

3.1. Распределение ответственности за реализацию мероприятий по обеспечению безопасности ПДн

В Министерстве должно быть определено лицо, ответственное за обеспечение безопасности ПДн (далее ответственный за БПДн).

В целях организации работ по защите ПДн ответственный за БПДн осуществляет следующие функции:

- участвует в разработке, согласовании документов Министерства, регламентирующих защиту ПДн, а также внесении в них изменений;
- организовывает установку и настройку СЗИ;
- проводит контроль функционирования и корректности настроек СЗИ, отслеживает события, генерируемые СЗИ;
- участвует в проведении внутренних проверок по обеспечению безопасности ПДн;
- выявляет и обрабатывает инциденты информационной безопасности;
- выявляет слабые места в СЗПДн и вносит предложения по их устранению;
- иные функции, предусмотренные инструкцией ответственного за БПДн и инструкцией ответственного пользователя СКЗИ.

Для выполнения работ по обеспечению безопасности персональных данных при их обработке в информационной системе в соответствии с законодательством Российской Федерации могут привлекаться на договорной основе юридические лица или индивидуальные предприниматели, имеющие лицензию на деятельность по технической защите конфиденциальной информации.

Ответственный за БПДн в рамках проведения работ по обеспечению безопасности ПДн взаимодействует с ответственным за организацию обработки ПДн Министерства и обслуживающими организациями.

Служащие и работники Министерства, а также обслуживающие организации обязаны выполнять правила обеспечения безопасности, определенные в соответствующих инструкциях.

3.2. Определение состава ПДн, ИСПДн, носителей ПДн и технологии обработки ПДн

На данном этапе осуществляется сбор начальной информации, на основании которой должна строиться СЗПДн. Также необходимо периодическое проведение данных мероприятий для проверки актуальности имеющихся данных о составе

ПДн и ИСПДн. В случае изменения в составе, расположении или принципах взаимодействия элементов ИСПДн должна быть проведена оценка влияния данных изменений на безопасность ПДн.

3.2.1. Определение ПДн, обрабатываемых в ИСПДн Министерства

Устанавливаются все категории ПДн, которые обрабатываются в ИСПДн Министерства, цели и правовое обоснование обработки ПДн, соответствие содержания и объема обрабатываемых ПДн заявленным целям. Составляется перечень ПДн, обрабатываемых в ИСПДн.

3.2.2. Определение ИСПДн и ее сегментов, участвующих в хранении и обработке ПДн

Составляется перечень ИСПДн и ее сегментов. Для каждого сегмента определяются обрабатываемые ПДн, перечень программных и технических средств, схемы взаимодействия технических средств и их расположения.

3.2.3. Определение носителей ПДн

Необходимо определить, на каких носителях ПДн будет обрабатываться информация, содержащая ПДн. Составляется перечень носителей ПДн с указанием мест их хранения и сотрудников, работающих с данными носителями или имеющих к ним доступ.

3.2.4. Определение технологии обработки ПДн

Необходимо определить принцип взаимодействия элементов ИСПДн Министерства между собой, с ИСПДн органов исполнительной власти Тульской области, со сторонними ИС, в которых обрабатываются ПДн, а также каналы связи, участвующие в их взаимодействии. Учитываются как цифровые каналы связи, так и физические методы передачи данных на носителях ПДн. Устанавливается и описывается среда передачи данных с указанием используемых технологий, протоколов и лиц, ответственных за обеспечение безопасности ПДн при их передаче по каналам связи.

3.3. Определение порядка обработки ПДн в ИСПДн. Определение порядка работы с носителями ПДн

Необходимо определить стадии жизненного цикла обработки ПДн и требования по порядку обработки ПДн на каждом этапе. Этапы жизненного цикла обработки ПДн включают в себя:

3.3.1. Внесение ПДн в ИСПДн

На данном этапе осуществляется сбор информации, содержащей ПДн, и занесение ее в ИСПДн для последующей обработки.

При этом должны учитываться предъявляемые требования безопасности, в частности:

- собираться и заноситься в ИСПДн должны только те ПДн, которые необходимы для реализации функций Министерства;
- информация, содержащая ПДн, должна быть получена на законном основании или с согласия субъекта ПДн;
- должны регистрироваться факты внесения ПДн в ИСПДн.

3.3.2. Хранение ПДн

Хранение ПДн должно осуществляться в ИСПДн и на учтенных носителях ПДн, разрешенных к использованию в ИСПДн.

Должна быть обеспечена безопасность ПДн во время их хранения на носителях ПДн. Защита ПДн во время их хранения обеспечивается:

- подсистемой обеспечения физической защиты, в частности хранением носителей ПДн в защищенном месте (сейф, металлический шкаф);
- хранением ПДн в защищенном виде. Возможно использование криптографических средств защиты информации;
- использованием подсистемы разграничения доступа СЗПДн для исключения несанкционированного доступа к ПДн;
- резервированием ПДн на съемные машинные носители, хранящиеся в защищенном месте.

3.3.3. Предоставление доступа к ПДн

Защита ПДн в ИСПДн Министерства от НСД обеспечивается подсистемой разграничения доступа. Для возможности обработки ПДн служащим и работникам Министерства должны быть предоставлены необходимые права доступа к ним.

Порядок доступа к ПДн и элементам ИСПДн должен быть регламентирован соответствующим локальным документом.

Доступ к ПДн предоставляется служащим и работникам Министерства в соответствии с их должностными обязанностями, а также по заявке, содержащей указание необходимости получения прав доступа и утвержденной руководителем Министерства.

Изменение прав доступа к ПДн должно фиксироваться в разрешительной системе доступа.

3.3.4. Уничтожение ПДн

Уничтожение ПДн осуществляется в соответствии с установленными правилами обработки ПДн.

Факты уничтожения ПДн должны актироваться с указанием сотрудников, осуществлявших уничтожение, перечня удаленных данных, а также причины и даты удаления.

3.4. Определение порядка доступа к ПДн служащих и работников Министерства

Необходимо определить, в рамках каких работ и функциональных обязанностей служащим и работникам необходимо предоставление доступа к ПДн. Определяется перечень служащих и работников, выполняющих данные работы и их роли, в соответствии с которыми назначаются требуемые права доступа. Определяется тип и срок предоставления доступа к ПДн для выполнения функциональных обязанностей. В результате составляется разрешительная система доступа к ресурсам ИСПДн.

3.5. Определение уровня защищенности ИСПДн

На основании постановления Правительства Российской Федерации от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» определяется уровень защищенности ИСПДн Министерства. Для определения уровня защищенности формируется комиссия, состоящая из представителей Министерства. Допускается включение в состав комиссии сотрудников сторонних организаций, имеющих лицензию на деятельность по технической защите конфиденциальной информации.

В соответствии с уровнем защищенности определяется перечень базовых мер по обеспечению безопасности ПДн на основании приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

3.6. Разработка частной модели угроз

На основании методических документов ФСТЭК России и ФСБ России разрабатывается частная модель угроз ПДн. Данный документ описывает актуальные угрозы ПДн Министерства, показатели их опасности и возможность реализации, а также набор дополнительных мер по обеспечению безопасности ПДн, выполнение которых необходимо для нейтрализации актуальных угроз.

Частная модель угроз направляется на рассмотрение в Управление ФСТЭК России по Центральному федеральному округу.

3.7. Разработка, внедрение, эксплуатация и контроль эффективности СЗПДн

СЗПДн состоит из следующих подсистем:

- подсистема разграничения доступа субъектов доступа (пользователи и процессы) к объектам доступа (информационные и технические ресурсы), предотвращающая несанкционированный доступ к ПДн;
- подсистема межсетевого экранирования, позволяющая реализовать сегментацию ЛВС и управление сетевым взаимодействием;
- подсистема регистрации и учета действий пользователей в ИСПДн;
- подсистема обеспечения целостности ПДн и ИСПДн;
- подсистема антивирусной защиты, позволяющая выявлять и устранять угрозы, связанные с вредоносным ПО;
- подсистема криптографической защиты ПДн;
- подсистема выявления уязвимостей в СЗПДн ИСПДн;
- подсистема физической защиты ПДн и элементов ИСПДн от несанкционированного доступа к ним.

Используемые в СЗПДн СЗИ должны пройти процедуру оценки соответствия в рамках сертификации ФСТЭК России и ФСБ России. На этапе внедрения и в процессе эксплуатации СЗПДн должен вестись учет используемых средств защиты. Необходимо определить правила проведения проверок функционирования и корректности настроек компонентов СЗПДн, обработки генерируемых ими событий.

3.7.1. Защита ПДн от НСД

Защита ПДн от НСД обеспечивается использованием мер по ограничению несанкционированного доступа к ПДн. Эффективность используемых мер достигается при условии соблюдения установленного порядка обработки ПДн в ИСПДн, что обеспечивается выполнением требований регламентирующих документов и инструкций по работе в ИСПДн.

3.7.1.1. Подсистема разграничения доступа и подсистема межсетевого экранирования

Система управления доступом позволяет регистрироваться в системе только авторизованным пользователям, при этом для авторизации используется сочетание логина, пароля и физического (iButton, eToken, RuToken) или программного ключа (файл .dst), что снижает вероятность несанкционированного доступа в случае компрометации каких-либо авторизационных данных.

Дополнительно осуществляется ограничение прав пользователей до минимально необходимых, что снижает возможность использования альтернативных способов получения доступа к ПДн.

Подсистема управления доступом внедряется на АРМ сотрудников, участвующих в обработке ПДн, и в системах, в которых обрабатываются ПДн.

В рамках подсистемы управления доступом используются встроенные механизмы операционной системы Microsoft Windows, позволяющие осуществлять управление доступом сотрудников на рабочие станции, серверы, к файлам и таблицам БД, хранящимся в СУБД.

Должны быть реализованы системы разграничения доступа к модулям управления подсистем СЗПДн, позволяющие осуществлять безопасную авторизацию, в том числе удаленных пользователей в случае необходимости, и предотвратить получение несанкционированного доступа к средствам администрирования СЗПДн.

Используемые подсистемы МЭ позволяют предотвратить доступ в ИСПДн из других сегментов ИСПДн Министерства, ИСПДн органов исполнительной власти Тульской области, из внешней сети Интернет и с неавторизованных узлов. Также подсистема МЭ позволяет установить набор правил доступа, предотвращающих какой-либо вид доступа, кроме установленного и необходимого для функционирования ИСПДн.

Для защиты ПДн от НСД в ИСПДн используются средства обнаружения вторжения. В качестве таких средств должны применяться системы обнаружения и предотвращения атак, позволяющие своевременно обнаруживать несанкционированную сетевую активность и попытки несанкционированного доступа.

Подсистемы межсетевого экранирования используются на границах сегментов ЛВС и АРМ правительства Тульской области.

Внедрение подсистем управления доступом и межсетевого экранирования осуществляется в соответствии со стандартами и правилами их настройки ответственными за БПДн.

3.7.1.2. Подсистема физической защиты ПДн и ИСПДн от НСД к ним

Доступ в помещения, где ведется обработка ПДн и располагаются элементы ИСПДн, должен осуществляется в соответствии с, установленным в Министерстве, порядком доступа в помещения, в которых ведется обработка ПДн.

При этом должны выполняться следующие требования по обеспечению физической защиты ПДн:

- определение контролируемой зоны;
- введение пропускного режима доступа в контролируемую зону;

- внедрение системы физического контроля и учета доступа в охраняемые помещения;
- использование мер обеспечения физической защиты охраняемых помещений;
- использование мер обеспечения физической безопасности элементов ИСПДн и носителей ПДн.

Весь предоставляемый в контролируемую зону, в охраняемые помещения, к элементам ИСПДн и носителям ПДн физический доступ должен протоколироваться.

За выполнение мер обеспечения физической безопасности в подразделениях Министерства ответственность несет руководитель Министерства или лицо, исполняющее его обязанности. Контроль выполнения требований по обеспечению физической безопасности осуществляет лицо, назначенное руководителем Министерства.

3.7.1.3. Подсистема обеспечения целостности ПДн и ИСПДн

Обеспечение целостности ПДн и элементов ИСПДн и СЗПДн обеспечивается с помощью следующих мер:

- осуществление резервного копирования ПДн и критичных данных ИСПДн;
- осуществление мониторинга системных изменений и модификации данных;
- осуществление резервирования критичных узлов и подсистем обеспечения жизнедеятельности ИСПДн.

Необходимо осуществлять регулярное резервное копирование критичной информации. К критичной информации относятся:

- ПДн;
- конфигурационные файлы подсистем ИСПДн и СЗПДн;
- журналы аудита;
- информационное обеспечение ИСПДн и СЗПДн.

Резервные копии данных сохраняются на съемные носители информации. Носители с резервными копиями хранятся в защищенном месте, отличном от места размещения системных элементов ИСПДн.

Для осуществления резервного копирования информации используется сертифицированный программно-аппаратный комплекс резервирования и восстановления, поддерживающий все используемые в ИСПДн платформы и позволяющий вести библиотеку резервных копий с возможностью оперативного поиска и восстановления данных.

Настройка и использование подсистемы резервного копирования осуществляется ответственными сотрудниками в соответствии со стандартами настройки и инструкцией по выполнению резервного копирования.

Резервное копирование осуществляется в соответствии с регламентом резервного копирования, который должен определять данные для резервирования, периодичность и время копирования, а также периодичность цикла хранения резервных копий.

Ответственность за выполнение резервного копирования несут системный администратор и ответственный за БПДн Министерства.

В целях выявления фактов нарушения целостности необходимо осуществлять мониторинг системных изменений и модификации данных.

Подсистемы контроля целостности должны сигнализировать о модификации данных или среды их обработки, позволяя выявлять факты нарушения целостности и производить восстановление информации с резервных копий в случае необходимости.

В качестве подсистемы контроля целостности используется сертифицированный программно-аппаратный комплекс защиты от НСД, позволяющий осуществлять контроль нарушения целостности на всех уровнях ИС.

Для программно-аппаратных подсистем СЗПДн контроль целостности конфигурации должен осуществляться с помощью регулярного аудита, в том числе рассмотрения журналов доступа и изменений, а также проверки контрольных сумм файлов конфигурации.

Должна быть настроена система автоматизированного экстренного оповещения ответственных сотрудников о фактах нарушения целостности.

Настройка подсистемы контроля целостности осуществляется ответственными сотрудниками в соответствии со стандартами настройки.

Ответственность за контроль целостности и реагирование на факты нарушения целостности несут системный администратор и ответственный за БПДн Министерства.

В целях предотвращения аппаратных и программных сбоев элементов ИСПДн и возможной потери данных необходимо обеспечить резервирование критичных узлов и систем обеспечения их функционирования.

ПДн и критичные данные должны храниться и обрабатываться на отказоустойчивых электронных массивах хранения информации (применяется технология RAID).

Рекомендуется реализовать резервирование критичных ИС, используемых для обработки ПДн, и каналов связи.

Необходимо использовать источники бесперебойного питания, позволяющие корректно завершить работу ИС без потери данных.

3.7.1.4. Подсистема регистрации и учета

Использование подсистемы регистрации и учета позволяет осуществлять протоколирование фактов и попыток доступа к ПДн, а также осуществлять учет

потоков и носителей ПДн. Данные записи могут быть использованы при расследовании инцидентов ИБ, а также в качестве дополнительной защиты от НСД.

Необходимо осуществлять регистрацию всех удачных и неудачных попыток осуществления доступа к ПДн как логическим, так и к физическим компонентам ИСПДн.

Необходима регистрация следующих данных:

- ИС, к которой осуществляется доступ;
- тип доступа;
- лицо, осуществляющее попытку доступа;
- данные или компонент, к которому осуществляется доступ;
- временная метка доступа;
- результат попытки доступа.

Должны регистрироваться и учитываться носители информации, содержащие ПДн. Учет носителей позволяет реализовать требования режима обработки и хранения ПДн, назначать сотрудников, ответственных за обеспечение безопасности конкретных носителей, осуществлять контроль использования и передачи ПДн.

В качестве технических мер в области регистрации и учета используется программно-аппаратный комплекс защиты от несанкционированного доступа, позволяющий вести детальную регистрацию действий пользователей в системе. Также используются встроенные системы протоколирования ОС Windows.

Настройка систем регистрации и учета осуществляется ответственными сотрудниками в соответствии со стандартами настройки и инструкциями по управлению данными системами.

Для регистрации и учета физического доступа, а также учета носителей ПДн используются журналы учета доступа в бумажном или в электронном виде.

Учет физического доступа осуществляется в соответствии с порядком предоставления физического доступа. Учет носителей ПДн осуществляется в соответствии с порядком использования носителей ПДн.

За выполнение мер регистрации и учета ответственность несет ответственный за БПДн.

3.7.1.5. Подсистема антивирусной защиты

Необходимо обеспечить защиту ПДн и ИС, участвующих в их обработке и хранении, от вредоносного ПО. Для предотвращения угрозы несанкционированного доступа с использованием вредоносного ПО в ИСПДн используется подсистема антивирусной защиты.

Подсистема антивирусной защиты обеспечивает постоянную защиту ПДн, ПО и среды их обработки от воздействия вредоносного ПО. В рамках антивирусной защиты реализуются следующие действия:

- обнаружение вредоносных объектов в ОС и среде обработки данных;
- обнаружение вредоносных объектов в исполняемых файлах и процессах;
- сканирование и обнаружение вредоносных объектов в файловой системе;
- мониторинг удаленных подключений и обнаружение вредоносных объектов в передаваемых файлах;
- нейтрализация угроз от вредоносных объектов в соответствии с выбранными настройками (лечение, удаление, блокирование).

Должно выполняться регулярное обновление базы сигнатур вредоносных объектов для обеспечения требуемого уровня защиты.

В качестве подсистемы антивирусной защиты используется программный комплекс защиты от вредоносного ПО.

Настройка подсистемы антивирусной защиты осуществляется ответственными сотрудниками в соответствии со стандартами настройки и инструкциями по управлению данными системами.

Ответственность за обеспечение защиты ПДн от воздействия вредоносного ПО несет ответственный за БПДн.

3.7.1.6. Подсистема криптографической защиты

В целях защиты ПДн от НСД при их хранении и передаче используется подсистема криптографической защиты. Данная подсистема позволяет обеспечить безопасность ПДн даже в случае получения несанкционированного доступа к ним во время хранения и передачи.

В качестве подсистемы криптографической защиты используются сертифицированные средства.

Использование данных средств защиты позволяет реализовать безопасную передачу и хранение ПДн.

Настройка и использование подсистемы криптографической защиты осуществляется ответственными сотрудниками в соответствии со стандартами настройки и инструкциями по управлению данными системами.

Управление криптографическими ключами осуществляется в соответствии с установленным регламентом.

3.7.2. Защита ПДн от ПЭМИН и утечек по техническим каналам

Для исключения утечки ПДн за счет ПЭМИН в ИСПДн реализуются следующие мероприятия:

- использование сертифицированных средств защиты информации;

- размещение объектов защиты на максимально возможном расстоянии относительно границы защищаемой территории;
- контроль защищаемой территории на предмет обнаружения устройств несанкционированного съема информации.

В ИСПДн для обработки информации рекомендуется использовать средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, безопасности и эргономическим требованиям к средствам отображения информации, и санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (ГОСТ 29216-91, ГОСТ Р 50948-96, ГОСТ Р 50949-96, ГОСТ Р 50923-96, СанПиН 2.2.2.542-96).

Для исключения просмотра текстовой и графической видовой информации, выводимой устройствами отображения информации средств вычислительной техники, информационно-вычислительных комплексов, технических средств обработки графической, видео- и буквенно-цифровой информации, входящих в состав ИСПДн, рекомендуется оборудовать помещения, в которых они установлены, шторами (жалюзи).

3.7.3. Проверка функционирования и корректности настроек компонентов СЗПДн, аудит событий, генерируемых компонентами СЗПДн

Проверка функционирования и корректности настроек компонентов СЗПДн, аудит событий, генерируемых компонентами СЗПДн, позволяют заблаговременно выявить и своевременно устранить потенциальные уязвимости СЗПДн. Необходимо проводить регулярный мониторинг состояния СЗПДн, полноты и достаточности мер по защите ПДн.

3.7.3.1. Мониторинг состояния СЗПДн

Мониторинг состояния СЗПДн позволяет своевременно выявить и предотвратить сбои в работе компонентов СЗПДн, а также обнаружить нарушения ИБ, связанные с некорректной настройкой подсистем СЗПДн. Данный процесс включает в себя:

- мониторинг состояния компонентов СЗПДн. Позволяет выявлять отклонения в условиях функционирования аппаратных или программных компонентов СЗПДн и осуществляется непосредственно ответственными за БПДн или с помощью ПО, предназначенного для контроля отклонений в функционировании СЗПДн;
- аудит настроек компонентов СЗПДн. Осуществляется ответственными за БПДн на ежеквартальной основе и представляет собой процесс проверки соответствия реальных настроек компонентов СЗПДн установленным требованиям.

3.7.3.2. Аудит событий, генерируемых компонентами СЗПДн

Аудит событий, генерируемых компонентами СЗПДн, направлен на обнаружение фактов и попыток (преднамеренного и непреднамеренного) нарушения информационной безопасности ПДн пользователями. Данная мера позволяет выявить нарушителей, создает информационную базу, необходимую для расследования инцидентов безопасности, и позволяет обнаруживать потенциальные уязвимости в ИСПДн.

Аудит событий, генерируемых компонентами СЗПДн, осуществляется автоматизировано с использованием подсистем регистрации и учета, подсистемы контроля целостности, а также подсистем управления доступом и межсетевого экранирования. В данной подсистеме должны быть настроены автоматизированные действия по информированию ответственных за БПДн о событиях, важных с точки зрения ИБ. Настройка оповещений осуществляется в соответствии со стандартами конфигурации данных подсистем. Необходимо осуществлять регулярную проверку событий в СЗПДн для выявления событий, не учтенных автоматизированной системой оповещения.

3.7.3.3. Тестирование средств и процедур безопасности

Тестирование средств и процедур безопасности направлено на выявление существующих или потенциальных уязвимостей ИСПДн и СЗПДН, определение полноты применяемых мер по защите ПДн. Тестирование состоит из анализа защищенности ИСПДн с помощью автоматизированных средств, а также системного анализа состояния ИСПДн и СЗПДн и мер по обеспечению безопасности ПДн.

Автоматизированный анализ защищенности ИСПДн осуществляется с помощью сетевого сканера безопасности, позволяющего выявлять уязвимости в используемых ИС. Данная процедура выполняется ответственным за БПДн в соответствии с регламентом анализа защищенности.

Анализ состояния ИСПДн и СЗПДн включает в себя:

- мониторинг актуальности используемого ПО и появления новых уязвимостей в нем для своевременного обновления и принятия необходимых мер по обеспечению безопасности;
- анализ существующих рекомендаций и стандартов по обеспечению безопасности используемых ИС и поддержание имеющихся стандартов по настройке и оперированию ИС в актуальном состоянии;
- регулярный анализ и пересмотр имеющихся процедур обеспечения безопасности ПДн.

3.8. Порядок реагирования на инциденты информационной безопасности

В целях защиты ПДн при выявлении инцидента безопасности определяется порядок реагирования на угрозы нарушения безопасности, который позволит максимально снизить возможные последствия и своевременно устранить инцидент.

Процедура реагирования на инциденты информационной безопасности состоит из следующих стадий:

- обнаружение инцидента;
- регистрация инцидента;
- обработка инцидента;
- уведомление необходимых лиц о произошедшем инциденте;
- устранение инцидента информационной безопасности;
- анализ инцидента.

3.8.1. Обнаружение инцидента ИБ

Инцидент информационной безопасности может быть обнаружен и зафиксирован следующими лицами:

- системным администратором ИС в ходе анализа недоступности информационной системы или отдельных сервисов;
- ответственным за БПДн.

Предположение об инциденте информационной безопасности делается на основе следующих событий:

- об инциденте сообщают сотрудники;
- в ходе мониторинга или аудита ИСПДн или СЗПДн обнаруживается явный инцидент ИБ;
- в ходе анализа файлов журнала регистрации событий делается вывод о возможности инцидента ИБ;
- сообщений подсистемы аудита событий, генерируемых компонентами СЗПДн, или подсистемы обнаружения вторжений.

Обо всех событиях, которые пользователь классифицирует как нарушение нормального функционирования информационной системы, сотрудник сообщает ответственному за БПДн.

3.8.2. Регистрация инцидента ИБ

Инцидент должен быть зарегистрирован в журнале регистрации инцидентов с пометкой «инцидент информационной безопасности».

При регистрации инцидента должны быть зафиксированы следующие сведения:

- Ф.И.О. сотрудника, обнаружившего инцидент;
- дата обнаружения;

- время обнаружения;
- сервис информационной безопасности, к которому относится инцидент;
- краткое описание инцидента.

3.8.3. Обработка инцидента ИБ

Под обработкой инцидента ИБ понимаются следующие действия:

- сбор дополнительной информации об инциденте ИБ;
- определение приоритета зарегистрированного инцидента ИБ.

Ответственный за БПДн обязан осуществить сбор дополнительной информации о зарегистрированном инциденте. К такой информации относятся:

- журналы событий;
- описание последовательности действий, которые привели к возникновению инцидента;
- статистика по аналогичным инцидентам, в том числе зарегистрированным за последний месяц (квартал).

Ответственный за БПДн обязан установить приоритет зарегистрированного инцидента, в соответствии с которым определяется время реагирования на инцидент и устранения его последствий, а также определяется план действий.

В случае регистрации инцидента, повлекшего разглашение ПДн, формируется комиссия для анализа, расследования и устранения инцидента.

3.8.4. Уведомление заинтересованных лиц о произошедшем инциденте ИБ

После регистрации инцидента производится уведомление ответственного за организацию обработки персональных данных в Министерстве, руководителя Министерства, а также лиц, ответственных за устранение инцидента информационной безопасности. В зависимости от приоритета инцидента и возможных последствий нарушения информационной безопасности руководителем Министерства дополнительно извещаются заинтересованные лица.

3.8.5. Устранение инцидента ИБ

Согласно выполненной классификации инцидента выбирается соответствующая процедура по устранению данного инцидента (предварительно разработанная и задокументированная).

Определяются сотрудники, ответственные за устранение инцидента.

Если процедуры устранения данного вида инцидентов не существует, то ответственный работник обязан ликвидировать его на основе имеющихся знаний, умений и навыков либо подключить других компетентных работников. При этом все действия, необходимые для устранения инцидента информационной безопасности, документируются.

Мероприятия по устранению последствий реализации угроз безопасности ПДн и проведению работ по восстановлению нормального функционирования ИСПДн могут включать в себя:

- восстановление данных и ПО с резервных копий;
- антивирусные мероприятия при возникновении вирусных заражений;
- смену паролей;
- восстановление настроек ИС (права доступа, настройки безопасности, настройки обеспечения взаимодействия ИС и т. д.);
- анализ и устранение выявленных уязвимостей;
- восстановление или замену аппаратных элементов ИСПДн.

Сотрудник, назначенный ответственным за устранение инцидента, обязан внести информацию о его ликвидации в Журнал регистрации инцидентов информационной безопасности.

Инцидент считается исчерпанным, когда ответственный сотрудник согласно своей компетентной оценке выполнил все необходимые действия для устранения возможных и текущих проблем, связанных с инцидентом, а заявитель получил извещение о решении инцидента и подтвердил его успешное решение.

3.8.6. Анализ инцидента ИБ

Анализ инцидентов информационной безопасности проводит ответственный за БПДн. Под анализом инцидента информационной безопасности понимаются следующие действия:

- поиск причины возникновения инцидента;
- классификация инцидента как умышленного или неумышленного;
- идентификация нарушителя;
- сбор доказательств совершения инцидента;
- привлечение правоохранительных органов (в случае необходимости);
- анализ статистики подобных инцидентов;
- определение последствий инцидента информационной безопасности.

Для поиска причины возникновения инцидента, а также для дальнейшего расследования документируются все факты и доказательства произошедшего инцидента информационной безопасности, в том числе следующие данные:

- технические – информация, полученная от технических средств сбора и анализа данных (снифферы, IDS/IPS и др.);
- операционные – данные, собранные в процессе опроса сотрудников Министерства.

Сбор доказательств совершения инцидента необходим для:

- привлечения к ответственности лиц за умышленные или непреднамеренные действия;
- анализа уязвимости информационной системы;

- ликвидации последствий инцидента информационной безопасности.

При классификации инцидента как умышленного производятся мероприятия по идентификации личности нарушителя.

Определение последствий инцидента информационной безопасности подразумевает оценку нанесенного ущерба, если его возможно представить в количественном виде.

После завершения устранения и анализа инцидента информационной безопасности по инициативе ответственного сотрудника может проводиться обсуждение его результатов совместно со всеми привлеченными и заинтересованными сторонами. По итогам обсуждения комиссия по расследованию инцидента делает соответствующие выводы об уязвимостях и угрозах информационной безопасности, а также определяет необходимые мероприятия по недопущению подобных инцидентов в будущем. Соответствующие выводы документируются и хранятся у ответственного за БПДн в Министерстве.

Ответственный за БПДн в Министерстве обеспечивает надежное защищенное хранение информации о произошедших инцидентах информационной безопасности. Доступ к данным сведениям других сотрудников возможен только в соответствии с их должностными обязанностями.

3.9. Оценка эффективности реализованных в рамках СЗПДн мероприятий по обеспечению безопасности ПДн

В соответствии с пунктом 4 части 2 статьи 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» в рамках мероприятий по обеспечению безопасности необходимо провести оценку эффективности СЗПДн. Оценка эффективности проводится в форме первичной аттестации информационной системы по требованиям защиты информации и периодических проверок эффективности СЗПДн.

4. Порядок пересмотра

Внесение изменений в Положение может носить как регламентный характер, так и быть вызвано изменениями в системе информационной безопасности или нормативных документах.

Пересмотр Положения производится в следующих случаях:

- изменение законодательства в области защиты ПДн;
- регламентный пересмотр Положения;
- внесение изменений в регламентные документы Министерства;
- внесение изменений в ИСПДн.

В случае внесения изменений в законодательство в области защиты ПДн необходимо провести пересмотр Положения для оценки его соответствия новым требованиям.

Регламентный пересмотр Положения производится раз в год и обусловлен необходимостью соответствия Положения текущему состоянию ИСПДн и используемых методов защиты ПДн.

Положение разрабатывается на основе концептуальных документов по информационной безопасности. В случае изменения взглядов на проблему защиты ПДн или целей обеспечения безопасности ПДн вносятся поправки в концептуальные нормативные документы и, как следствие, требуется пересмотр Положения.

В случае внесения изменений в ИСПДн Положение должно быть дополнено и/или исправлено, чтобы отвечать текущему состоянию ИСПДн.

При внесении изменений в Положение проводятся следующие мероприятия:

- обследование и анализ изменений в ИСПДн в целом, в СЗПДн, в системе нормативных и регламентных документов;
- внесение изменений в перечень защищаемых объектов и ресурсов (при необходимости);
- формулировка и описание дополнительных (измененных) требований к СЗПДн, мер и процедур защиты ПДн;
- утверждение изменений в Положении.

Приложение № 5
к приказу министерства сельского
хозяйства Тульской области
от 10.03.2017 № 8-осн.

ИНСТРУКЦИЯ
пользователя средств криптографической защиты информации в министерстве сельского хозяйства Тульской области

1. Настоящая инструкция регламентирует обязанности и права пользователя средств криптографической защиты информации (далее – СКЗИ) в работе по обеспечению безопасности средств криптографической защиты информации и эксплуатации СКЗИ в министерстве сельского хозяйства Тульской области.

2. Доступ к криптосредствам предоставляется только после соответствующего обучения пользователей работе с криптосредствами.

3. Пользователь криптосредств обязан:

не разглашать информацию, к которой он допущен, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

не допускать снятия копий с ключевых документов, вывода ключевых документов на дисплей (монитор) персональной электронно-вычислительной машины (далее – ПЭВМ) или принтер;

не допускать записи на ключевой носитель посторонней информации;

не допускать установки ключевых документов в другие ПЭВМ;

соблюдать требования по обеспечению безопасности конфиденциальной информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

сообщать о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ и ключевых документах к ним;

немедленно уведомлять ответственного пользователя СКЗИ о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к раскрытию защищаемой конфиденциальной информации;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы ответственному пользователю СКЗИ под запись в журналах учета при увольнении или отстранении от исполнения обязанностей, связанных с использованием СКЗИ.

4. Пользователь криптосредств имеет право:

обращаться к ответственному пользователю СКЗИ с просьбой об оказании технической и методической помощи по использованию установленных средств криптографической защиты информации;

передавать криптоключи на хранение ответственному пользователю СКЗИ.

5. Передача и хранение криптосредств.

Криптосредства, эксплуатационная и техническая документация, правила пользования и ключевые документы между пользователями не передаются.

Хранение ключевых документов пользователям криптосредств должно осуществляться в надежно запираемых шкафах (ящики, сейфы) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним.

О нарушениях, которые могут привести к компрометации криптоключей или передаче (хранению) с их использованием информации, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств.

6. События, квалифицируемые как явная компрометация ключей:

утрата ключевых носителей;

утрата ключевых носителей с последующим обнаружением;

увольнение работников, имевших доступ к ключевой информации;

нарушение печати на сейфе с ключевыми носителями;

нарушение правил хранения и уничтожения (после окончания срока действия) ключевой информации;

случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате несанкционированных действий злоумышленника).

7. К событиям, квалифицируемым как подозрение наличия факта компрометации криптографического ключа и требующим проведения расследования и принятия решения на предмет происшествия явной компрометации, относится возникновение подозрений в утечке информации в системе защищенной связи.

8. Лица, виновные в нарушении правил пользования криптосредствами, могут быть привлечены к административной или дисциплинарной ответственности.

Приложение № 6
к приказу министерства сельского
хозяйства Тульской области
от 10.03.2017 № 8-осн.

ИНСТРУКЦИЯ
по порядку использования и организации работы со средствами криптографической защиты информации в министерстве сельского хозяйства Тульской области

1. Общие положения

1.1. Настоящая инструкция устанавливает единые требования по обеспечению безопасности функционирования средств криптографической защиты информации (далее – СКЗИ), эксплуатации СКЗИ в министерстве сельского хозяйства Тульской области (далее – министерство) и определяет порядок учета, выдачи, хранения, уничтожения СКЗИ, а также действия при компрометации ключей.

1.2. Инструкция разработана в соответствии с:

Федеральным законом от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) от 13 июня 2001 года № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащих сведений, составляющих государственную тайну»;

Приказом Федеральной службы безопасности Российской Федерации от 09 февраля 2005 года № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;

Приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года № 378 «Об утверждении 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».

1.3. В настоящей инструкции использована следующая терминология:

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

Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или АС, от внутренних или внешних угроз.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Защита информации – деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Криптографическая (шифровальная) защита – защита информации от ее несанкционированного доступа и модификации посторонними лицами при помощи алгоритмов криптографического преобразования.

Контролируемая зона – пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и (или) транспортных средств.

Конфиденциальность – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Компрометация ключа – хищение, утрата, разглашение, несанкционированное копирование и другие происшествия, в результате которых криптоключи могут стать доступными несанкционированным лицам и (или) процессам.

Ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Ключевой документ (криптоключ) – сохраняемая в тайне, закрытая информация, используемая криптографическим алгоритмом при шифровании/расшифровании сообщений, постановке и проверке электронной подписи (далее – ЭП), вычислении кодов аутентичности.

Криптосредство – шифровальное (криптографическое) средство, предназначенное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности к криптосредствам относятся СКЗИ – шифровальные (криптографические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Сертификат ключа проверки электронной подписи – электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность

ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.

Шифровальные (криптографические) средства:

а) средства шифрования – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

б) средства имитозащиты – аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной подписи – аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;

г) средства кодирования – средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации);

е) ключевые документы (независимо от вида носителя ключевой информации).

Несанкционированный доступ (НСД) – доступ, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка информации – совокупность операций сбора, накопления, ввода-вывода, приема-передачи, записи, хранения, регистрации, уничтожения, преобразования и отображения, осуществляемых над информацией.

Ответственный пользователь – должностное лицо, назначенное ответственным за обеспечение функционирования и безопасности криптосредств в министерстве.

Пользователь криптосредств – субъект, наделенный правом применения средства криптографической защиты для выполнения возложенных обязанностей.

Среда функционирования криптосредства – совокупность технических и программных средств, совместно с которыми предполагается штатное функционирование криптосредства и которые способны повлиять на выполнение предъявляемых к криптосредству требований.

Средство защиты информации – техническое, программное средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Удостоверяющий центр – юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом.

Электронный документ – документ, в котором информация представлена в электронно-цифровой форме.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения лица, подписывающего информацию.

2. Организационные требования

2.1. Государственные гражданские служащие и работники министерства, замещающие должности, не отнесенные к должностям государственной гражданской службы (далее – служащие и работники), использующие при работе СКЗИ, должны быть ознакомлены с требованиями настоящей инструкции и другими документами, регламентирующими обеспечение безопасности функционирования СКЗИ. Эти служащие и работники несут персональную ответственность за несоблюдение требований указанных документов в соответствии с законодательством Российской Федерации.

2.2. Обеспечение функционирования и безопасности СКЗИ в министерстве возлагается на ответственного пользователя СКЗИ, имеющего необходимый уровень квалификации и назначаемого приказом министра. Функция ответственного пользователя частично может быть возложена на основании договора на стороннюю организацию – лицензиата ФСБ России. Ответственный пользователь СКЗИ должен обладать необходимым уровнем квалификации для обеспечения защиты конфиденциальной информации с использованием СКЗИ.

2.3. Ответственный пользователь СКЗИ осуществляет:

обучение лиц, использующих СКЗИ, правилам работы с ними;

проверку готовности пользователей СКЗИ к самостоятельному использованию СКЗИ и составление заключений о возможности эксплуатации СКЗИ (с указанием типа и номеров используемых СКЗИ, номеров аппаратных, программных и аппаратно-программных средств, где установлены или к которым подключены СКЗИ, с указанием номеров печатей (пломбиров), которыми опечатаны (опломбированы) технические средства, включая СКЗИ, и результатов проверки функционирования

СКЗИ);

поэкземплярный учет используемых СКЗИ, эксплуатационной и технической документации к ним;

учет лиц, непосредственно допущенных к работе со средствами криптографической защиты информации (пользователей СКЗИ);

поддержание в актуальном состоянии перечня пользователей СКЗИ;

контроль за соблюдением условий использования СКЗИ, предусмотренных эксплуатационной и технической документацией к СКЗИ;

подачу заявок в удостоверяющий центр на изготовление ключевых документов или исходной ключевой информации;

разбирательство и составление заключений по фактам нарушения условий хранений носителей конфиденциальной информации, использования СКЗИ, которые могут привести к нарушению или к снижению уровня защищенности информации;

принятие мер по минимизации возможных последствий при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т. п.;

разбирательства по фактам нарушения условий хранения и использования СКЗИ.

2.4. К работе с СКЗИ пользователи допускаются решением министра для исполнения обязанностей, связанных с использованием СКЗИ. Пользователи несут персональную ответственность за сохранность СКЗИ, ключевой, эксплуатационной и технической документации.

2.5. Пользователи СКЗИ (ответственный пользователь СКЗИ) обязаны:

не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ, ключевых документах к ним и других мерах защиты;

не допускать снятия копий с ключевых документов, вывода ключевых документов на дисплей (монитор) ПЭВМ или принтер, записи на ключевой носитель посторонней информации, установки ключевых документов на другие ПЭВМ;

соблюдать требования по обеспечению безопасности конфиденциальной информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

сообщать о ставших им известными попытках посторонних лиц получить сведения об используемых СКЗИ и ключевых документах к ним;

немедленно уведомлять руководство министерства о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к несанкционированному доступу к защищаемой конфиденциальной информации;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы ответственному пользователю СКЗИ под запись в журналах учета при увольнении или отстранении от исполнения обязанностей, связанных с

использованием СКЗИ.

2.6. Пользователи СКЗИ могут быть допущены к работе с СКЗИ только после соответствующего обучения. Обучение пользователей правилам работы с СКЗИ осуществляет ответственный пользователь СКЗИ. Документом, подтверждающим должную специальную подготовку пользователей и возможность их допуска к самостоятельной работе с СКЗИ, является заключение, оформленное в виде акта на основании принятых от этих лиц зачетов.

2.7. Установка криптографических средств, настройка криптоключей и сертификатов осуществляется по заявке ответственного пользователя криптосредств или служащего (работника) министерства, поданной в службу технической поддержки. После установки, настройки и проверки работоспособности криптографических средств составляется акт установки и ввода в эксплуатацию криптосредств (криптоключей).

2.8. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями криптосредств и ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Передача учтенных СКЗИ без санкции ответственного пользователя категорически запрещается.

2.9. В помещениях, в которых размещена информационная система, необходима организация режима обеспечения безопасности помещений, препятствующая возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения.

2.10. Текущий контроль за организацией и обеспечением функционирования СКЗИ возлагается на министра и ответственного пользователя СКЗИ в пределах их служебных полномочий.

3. Порядок учета и выдачи средств криптографической защиты информации

3.1. Служащие и работники министерства, допущенные к работе с СКЗИ, подлежат обязательному учету. Ответственный пользователь СКЗИ в министерстве ведет на каждого пользователя СКЗИ лицевой счет (приложение № 1), в котором регистрирует числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы. Лицевые счета и пользователи учитываются в журнале лицевых счетов (журнал пользователей СКЗИ) (приложение № 2).

3.2. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учету в журнале поэкземплярного учета (приложение № 3). При этом программные СКЗИ должны учитываться с аппаратными средствами, вместе с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие СКЗИ учитываются совместно с соответствующими

аппаратными средствами. Единицей поэкземплярного учета ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

3.3. Все полученные экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учета пользователям СКЗИ. Пользователи несут персональную ответственность за их сохранность.

3.4. Все необходимые для работы экземпляры СКЗИ, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в журнале поэкземплярного учета пользователям СКЗИ, несущим персональную ответственность за их сохранность.

3.5. Если в эксплуатационной и технической документации к СКЗИ предусмотрено применение разовых ключевых носителей или криптоключи вводят и хранят (весь срок их действия) непосредственно в СКЗИ, то такой разовый ключевой носитель или электронная запись соответствующего криптоключа должны регистрироваться в аппаратном журнале (приложение № 3) непосредственно пользователем СКЗИ. В аппаратном журнале отражают также данные об эксплуатации СКЗИ и другие сведения, предусмотренные эксплуатационной и технической документацией. В иных случаях аппаратный журнал на СКЗИ не заводится (если нет прямых указаний о его ведении в эксплуатационной или технической документации к криптосредствам).

3.6. СКЗИ, эксплуатационная и техническая документация, правила пользования и ключевые документы между пользователями не передаются. На период отсутствия основного пользователя с его разрешения и по распоряжению министра может быть произведена временная передача СКЗИ, их эксплуатационной и технической документации, а также правил пользования другому пользователю СКЗИ для обеспечения рабочего процесса. Ключевые документы при этом передавать категорически запрещается.

3.7. Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями СКЗИ и (или) ответственным пользователем СКЗИ под расписку в соответствующих журналах поэкземплярного учета и с отметкой в лицевом счете пользователя. Такая передача между пользователями СКЗИ должна быть санкционирована ответственным пользователем СКЗИ.

4. Порядок уничтожения средств криптографической защиты информации

4.1. СКЗИ, непригодные для дальнейшего использования или надобность в использовании которых миновала, уничтожаются (утилизируются) по решению министра.

4.2. Уничтожение криптоключей (исходной ключевой информации) может

производиться путем физического уничтожения ключевого носителя, на котором они расположены, или путем стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования).

4.3. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Data Key, Smart Card, Touch Memory и т. п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

4.4. Ключевые носители уничтожают путем нанесения им неустранимого физического повреждения, исключающего возможность дальнейшего использования, а также восстановления ключевой информации.

4.5. Бумажные и прочие сгораемые ключевые носители, а также эксплуатационная и техническая документация к криптосредствам уничтожаются путем сжигания или с помощью бумагорезательных машин.

4.6. Ключевые документы должны быть уничтожены в сроки, указанные в правилах пользования к соответствующим СКЗИ, но не позднее 10 суток после вывода их из действия (окончания срока действия). Отметки о деинсталляции СКЗИ, уничтожении эксплуатационной, технической документации, правил пользования, ключевых документов оформляются в соответствующих журналах учета.

4.7. Уничтожение большого объема ключевых документов может быть оформлено актом. Уничтожение по акту производит комиссия в составе не менее двух человек из числа лиц, допущенных к пользованию СКЗИ. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведенном уничтожении делаются отметки в журнале поэкземплярного учета.

4.8. СКЗИ, полученные от сторонних организаций в рамках оказания услуг по криптографической защите информации в министерстве, не могут уничтожаться (утилизироваться) служащими (работниками) министерства самостоятельно; требуется обязательное уведомление и привлечение сотрудников организаций – поставщиков СКЗИ. Порядок уничтожения (утилизации) СКЗИ должен соответствовать эксплуатационной и технической документации к СКЗИ.

5. Действия при компрометации или повреждении ключевой информации. Порядок проведения расследования

5.1. *Передача по техническим средствам связи служебных сообщений, касающихся организации и обеспечения безопасности с использованием СКЗИ защищаемой информации, производится только в зашифрованном виде.*

5.2. *Передача по техническим средствам связи закрытых ключей не допускается за исключением специально организованных систем, правилами пользования которых предусматривается управление ключевой системой с использованием технических каналов связи.*

5.3. Под компрометацией криптографического ключа понимается утрата доверия к тому, что данный ключ обеспечивает необходимую защиту информации. Криптоключи, в отношении которых возникло подозрение в компрометации, необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам.

5.4. К событиям, связанным с компрометацией криптографических ключей, относятся:

утеря (хищение) носителей ключевой информации, в том числе с последующим их обнаружением;

увольнение сотрудника, имевшего доступ к ключевой информации;

передача закрытых ключей по линиям связи;

нарушение правил хранения или уничтожения криптоключа;

несанкционированное или безучетное копирование ключевой информации;

нарушение целостности печати на сейфе с ключевыми носителями;

раскрытие фактов утечки (искажения или изменения) передаваемой информации;

все случаи, когда нельзя достоверно установить, что произошло с носителем ключевой информации.

5.5. При наступлении любого из перечисленных случаев или иных нарушениях, которые могут привести к компрометации криптоключей, пользователь должен прекратить использование СКЗИ и немедленно сообщить о произошедшем ответственному пользователю.

5.6. Осмотр ключевых носителей посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

5.7. В каждом случае по факту компрометации или по подозрению в компрометации ключевых документов специально назначенной комиссией проводится служебное расследование. Результатом расследования является квалификация или не квалификация данного события как компрометации.

5.8. В случаях недостачи, непредъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры по их розыску.

Мероприятия по розыску и локализации последствий компрометации ключевых документов организовывает и осуществляет министр.

5.9. Пользователями совместно с ответственным пользователем СКЗИ производится информирование всех заинтересованных участников информационного обмена о факте компрометации ключевой информации.

5.10. Выведенные из действия скомпрометированные ключевые документы после проведения расследования уничтожаются, о чем делается соответствующая запись в журнале поэкземплярного учета.

5.11. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, по решению министра допускается использование скомпрометированных криптоключей, если это не противоречит руководящей документации организации, выдавшей криптоключи. В этом случае период использования скомпрометированных криптоключей не должен превышать 1 дня, а защищаемая информация должна быть как можно менее ценной.

6. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним

6.1. При оборудовании помещений должны выполняться требования к размещению, монтажу СКЗИ, а также другого оборудования, функционирующего с СКЗИ согласно эксплуатационной документации на СКЗИ.

6.2. Перечень сотрудников, имеющих доступ в помещения, в которых установлены криптосредства, утверждается приказом Об утверждении списка лиц, допущенных к работе со средствами криптографической защиты информации в министерстве сельского хозяйства Тульской области.

6.3. Доступ в помещения, в которых установлены криптосредства, в нерабочее время предоставляется по согласованию министра.

6.4. По окончании рабочего дня помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от помещений должны быть сданы под расписку в соответствующем журнале на пост охраны.

6.5. Режим охраны помещений, в том числе правила допуска сотрудников и посетителей в рабочее и нерабочее время, осуществляется в соответствии с «Порядком доступа сотрудников органов исполнительной власти и аппарата правительства Тульской области в помещения, в которых ведется обработка персональных данных», утвержденным постановлением правительства Тульской области «О мерах по реализации отдельных положений Федерального закона «О персональных данных» от 29 марта 2014 года № 213.

6.6. Системные блоки ПЭВМ со СКЗИ должны быть опечатаны для осуществления контроля их вскрытия.

6.7. Применяемые СКЗИ должны быть сертифицированы в соответствии с действующим законодательством.

6.8. Пользователи криптосредств хранят выданные им для использования ключевые документы в хранилищах индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним и непреднамеренное уничтожение. В случае отсутствия индивидуального хранилища по окончании рабочего дня пользователь обязан сдать СКЗИ ответственному пользователю СКЗИ.

6.9. Хранение эксплуатационной и технической документации к СКЗИ, а также копий сертификатов открытых ключей ЭП в бумажном виде осуществляется у пользователя СКЗИ.

6.10. Хранение криптоключей и инсталляционного ПО СКЗИ допускается в одном сейфе с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами, применение.

6.11. Ответственным пользователем криптосредств ведется журнал учета сейфов, металлических шкафов и хранилищ документов, где осуществляется хранение эксплуатационной и технической документации к СКЗИ, а также копий сертификатов открытых ключей ЭП и самих ключевых документов пользователей (приложение № 5).

Приложение № 1
к инструкции по порядку
использования и организации работы
со средствами криптографической
защиты в министерстве сельского
хозяйства Тульской области

Журнал
лицевых счетов пользователей криптосредств

№	Ф. И. О. пользователя	Должность	№ лицевого счета	Дата открытия	Дата закрытия
1	2	3	4	5	6

Лицевой счет № _____

Пользователь: _____

№ п/п	Наименование криптосредства, эксплуатационной и технической документации, ключевых документов	Серийные номера криптосредства, эксплуатационной и технической документации, номера серий ключевых документов	Номера экземпляров (криптономера) ключевых документов	Выдано (№ письма, акта и дата)	Возвращено или уничтожено (№ письма, акта и дата)	Примечание
1	2	3	4	5	6	7

Приложение № 2
к инструкции по порядку
использования и организации работы
со средствами криптографической
защиты в министерстве сельского
хозяйства Тульской области

Журнал поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов в министерстве сельского хозяйства Тульской области

№ п/п	Наименование криптосредств, эксплуатационной и технической документации к ним, вид носителя ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним, номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о получении		Отметка о выдаче	
				От кого получены	Дата и номер сопроводительного письма	Ф.И.О. пользователя криптосредств	Дата и расписка в получении
1	2	3	4	5	6	7	8

Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Примечание
Ф. И. О. пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Ф. И. О. пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
9	10	11	12	13	14	15

Приложение № 3
к инструкции по порядку
использования и организации работы
со средствами криптографической
защиты в министерстве сельского
хозяйства Тульской области

Технический (аппаратный) журнал

№ п/п	Дата	Тип и регистрационные номера используемых криптосредств	Записи по обслуживанию криптосредств	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны криптосредств, в которую введены криптоключи	Дата	Подпись пользователя криптосредств	
1	2	3	4	5	6	7	8	9	10

Приложение № 4
к инструкции по порядку
использования и организации работы
со средствами криптографической
защиты в министерстве сельского
хозяйства Тульской области

Акт на уничтожение криптосредств

№ _____

г._____ «____» _____ 20 __г.

Комиссия в составе _____
(должности, фамилии, инициалы членов комиссии)

на основании _____подготовила к уничтожению
(основание для уничтожения)

_____
(наименование, тип криптосредств, их номера, номера серий, комплектов, экземпляров)

в количестве _____экземпляров.
(цифрами и прописью)

Всего подлежит уничтожению _____наименований экземпляров.
(цифрами и прописью)

Председатель комиссии:

_____ _____
(подпись) (фамилия)

Члены комиссии:

_____ _____
(подпись) (фамилия)

_____ _____
(подпись) (фамилия)

Перечисленные криптосредства (программное обеспечение криптосредств, ключевая информация, содержащиеся на носителях информации, аппаратные, программно-аппаратные криптосредства и т.д.) после утверждения акта полностью уничтожены путем

_____
(переформатирования, удаления программного обеспечения криптосредств, физического уничтожения носителей

_____ с использованием программы_____,
многократного использования) (название программы)

входящей в комплект криптосредства «_____» _____ 20 ___ г.

Председатель комиссии:

_____	_____
(подпись)	(фамилия)

Члены комиссии:

_____	_____
(подпись)	(фамилия)
_____	_____
(подпись)	(фамилия)

Отметки об уничтожении криптосредств (программного обеспечения криптосредств, ключевой информации, содержащихся на магнитных носителях информации, аппаратных, программно-аппаратных криптосредств), перечисленных в акте, в журнале

_____ произвел
(наименование журнала учета, его №)

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

Приложение № 5
к инструкции по порядку
использования и организации работы
со средствами криптографической
защиты в министерстве сельского
хозяйства Тульской области

Журнал учета сейфов, металлических шкафов и хранилищ документов

№ п/п	Тип хранилища	Заводской/ инвентарный номер	Местонахождение хранилища	Фамилия и инициалы ответственного	Количество ключей	Место хранения дубликатов ключей	Примечание
1	2	3	4	5	6	7	8