ФЕДЕРАЛЬНАЯ СЛУЖБА ИСПОЛНЕНИЯ НАКАЗАНИЙ

УПРАВЛЕНИЕ ПО ХАНТЫ-МАНСИЙСКОМУ АВТОНОМНОМУ ОКРУГУ – ЮГРЕ

(УФСИН РОССИИ ПО ХАНТЫ-МАНСИЙСОМУ АВТОНОМНОМУ ОКРУГУ – ЮГРЕ)

П Р И К А З

Сургут

01 апреля 2016 г. № 150

О назначении ответственных лиц
за организацию обработки персональных данных

В соответствии с пунктом 1 постановления Правительства Российской Федерации от 21 марта 2012 г. № 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», п р и к а з ы в а ю:

1. Назначить ответственным за организацию обработки персональных данных в Управлении Федеральной службы исполнения наказаний по Ханты-Мансийскому автономному округу – Югре (далее – УФСИН России по Ханты-Мансийскому автономному округу – Югре) заместителя начальника полковника внутренней службы Амелишко Михаила Михайловича.

2. Утвердить Инструкцию ответственному за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре (приложение № 1).

3. Утвердить перечень информационных систем персональных данных (далее ИСПДн) в УФСИН России по Ханты-Мансийскому автономному округу – Югре (приложение № 2).

4. Утвердить список лиц, ответственных за обеспечение безопасности персональных данных (администраторов безопасности) при их обработке в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре (приложение № 3).

5. Утвердить Инструкцию ответственному за обеспечение безопасности персональных данных в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре (приложение № 4).

6. Методическое руководство и контроль за эффективностью предусмотренных мер по технической защите информации, содержащей персональные данные в УФСИН России по Ханты-Мансийскому автономному округу – Югре, возложить на начальника федерального казенного учреждения «Центр инженерно-технического обеспечения и вооружения УФСИН России по Ханты-Мансийскому автономному округу – Югре» полковника внутренней службы Демчука Алексея Владимировича.

7. Контроль за исполнением настоящего приказа оставляю за собой.

Начальник
полковник внутренней службы Д.Н. Безруких

Исп. Сбоев В.Г.
тел. (3462)21-95-51, вн.151

Приложение № 1

к приказу УФСИН России
по Ханты-Мансийскому
автономному округу – Югре
от _____ № _____

Инструкция
ответственному за организацию обработки персональных данных
в УФСИН России по Ханты-Мансийскому автономному округу – Югре

1. Общие положения

1.1. Инструкция ответственного за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре (далее – Инструкция) разработана в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 21 марта 2012 г. № 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», другими нормативными правовыми актами.

1.2. Настоящая Инструкция определяет ответственность, основные функции, задачи и права ответственного за организацию обработки персональных данных (далее – Ответственный) в УФСИН России по Ханты-Мансийскому автономному округу – Югре.

1.3. Ответственный назначается приказом начальника УФСИН России по Ханты-Мансийскому автономному округу – Югре.

1.4. В своей работе Ответственный руководствуется законодательными и иными нормативными актами Российской Федерации в области обеспечения безопасности персональных данных (далее - ПДн), настоящим положением, приказами и указаниям Руководителя организации и другими руководящими документами по обеспечению безопасности ПДн.

2. Основные функции и задачи Ответственного

2.1. Основными задачами Ответственного являются:

проведение единой политики в УФСИН России по Ханты-Мансийскому автономному округу – Югре и координация работ по организации обработки и обеспечению безопасности ПДн;

планирование мероприятий по организации обработки персональных данных, разработка организационно-распорядительной документации, регламентирующей порядок обработки и защиты ПДн;

организация доведения до сведений сотрудников соответствующих структурных подразделений положений законодательства Российской Федерации

о персональных данных, правовых актов по вопросам обработки персональных данных, требований к защите ПДн;

организация обучения сотрудников непосредственно осуществляющих обработку персональных данных;

организация опубликования документов, определяющих политику в отношении обработки персональных данных, на официальном сайте государственного или муниципального органа в течение 10 дней после их утверждения;

организация внутреннего контроля за соблюдением требований законодательства Российской Федерации и инструкций при обработке ПДн в УФСИН России по Ульяновской области;

организация подачи уведомления в уполномоченный орган по защите прав субъектов персональных данных о своем намерении осуществлять обработку персональных данных

2.2. Для выполнения поставленных задач на Ответственного возлагаются следующие функции:

участие на стадии внедрения информационных систем персональных данных (далее – ИСПДн) в разработке процесса обработки персональных данных по вопросам:

организации порядка учета, хранения и обращения с документами и носителями информации;

организации контроля выполнения требований действующих нормативных правовых актов по вопросам защиты информации при обработке ПДн;

поддержания списка лиц, допущенных к обработке ПДн в актуальном состоянии.

2.3. Для реализации поставленных задач и возложенных функций Ответственный обязан:

знать законодательство Российской Федерации в области обработки и защиты персональных данных, локальные правовые акты УФСИН России по Ханты-Мансийскому автономному округу – Югре по вопросам обработки персональных данных, руководствоваться ими в своей деятельности в части касающейся выполнения возложенных должностных обязанностей;

требовать прекращения обработки ПДн в ИСПДн, как в целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн или средств защиты;

участвовать в проведении служебных проверок по фактам разглашения ПДн, нарушения условий функционирования системы обработки и защиты персональных данных в ИСПДн.

2.4. Ответственному запрещается:

использовать в своих и в чьих-либо личных интересах ресурсы ИСПДн, предоставлять такую возможность другим лицам;

производить действия, приводящие к нарушению обработки ПДн.

3. Права Ответственного

3.1. Для выполнения возложенных задач и функций Ответственный имеет право:

получать доступ к программным и аппаратным средствам ИСПДн, средствам их защиты, а также просмотру прав доступа к ресурсам на серверах информационных систем персональных данных;

требовать от пользователей ИСПДн соблюдения мер по обеспечению безопасности персональных данных при их обработке;

осуществлять контроль за реализацией организационных и распорядительных документов по организации обработки и обеспечению безопасности ПДн;

инициировать проведение служебных проверок по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

осуществлять оперативное вмешательство в работу пользователя ИСПДн при явной угрозе безопасности информации в результате несоблюдения установленной технологии обработки информации и невыполнения требований по безопасности;

вносить предложения начальнику УФСИН России по Ханты-Мансийскому автономному округу – Югре о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) персональных данных в ИСПДн.

4. Ответственность Ответственного

4.1. Ответственный несет персональную ответственность за:

соблюдение требований законодательства, регламентирующего обработку персональных данных;

правильность и объективность принимаемых решений;

выполнение возложенных на него обязанностей, предусмотренных настоящей Инструкцией;

4.2. В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Заместитель начальника УФСИН России
по Ханты-Мансийскому автономному округу – Югре
полковник внутренней службы М.М. Амелишко

Приложение № 2

к приказу УФСИН России
по Ханты-Мансийскому
автономному округу - Югре
от _____ № _____

ПЕРЕЧЕНЬ
информационных систем персональных данных
в УФСИН России по Ханты-Мансийскому автономному округу - Югре

№	Наименование ИС	Содержание сведений	Средства обработки
1	ИСПДн «Финансово-экономический отдел»	Содержит сведения о сотрудниках: Ф.И.О., паспортные данные, СНИЛС и ИНН	MS Office, Fine Read, Adobe Acrobat, Автоматизированная система управления бюджетными средствами ФСИН России, ППО Автоматизированная система Федерального казначейства, Комплекс «АКСИОК»,
2	ИСПДн «Главная бухгалтерия»	Содержит сведения о сотрудниках: Ф.И.О., дата рождения, паспортные данные, адрес места регистрации, ИНН, СНИЛС, доход расчетные счета	MS Office, 1С:Предприятие, СУФД, Комплекс «АКСИОК», «Контур-Экстерн», «Контур-Зарплата»
3	ИСПДн «Отдел кадров»	Содержит сведения о сотрудниках, служащих (работников УИС), кандидатов, поступающих на службу в УИС и в ведомственные учебные заведения ФСИН России, и их близких родственников: Ф.И.О., дата и место рождения, место регистрации и проживания, паспортные данные, сведения о СНИЛС и ИНН, свидетельства о рождении, заключении и расторжении брака, документы об образовании, информация о наличии или отсутствии компрометирующих материалов, личные номера сотрудников, наименования замещаемой должности, сведения о стаже, сведения о доходах, сведения о дисциплинарные взыскания и поощрения, биометрические параметры (справки ВВК)	MS Office

4	ИСПДн «Группа специального учета отдела безопасности»	Содержит сведения об осужденных, подозреваемых, обвиняемых: Ф.И.О., дата и место рождения, гражданство, национальность, семейное положение, образование, адрес фактического проживания и адрес места регистрации, паспортные данные, сведения об осуждении, информация о прежних судимостях, дактилоскопический материал, место отбывания наказаний, информация о родственниках (Ф.И.О., дата и место рождения, гражданство, адрес фактического проживания и адрес места регистрации), материалы личных дел	MS Office, ПТК АКУС
5	ИСПДн «Группа пенсионного обеспечения»	Содержит сведения о пенсионерах: Ф.И.О., дата и место рождения, пол, адрес места жительства, паспортные данные, сведения об обучении, трудовой деятельности, службе, состоянии здоровья, лицевых счетах, размерах пенсий (пособий), заключения ВВК, сведения об инвалидности	MS Office, ПК «Пенсия», ПАК «АНЕТ», ПК «Назначение и выплата пенсии»
6	ИСПДн «Группа воспитательной работы с осужденными»	Содержит сведения об осужденных, подозреваемых, обвиняемых: Ф.И.О., дата и место рождения, гражданство, национальность, семейное положение, образование, адрес фактического проживания и адрес места регистрации, сведения об осуждении, информация о прежних судимостях, место отбывания наказания, информация о родственниках, материалы личных дел осужденных	MS Office, ПТК АКУС
7	ИСПДн «Психологическая служба»	Содержит сведения о сотрудниках и кандидатах на службу: Ф.И.О., дата рождения, образование, семейное положение, состояние здоровья, место жительства, место работы, должность, звание, результаты психологических исследований, материалы личных дел. Об осужденных, обвиняемых, подозреваемых: Ф.И.О., дата рождения, образование, семейное положение, судимости, состояние здоровья, место жительства, результаты психологических исследований, материалы личных дел	MS Office, Psychometric Expert.

8	ИСПДн «Группа профессиональной подготовки»	Содержит сведения о сотрудниках: Ф.И.О., дата рождения, образование, должность, звание, результаты зачетов по служебно- боевой подготовке, спортивные звания (разряды), квалификационные звания, страховые свидетельства по случаям получения травм, состояние здоровья, родственные связи, сведения о инвалидности детей сотрудников, сведения о ветеранах боевых действий, номера удостоверений, периоды командировок	MS Office
9	ИСПДн «Инспекция по личному составу и противодействия коррупции»	Содержит сведения о сотрудниках, служащих и их родственниках: Ф.И.О., дата и место рождения, место регистрации и проживания, паспортные данные, сведения о СНИЛС и ИНН, свидетельства о рождении, заключении и расторжении брака, образование, должность, звание, личный номер сотрудника, семейное положение, родственные связи, сведения о доходах, имуществе и обязательствах имущественного характера, биометрические параметры (справки ВВК), информация о наличии или отсутствии компрометирующих материалов	MS Office
10	ИСПДн «Прием граждан»	Содержит сведения о сотрудниках и иных гражданах: Ф.И.О., место регистрации и проживания, адрес электронной почты, контактные телефоны, иные персональные данные, содержащиеся в обращении (жалобе)	MS Office, журнальный учет

Заместитель начальника УФСИН России
по Ханты-Мансийскому автономному округу – Югре
полковник внутренней службы М.М. Амелишко

Приложение № 3

к приказу УФСИН России
по Ханты-Мансийскому
автономному округу – Югре
от _____ № _____

СПИСОК ЛИЦ,

ответственных за обеспечение безопасности персональных данных (администраторов безопасности) при их обработке в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре

Деточкина Наталья Николаевна	старший инспектор группы пенсионного обеспечения УФСИН России по Ханты-Мансийскому автономному округу – Югре, майор внутренней службы;	ИСПДн «Группа пенсионного обеспечения»
Коновалов Владимир Владимирович	начальник инспекции по личному составу и противодействия коррупции УФСИН России по Ханты-Мансийскому автономному округу – Югре, подполковник внутренней службы;	ИСПДн «Инспекции по личному составу и противодействию коррупции»
Отшанова Ольга Николаевна	старший инспектор группы специального учета отдела безопасности УФСИН России по Ханты-Мансийскому автономному округу – Югре, капитан внутренней службы;	ИСПДн «Группа специального учета отдела безопасности»
Михеев Сергей Николаевич	Инспектор группы профессиональной подготовки УФСИН России по Ханты-Мансийскому автономному округу – Югре, майор внутренней службы;	ИСПДн «Отдел по работе с личным составом
Клюкина Елена Вячеславовна	начальник финансово-экономического отдела УФСИН России по Ханты-Мансийскому автономному округу – Югре, майор внутренней службы	ИСПДн «Финансово-экономический отдел»
Фролов Григорий Николаевич	главный бухгалтер главной бухгалтерии УФСИН России по Ханты-Мансийскому автономному округу – Югре, полковник внутренней службы;	ИСПДн «Главная бухгалтерия»

Воронов Евгений Михайлович	-	старший инспектор группы воспитательной работы с осужденными УФСИН России по Ханты-Мансийскому автономному округу – Югре, майор внутренней службы	ИСПДн «Отдел воспитательной работы с осужденными»
Бордунова Ольга Валерьевна	-	начальник психологической службы УФСИН России по Ханты-Мансийскому автономному округу – Югре, подполковник внутренней службы;	ИСПДн «Психологическая служба»
Соснина Марина Николаевна		заместитель начальника отдела кадров УФСИН России по Ханты-Мансийскому автономному округу – Югре, майор внутренней службы;	ИСПДн «Отдел кадров»
Тесля Галина Ивановна		начальник секретариата УФСИН России по Ханты-Мансийскому автономному округу – Югре, майор внутренней службы.	ИСПДн «Прием граждан»

Заместитель начальника УФСИН России
по Ханты-Мансийскому автономному округу – Югре
полковник внутренней службы М.М Амелишко

Приложение № 4

к приказу УФСИН России
по Ханты-Мансийскому
автономному округу – Югре
от _____ № _____

Инструкция
ответственному за обеспечение безопасности персональных данных
в УФСИН России по Ханты-Мансийскому автономному округу – Югре

1. Общие положения

1.1. Настоящая инструкция определяет порядок работы лиц, ответственных за обеспечение безопасности персональных данных (администраторов безопасности информационной системы персональных данных) (далее – Администратор) в информационной системе персональных данных (далее – ИСПДн) Управления Федеральной службы исполнения наказаний по Ханты-Мансийскому автономному округу – Югре (далее – УФСИН России по Ханты-Мансийскому автономному округу – Югре) и устанавливает единые требования по обеспечению безопасности персональных данных (далее – ПДн) обрабатываемых в УФСИН России по Ханты-Мансийскому автономному округу – Югре и регламентирует порядок работы администраторов со средствами криптографической защиты информации (далее – СКЗИ).

1.2. Администратор назначается приказом начальника УФСИН России по Ханты-Мансийскому автономному округу – Югре и руководствуется в своей деятельности:

настоящей инструкцией;

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну утвержденной приказом ФАПСИ при Президенте РФ от 13 июня 2001 г. № 152;

эксплуатационной и технической документацией на применяемые СКЗИ и средства антивирусной защиты;

руководящими и нормативными документами ФСТЭК и ФСБ России, внутренними инструкциями и распоряжениями, регламентирующими порядок действий по защите информации в ИСПДн.

1.3. Администратор отвечает за поддержание необходимого уровня безопасности объектов защиты.

1.4. Администратор назначается из числа наиболее подготовленных сотрудников структурного подразделения, эксплуатирующего ИСПДн и обеспечивает решение вопросов информационной безопасности дополнительно к своим непосредственным должностным обязанностям.

1.5. Администратор осуществляет методическое руководство пользователей ИСПДн в вопросах обеспечения безопасности ПДн. Требования администратора, связанные с выполнением им своих должностных обязанностей, обязательны для исполнения всеми пользователями, обрабатывающими ПДн в ИСПДн.

1.6. Администратор несет персональную ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники, а также осуществляемой без использования средств автоматизации в ИСПДн, в том числе по контролю действий пользователей при поддержании необходимого уровня защиты ПДн и обеспечение функционирования СКЗИ.

2. Должностные обязанности

Администратор обязан:

2.1. Знать и выполнять требования нормативных правовых актов, нормативных и методических документов, а также внутренних документов, регламентирующих вопросы обработки ПДн и защиты информации, в том числе Инструкции пользователя, обрабатывающего ПДн в УФСИН России по Ханты-Мансийскому автономному округу – Югре.

2.2. Вести учет используемых в ИСПДн СКЗИ, ключевых документов и эксплуатационной и технической документации к ним.

2.3. Участвовать в приемке новых программных средств, устанавливаемых на автоматизированных рабочих местах, на которых обрабатываются ПДн.

2.4. Обеспечивать доступ к защищаемой информации пользователям, согласно их правам.

2.5. Уточнять в установленном порядке обязанности пользователей.

2.6. Анализировать состояние защиты информации при обработке ПДн.

2.7. Контролировать физическую сохранность средств и оборудования, используемых для обработки ПДн.

2.8. Контролировать неизменность состояния средств защиты информации, их параметров и реализуемых режимов защиты.

2.9. Контролировать правильность работы пользователей по обработке ПДн и применению СКЗИ.

2.10. Совместно с Администратором сети выдавать пользователям личные пароли доступа к автоматизированной системе ПДн, соблюдать и контролировать организацию парольной защиты.

2.11. Не допускать установку, использование, хранение и размножение в автоматизированных системах обработки ПДн программных средств, не связанных с выполнением функциональных задач.

2.12. Не допускать к работе по обработке ПДн посторонних лиц.

2.13. Осуществлять периодические контрольные проверки рабочих мест пользователей.

2.14. Докладывать ответственному за организацию обработки ПДн о нештатных ситуациях при обработке ПДн и допущенных пользователями нарушениях установленных требований по защите информации.

2.15. В случае отказа работоспособности технических средств и программного обеспечения, необходимых для обработки ПДн, в том числе СКЗИ, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.16. Принимать меры по реагированию в случае возникновения внештатных и аварийных ситуаций с целью ликвидации их последствий.

3. Права Администратора

Администратор имеет право:

3.1. Контролировать работу пользователей на автоматизированных рабочих местах ИСПДн.

3.2. Требовать прекращения обработки информации как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн.

3.3. Участвовать в служебных расследованиях по фактам нарушения установленных требований обеспечения информационной безопасности.

4. Правила работы со средствами криптографической защиты информации

4.1. При работе с СКЗИ Администратор осуществляет:

4.1.1. Учёт криптосредств, эксплуатационной и технической документации с использованием условных наименований и регистрационных номеров.

4.1.2. Выдачу средств криптографической защиты информации пользователям.

4.1.3. При необходимости изготовление (генерацию) ключевых документов из исходной ключевой информации.

4.1.4. Совместно с Администратором сети установку и ввод в эксплуатацию СКЗИ в соответствии с эксплуатационной и технической документацией к этим средствам.

4.1.5. Контроль за соблюдением пользователями, конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых криптосредств и ключевых документах к ним.

4.1.6. Надёжное хранение СКЗИ, ключевых документов, эксплуатационной и технической документации к криптосредствам.

4.1.7. Учёт лиц, допущенных к работе со средствами криптографической защиты информации (пользователей).

4.1.8. Контроль за соблюдением условий использования криптосредств, предусмотренных эксплуатационной и технической документацией к ним.

4.1.9. Разбирательства по фактам нарушения условий хранения и использования криптосредств, которые могут привести к нарушению или к снижению уровня защищённости информации.

4.2. Порядок учета СКЗИ:

4.2.1. Должностные лица, допущенные к работе с криптосредствами, заносятся в список пользователей. Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, а также ключевые документы подлежат учету в журнале поэкземплярного учета (приложение). При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование.

Единицей поэкземплярного учета ключевых документов считается носитель с ключевой информацией. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

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

4.2.3. Передача криптосредств, эксплуатационной и технической документации к ним, ключевых документов допускается только между пользователями и Администратором под расписку в соответствующих журналах поэкземплярного учета. Передача учтенных СКЗИ без санкции Администратора **категорически запрещается.**

4.3. Порядок уничтожения СКЗИ:

4.3.1. СКЗИ непригодные для дальнейшего использования, или надобность в использовании которых миновала, уничтожаются (утилизируются) Администратором по согласованию с организацией выдавшей данное СКЗИ.

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

4.3.3. Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), DataKey, SmartCard, TouchMemory 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 криптосредствам.

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

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

4.3.5. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим криптосредствам.

4.3.6. Ключевые документы уничтожаются пользователями совместно с Администратором под расписку в журнале поэкземплярного учета, при этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. О проведенном уничтожении делаются отметки в журнале поэкземплярного учета.

4.4. Действия при компрометации или повреждении ключевой информации. Порядок проведения расследования:

4.4.1. 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.

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

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

передача закрытых ключей по открытым каналам связи;

нарушение правил хранения или уничтожения криптоключа;

несанкционированное или безучетное копирование ключевой информации;

нарушение целостности печати на сейфе с ключевыми носителями;

вскрытие фактов утечки (искажения или изменения) передаваемой информации;

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

4.4.3. При наступлении любого из перечисленных случаев, или иных нарушениях, которые могут привести к компрометации криптоключей, Администратор должен проконтролировать прекращение использования Пользователем СКЗИ и сообщить о данных фактах ответственному за организацию обработки персональных данных в УФСИН России по Ханты-Мансийскому автономному округу – Югре.

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

4.4.5. В каждом случае, по факту (или предполагаемой) компрометации ключевых документов, специально назначенной комиссией, проводится служебное расследование. Результатом расследования является квалификация или не квалификация данного события как компрометация.

В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения принимаются срочные меры к их розыску.

4.4.6. О факте компрометации ключевой информации Администратором производится информирование всех заинтересованных участников информационного обмена.

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

4.4.8. Для своевременно восстановления связи Администратором создается резервный запас криптоключей в необходимом количестве. Использование резервных ключей осуществляется в случаях крайней необходимости, по решению Администратора.

4.4.9. Хранение резервных носителей ключевой информации, осуществляется Администратором отдельно от рабочих (актуальных) ключей, с целью обеспечения невозможности их одновременной компрометации.

5. Правила взаимодействия администраторов

В случае необходимости взаимодействия Администраторов безопасности персональных данных в ИСПДн УФСИН России по Ханты-Мансийскому автономному округу – Югре для обеспечения безопасности обработки персональных данных (организации взаимодействия криптосредств), такое взаимодействие осуществляет Ответственный за организацию обработки персональных данных, указания которого являются обязательными для всех администраторов и пользователей.

6. Ответственность администратора

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Заместитель начальника УФСИН России
по Ханты-Мансийскому автономному округу – Югре
полковник внутренней службы М.М. Амелишко