Об утверждении руководящих

документов по организации защиты

персональных данных

при их обработке в информационных

системах персональных данных

В соответствии с распоряжением Администрации города от 30.12.2005 № 3686 «Об утверждении Регламента Администрации города» (с последу-ющими изменениями), во исполнение требований федеральных законов от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями от 01.12.2014), от 27.07.2006 № 152-ФЗ «О персональных данных» (с изменениями от 21.07.2014), постановлений Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информа-ционных системах персональных данных», от 21.03.2012 № 211 «Об утвер-ждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и приня-тыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами» (с изме-нениями от 06.09.2014), приказов Федеральной службы по техническому и экспортному контролю России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплу-атации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» (с изменениями от 12.04.2010), от 10.07.2014 № 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», Типовыми требованиям по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденными руководством 8 Центра Федеральной службы безопасности Российской Федерации 21.02.2008 № 149/6/6-622, Приказа Федерального агент-ства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограни-ченным доступом, не содержащей сведений, составляющих государственную тайну»:

1. Утвердить:

1.1. Инструкцию по организации парольной защиты согласно приложению 1.

1.2. Инструкцию по организации антивирусной защиты согласно приложению 2.

1.3. Инструкцию по организации резервирования и восстановления программного обеспечения, баз данных информационных систем персональных данных согласно приложению 3.

1.4. Правила работы с носителями персональных данных согласно приложению 4.

1.5. Правила эксплуатации криптосредств и криптографических ключей к ним согласно приложению 5.

1.6. Руководство пользователя в части обеспечения безопасности персо-нальных данных при их обработке в информационных системах персональных данных согласно приложению 6.

2. Структурным подразделениям Администрации города руководство-ваться утвержденными правилами и инструкциями при обработке персональных данных и работе со средствами криптографической защиты.

3. Муниципальному казённому учреждению «Управление информа-ционных технологий и связи города Сургута» руководствоваться утвержден-ными правилами и инструкциями в части возложенных функций по обеспечению защиты персональных данных при их обработке в информационных системах персональных данных.

4. Контроль за выполнением постановления возложить на заместителя главы Администрации города Базарова В.В.

Глава города Д.В. Попов

Приложение 1

к постановлению

Администрации города

от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

Инструкция

по организации парольной защиты

1. Общие положения

1.1. Настоящая инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей при работе с паролями с целью исклю-чения несанкционированного доступа (далее – НСД) к ресурсам ИСПДн, содержащих персональные данные (далее – ПДн).

1.2. Настоящая инструкция не распространяется на правила генерации парольной информации, используемой в средствах криптографической защиты информации.

1.3. Защите паролем подлежит доступ к объектам парольной защиты, а именно к:

- базовым системам ввода-вывода автоматизированных рабочих мест;

- настройкам сетевого оборудования;

- настройкам операционных систем;

- настройкам средств виртуализации;

- настройкам средств защиты информации (в том числе средств антиви-русной защиты);

- запуску специализированного программного обеспечения, предназначен-ного для обработки ПДн;

- настройкам систем управления баз данных и базам данных;

- ресурсам файловых массивов.

1.4. Объекты парольной защиты должны быть настроены таким образом, чтобы:

- исключить возможность просмотра ранее вводимых паролей;

- блокировать доступ пользователей после пятикратной ошибки при вводе пароля и сигнализировать о наступлении данного события.

2. Порядок заведения и регистрации паролей доступа пользователей

2.1. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями пользователей при работе с паролями возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.

2.2. При введении нового пользователя уполномоченная организация по обеспечению безопасности персональных данных назначает временный пароль, который должен быть сменен пользователем при первом входе в систему.

2.3. Пользователь обязан запомнить личные пароли, хранить их таким образом, чтобы исключить несанкционированное ознакомление. Запрещается передавать пароли.

3. Принципы выбора и формирования личных паролей

3.1. Личные пароли должны генерироваться и распределяться централизо-ванно либо выбираться пользователями самостоятельно с учетом следующих требований:

- длина пароля должна быть не менее 6 символов;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем или нижнем регистрах, цифры и/или специальные символы (@, #, $, ^, \*, % и тому подобное);

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и так далее), а также общепри-нятые сокращения (ЭВМ, ЛВС, USER, ПОЛЬЗОВАТЕЛЬ и тому подобное);

- при смене пароля новое значение должно отличаться от предыдущего;

- допускается использовать русские слова, набираемые в латинском регистре (без переключения клавиатуры);

- пользователь не имеет права сообщать личный пароль другим лицам.

3.2. Внеплановая смена личного пароля или удаление записи пользователя в случае прекращения полномочий пользователя (увольнение, переход на другую работу и тому подобное) должна производиться уполномоченной организацией по обеспечению безопасности персональных данных немедленно после окончания последнего сеанса работы данного пользователя с системой.

3.3. Внеплановая полная смена паролей всех пользователей ИСПДн должна производиться в случае прекращения полномочий (увольнения, перехода на другую работу и тому подобное) сотрудника уполномоченной организации по обеспечению безопасности персональных данных ответствен-ного за ИСПДн.

3.4. В случае компрометации личного пароля пользователя должны быть предприняты меры в соответствии с требованиями пункта 3.2 или пункта 3.3 настоящей инструкции в зависимости от полномочий владельца скомпромети-рованного пароля.

4. Период действия паролей пользователей

4.1. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в год.

4.2. Полная плановая смена паролей сотрудников уполномоченной органи-зации по обеспечению безопасности персональных данных проводится регулярно, не реже одного раза в шесть месяцев.

5. Правила работы и обязанности пользователей и сотрудников уполно-моченной организации по обеспечению безопасности персональных данных по использованию и сохранению в тайне личных паролей

5.1. Информация о паролях пользователей является информацией ограни-ченного доступа, предназначенной для идентификации и доступа каждого конкретного пользователя к ресурсам ИСПДн согласно разрешительной системе доступа.

5.2. Во время работы ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и другое).

5.3. При отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. В операционной системе Microsoft Windows для этого необходимо нажать одновременно комбинацию клавиш «Ctrl»+«Alt»+«Del» и выбрать опцию «Блокировать компьютер» (в операционных системах Microsoft Windows 7 и выше возможно использо-вание комбинации клавиш «Win»+L). В иных операционных системах необходимые действия по блокированию компьютера необходимо посмотреть в документации пользователя.

5.4. Пользователь обязан незамедлительно сообщать в уполномоченную организацию по обеспечению безопасности персональных данных о выяв-ленном факте утери, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

5.5. Запрещается:

- умышленное и неумышленное ознакомление с парольной информацией сотрудников и посторонних лиц независимо от их должности;

- передача личного пароля сослуживцам или посторонним лицам;

- запись личного пароля на бумагу и хранение его в доступном для озна-комления посторонними лицами и другими сотрудниками месте;

- вход в систему с использованием чужих идентификаторов или паролей;

- оставление без присмотра рабочего места при работе в ИСПДн.

5.6. Владельцы паролей должны быть ознакомлены под роспись с пере-численными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

5.7. Ответственность за организацию контроля требований настоящей инструкции и соблюдение установленного порядка возлагается на ответствен-ного за организацию обработки персональных данных.

5.8. Ответственность за проведение мероприятий по обеспечению соблюдения требований настоящей инструкции и периодический контроль за состоянием парольной защиты возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.

Приложение 2

к постановлению Администрации города

от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_

Инструкция

по организации антивирусной защиты

1. Общие положения

1.2. Настоящая инструкция определяет требования к организации защиты информационных систем персональных данных (далее – ИСПДн) от разруша-ющего воздействия компьютерных вирусов и устанавливает ответственность руководителей и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.3. К использованию в ИСПДн допускаются только лицензионные и сертифицированные по требованиям безопасности информации антиви-русные средства.

1.4. Установка и настройка средств антивирусного контроля на компью-терах осуществляется в соответствии с руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. При загрузке компьютера в автоматическом режиме должен прово-диться антивирусный контроль дисков и файлов на них.

2.2. Обязательному антивирусному контролю подлежит любая инфор-мация (текстовые файлы любых форматов, файлы данных, исполняемые файлы) на съемных носителях. Разархивирование и контроль входящей инфор-мации необходимо проводить непосредственно после ее приема. Контроль исходящей информации необходимо проводить непосредственно перед архиви-рованием и отправкой (записью на съемный носитель).

2.3. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в три месяца.

2.4. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после уста-новки (изменения) программного обеспечения также должна быть выполнена антивирусная проверка на компьютере.

2.5. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и тому подобное) пользователь самостоятельно должен провести внеочередной антивирусный контроль своего компьютера.

2.6. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

- приостановить работу;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов в уполномоченную организацию по обеспечению безопасности персональных данных;

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;

- провести лечение или уничтожение зараженных файлов.

2.7. Обновление баз системы антивирусного контроля должно проводиться не реже одного раза в неделю.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в соответствии с требованиями настоящей инструкции возлагается на ответственного за орга-низацию обработки персональных данных.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей инструкции возлагается на уполномо-ченную организацию по обеспечению безопасности персональных данных.

3.3. Периодический контроль за состоянием антивирусной защиты в ИСПДн, за соблюдением установленного порядка антивирусного контроля и выполне-нием требований настоящей инструкции осуществляется уполномоченной организацией по обеспечению безопасности персональных данных.

3.4. Ответственность за организацию своевременного обновления антиви-русных баз возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.

Приложение 3

к постановлению Администрации города

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

Инструкция

по организации резервирования и восстановления программного обеспечения, баз данных информационных систем персональных данных

1. Общие положения

1.1. Настоящая инструкция разработана с целью обеспечения возможности незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним.

1.2. Настоящая инструкция определяет правила и объемы резервирования, а также порядок восстановления работоспособности информационных систем персональных данных (далее – ИСПДн).

1.4. В ИСПДн резервированию подлежат:

- базы данных;

- специальное программное обеспечение;

- общее программное обеспечение;

- программное обеспечение средств защиты информации.

2. Порядок резервирования и хранения резервных копий баз данных и программного обеспечения

2.1. Обязательному резервированию подлежат:

- базы данных (текстовые и табличные файлы, а также файлы баз данных специализированных программных продуктов, хранящиеся на компьютере);

- специальное (прикладное) программное обеспечение, используемое для обработки персональных данных;

- программное обеспечение средств защиты информации, в том числе средств антивирусной и криптографической защиты;

- общее программное обеспечение (операционная система и программные драйверы устройств (принтеры, мониторы, видеокарты и тому подобное), поставляемые со средствами вычислительной техники, входящими в состав ИСПДн).

2.2. Резервирование баз данных, а также текстовых и табличных файлов, содержащих персональные данные, допускается только на учтенные установ-ленным порядком отчуждаемые носители информации.

2.3. Резервирование осуществляется не реже одного раза в месяц.

2.4. Носители информации, содержащие резервные копии данных ИСПДн, не могут быть переданы за пределы контролируемой зоны оператора и уполно-моченной организации по обеспечению безопасности персональных данных без согласования с уполномоченной организации по обеспечению безопасности персональных данных.

2.5. Копирование информации с носителей информации, содержащих резервные копии данных ИСПДн, за исключением случая восстановления работоспособности ИСПДн, запрещается.

2.6. Резервирование общего программного обеспечения осуществляется путем создания контрольной точки восстановления системы.

2.7. Резервирование программного обеспечения средств защиты информации обеспечивается путем хранения носителей дистрибутивов программного обеспечения средств защиты информации и обновлений к ним в уполномо-ченной организации по обеспечению безопасности персональных данных.

2.8. Носители обновлений общего и прикладного программного обеспечения, а также программного обеспечения средств защиты информации должны быть маркированы датой их получения (датой выхода обновления).

3. Порядок восстановления работоспособности ИСПДн

3.1. Восстановление работоспособности ИСПДн осуществляется в случаях сбоев, отказов и аварий технических средств и систем ИСПДн, а также ее прог-раммного обеспечения.

3.2. Работы по восстановлению работоспособности в общем случае осуще-ствляются в следующей последовательности:

- проверка исправности и работоспособности средств обеспечения функционирования информационных систем;

- восстановление работоспособности (ремонт или замена) средств обеспе-чения функционирования информационных систем, при необходимости;

- проверка исправности и работоспособности средств вычислительной техники;

- восстановление работоспособности (ремонт или замена) средств вычислительной техники при необходимости;

- проверка правильности функционирования общего программного обеспе-чения ИСПДн;

- восстановление нормального функционирования общего программного обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним при необходимости;

- проверка правильности функционирования средств защиты информации;

- восстановление нормального функционирования средств защиты инфор-мации с использованием дистрибутивов и обновлений к ним при необходимости;

- проверка правильности функционирования специального программного обеспечения ИСПДн;

- восстановление нормального функционирования специального програм-много обеспечения ИСПДн с использованием дистрибутивов и обновлений к ним при необходимости;

- проверка целостности баз данных ИСПДн;

- восстановление баз данных ИСПДн с использованием резервной копии при необходимости;

Данные работы осуществляются в соответствии с эксплуатационной доку-ментацией до полного восстановления работоспособности.

3.3. Восстановление персональных данных, созданных после их послед-него резервирования, осуществляется пользователями, осуществившими их внесение в базы данных ИСПДн.

3.4. В случае необходимости привлечения для восстановления работоспо-собности ИСПДн представителей сторонних организаций должна быть обеспе-чена невозможность их ознакомления с персональными данными, а также несанкционированного копирования на машинные носители информации.

3.5. Ответственность за проведение мероприятий по обеспечению соблюдения требований настоящей инструкции возлагается на уполномоченную организацию по обеспечению безопасности персональных данных.

Приложение 4

к постановлению Администрации города

от \_\_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_

Правила

работы с носителями персональных данных

1. Общие положения

1.1. Правила работы с машинными носителями персональных данных (далее – правила) определяют обязанности, права и ответственность пользова-телей, осуществляющих учет, хранение и обращение со съемными носителями персональных данных, а также их уничтожение.

1.2. В настоящих правилах используются следующие термины и определения:

- оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами органи-зующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персо-нальными данными;

- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

- хранилище носителей персональных данных – сейф или запираемый шкаф (ящик);

- носитель персональных данных – отчуждаемый машиночитаемый носитель информации (в том числе магнитный и электронный), на котором осуществля-ются запись и хранение сведений, на основе которых можно установить его личность.

1.3. Настоящие правила являются обязательными для всех пользователей, ведущих обработку персональных данных в информационных системах персональных данных.

2. Учет носителей персональных данных

2.1. Все находящиеся на хранении и в обращении у оператора носители персональных данных подлежат учету. Каждый носитель персональных данных, с записанными на нем персональными данными должен иметь этикетку, на которой указывается его уникальный регистрационный номер.

2.2. Учет и выдача носителей персональных данных производится с отметкой в журнале учета машинных носителей информации, осуществляется уполно-моченной организацией по обеспечению безопасности персональных данных при их обработке в муниципальных ИСПДн (далее – уполномоченная организация).

2.3. Пользователи, участвующие в обработке персональных данных, в случае необходимости получают учтенный носитель персональных данных от уполномоченной организации для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета носителей персональных данных.

2.4. По окончании работ пользователь сдает носитель персональных данных для хранения уполномоченной организации, о чем делается соответствующая запись в журнале учета.

3. Хранение носителей персональных данных

3.1. По окончании рабочего дня все носители персональных данных, содер-жащие персональные данные, помещаются в хранилище носителей персональных данных. Исключение составляют носители, персональные данные с которых или на которых формируются или обрабатываются в данный момент на рабочем месте.

3.2. Хранилище носителей персональных данных запирается на ключ и опечатывается, при этом доступ посторонних лиц к ключу и печати должен быть исключен.

3.3. Перед вскрытием хранилища носителей персональных данных необхо-димо проверить целостность печати на хранилище.

3.4. В случае обнаружения повреждений оттиска печати на хранилище, утраты печати или ключа от хранилища необходимо незамедлительно сообщить ответственному за организацию обработки персональных данных.

3.5. За сохранность конкретного носителя персональных данных отвечает пользователь, получивший этот носитель в пользование под расписку в журнале учета.

3.6. Не допускается:

- хранение носителей персональных данных вместе с носителями открытой информации, на рабочих столах либо оставление их без присмотра или передача на хранение другим лицам;

- вынос носителей персональных данных из служебных помещений для работы с ними на дому, в гостиницах и так далее.

3.7. Командируемым работникам под их личную ответственность с пись-менного разрешения руководителя оператора разрешается иметь при себе в пути следования носители персональных данных.

4. Передача носителей персональных данных

4.1. Передача носителей персональных данных от одного пользователя другому производится с обязательной отметкой в журнале учета.

4.2. При отправке или передаче носителей персональных данных адресатам на носители записываются только предназначенные адресатам данные.

4.3. Вынос носителей персональных данных для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя оператора.

4.4. Передача носителей персональных данных в другие организации производится курьерской службой, а также заказными почтовыми отправ-лениями. При пересылке носителей персональных данных почтовыми отправлениями они должны быть помещены в дополнительный конверт.

4.5. Персональные данные запрещается передавать по каналам факсимильной связи, с использованием глобальных сетей без использования мер защиты.

5. Утрата носителей персональных данных

5.1. О фактах утраты носителей персональных данных либо разглашения содержащихся на них сведений немедленно ставится в известность ответ-ственный за организацию обработки персональных данных.

5.2. На утраченные носители составляется акт. Соответствующие отметки вносятся в журналы учета носителей персональных данных.

5.3. По факту утраты носителей персональных данных проводится служебное расследование и составляется акт, который представляется ответственному за организацию обработки персональных данных, для принятия решения.

6. Уничтожение носителей персональных данных

6.1. Съемные носители персональных данных, пришедшие в негодность или отслужившие установленный срок, подлежат уничтожению.

6.2. Уничтожение носителей персональных данных производится соот-ветствующей комиссией, осуществляющей уничтожение носителей персональных данных и иной конфиденциальной информации, находящейся на программно-технических средствах ИСПДн.

6.3. Состав комиссии утверждается приказом руководителя оператора.

6.4. В состав комиссии должен входить сотрудник уполномоченной организации.

6.5. По окончании сроков хранения носители персональных данных, подлежащие уничтожению, физически уничтожаются с целью невозможности восстановления и дальнейшего использования. Это достигается путем дефор-мирования, нарушения единой целостности носителя персональных данных или его сжигания. Подлежащие уничтожению файлы с персональными данными, расположенные на жестком диске, удаляются путем многократной перезаписи файлов случайными символами.

6.6. Перед утилизацией оборудования все его компоненты, включая носители информации, например, жесткие диски, необходимо проверять, чтобы гарантировать, что персональные данные и лицензированное программное обеспечение были удалены.

6.7. Поврежденные носители могут потребовать оценки рисков, для того чтобы определить, следует ли их уничтожить или ремонтировать.

6.8. В случае допустимости повторного использования носителя формата FDD, CD-RW, DVD-RW, flash-носителей применяется программное удаление («затирание») содержимого диска путем его форматирования с последующей записью новой информации на данный носитель.

6.9. По результатам уничтожения носителей персональных данных комиссией составляется и подписывается соответствующий акт об уничто-жении носителей.

6.10. В течение трех дней после составления акты об уничтожении направ-ляются комиссией на утверждение руководителю оператора.

6.11. Факт уничтожения носителей персональных данных фиксируется в журнале учета с указанием даты и номера акта уничтожения. Данный журнал является документом конфиденциального характера.

Приложение 5

к постановлению Администрации города

от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_

Правила

эксплуатации криптосредств и криптографических ключей к ним

1. Общие положения

1.1. Настоящие правила эксплуатации криптосредств и криптографических ключей к ним (далее – правила) определяют порядок учета, хранения и исполь-зования криптосредств и криптографических ключей, а также порядок изготовления, смены и уничтожения криптографических ключей в целях обес-печения безопасности эксплуатации криптосредств.

1.2. Настоящие правила разработаны на основе следующих документов:

- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденное приказом Федеральной службы безопасности России от 09.02.2005 № 66;

- Инструкция об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографи-ческой защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну», утвержденная приказом Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13.06.2001 № 152;

- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра Федеральной службы безопасности России 21.02.2008 № 149/6/6-622.

1.3. В настоящих правилах используются следующие термины и определения:

- оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами органи-зующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персо-нальными данными;

- персональные данные – любая информация, относящаяся прямо или косвенно к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных);

- криптосредство – шифровальное (криптографическое) средство, предназ-наченное для защиты информации, не содержащей сведений, составляющих государственную тайну. В частности, к криптосредствам относятся средства криптографической защиты информации (СКЗИ) – шифровальные (криптогра-фические) средства защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну;

- криптографическая защита – защита информации от ее несанкциониро-ванной модификации и доступа посторонних лиц при помощи алгоритмов криптографического преобразования;

- открытый ключ – уникальная последовательность данных, связанная с закрытым ключом с помощью особого математического соотношения. Открытый ключ пользователя известен всем другим пользователям, но это не позволяет вычислить закрытый ключ;

- закрытый ключ – уникальная последовательность данных, которая известна только владельцу ключа и сохраняется им в тайне;

- криптографические ключи – открытый и закрытый ключи;

- ключевой документ – контейнер с криптографическими ключами на ключевом носителе;

- компрометация ключа – хищение, утрата, разглашение, несанкциониро-ванное копирование и другие происшествия, в результате которых теряется доверие к тому, что используемые ключи обеспечивают безопасность информации;

- ПЭВМ – персональная электронно-вычислительная машина (персо-нальный компьютер);

- остальные термины и определения, используемые в настоящих правилах, должны пониматься в соответствии с законодательством Российской Федерации.

1.4. Настоящие правила являются обязательными для всех пользователей криптосредств.

2. Организация деятельности по эксплуатации криптосредств

2.1. При осуществлении деятельности с криптосредствами следует производить:

- установку и ввод в эксплуатацию криптосредств в соответствии с эксплуатационной и технической документацией к ним;

- проверку готовности криптосредств к использованию с составлением заключений о возможности их эксплуатации;

- обучение сотрудников, использующих криптосредства (пользователей криптосредств), работе с ними;

- поэкземплярный учет используемых криптосредств, эксплуатационной и технической документации к ним;

- учет пользователей криптосредств;

- контроль за соблюдением условий использования криптосредств, преду-смотренных эксплуатационной и технической документацией к ним;

- разбирательство и составление заключений по фактам нарушения условий использования криптосредств.

2.2. Пользователи криптосредств допускаются к работе с криптосред-ствами приказом оператора и несут персональную ответственность за сохранность криптосредств, ключевой, эксплуатационной и технической документации, эксплуатируемых пользователем.

2.3. Обеспечение функционирования и безопасности криптосредств возлагается на ответственного пользователя криптосредств, имеющего необхо-димый уровень квалификации, назначаемого приказом оператора (далее – ответственный пользователь криптосредств). Функции ответственного пользо-вателя криптосредств возлагаются на одного из пользователей криптосредств. На время отсутствия ответственного пользователя криптосредств должен быть назначен сотрудник, его замещающий.

2.4. Пользователи криптосредств обязаны соблюдать требования настоящих правил и других документов, принятых у оператора, регламентирующих эксплуатацию криптосредств, и несут ответственность за несоблюдение ими данных требований в соответствии с законодательством Российской Федерации.

2.5. Перед началом работы с криптосредствами пользователи крипто-средств должны пройти советующий инструктаж.

2.6. Ознакомление пользователей криптосредств с документами по эксплу-атации криптосредств осуществляет ответственный пользователь криптосредств под роспись в журнале прохождения обучения сотрудников по обеспечению безопасности персональных данных и работе со средствами защиты информации.

3. Учет, хранение, передача криптосредств и криптографических ключей к ним

3.1. Используемые или хранимые криптосредства, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземп-лярному учету ответственным пользователем криптосредств в журнале поэкземплярного учета криптосредств, эксплуатационной и технической документации к ним, ключевых документов (далее – журнал поэкземплярного учета).

3.2. При этом программные криптосредства должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функцио-нирование. Если аппаратные или аппаратно-программные криптосредства подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

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

3.4. Криптосредства подлежат учету с использованием индексов или условных наименований и регистрационных номеров.

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

3.6. В техническом (аппаратном) журнале, ведущемся непосредственно пользователем криптосредств, отражают данные об эксплуатации крипто-средств и другие сведения, предусмотренные эксплуатационной и технической документацией.

3.7. В случаях если нет прямых указаний в эксплуатационной или техниче-ской документации к криптосредствам о ведении технического (аппаратного) журнала на криптосредства, он не заводится.

3.8. Инсталлирующие криптосредства носители, эксплуатационная и техническая документация к криптосредствам, ключевые документы, в том числе резервные ключевые документы пользователей криптосредств, предназначенные для применения в случае компрометации действующих ключевых документов, хранятся у ответственного пользователя криптосредств.

3.9. Ключевые носители с криптографическими ключами хранятся у пользователей криптосредств.

3.10. Хранение осуществляется в шкафах (ящиках, хранилищах) индиви-дуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

3.11. Если у пользователя криптосредств отсутствует шкаф (ящик, хранилище) индивидуального пользования, ключевые носители с криптогра-фическими ключами по окончании рабочего дня в опечатанном пенале сдаются ответственному пользователю криптосредств.

3.12. Ключевые носители с неработоспособными криптографическими ключами ответственный пользователь криптосредств принимает от пользо-вателя криптосредств и делает соответствующие пометки журнале поэкземп-лярного учета. Неработоспособные криптографические ключи подлежат уничтожению.

3.13. Аппаратные средства, с которыми осуществляется штатное функцио-нирование криптосредств, а также аппаратные и аппаратно-программные криптосредства должны быть оборудованы средствами контроля за их вскрытием (опечатаны, опломбированы). Место опечатывания (опломбирования) должно быть таким, чтобы его можно было визуально контролировать.

3.14. При наличии технической возможности на время отсутствия пользо-вателей криптосредств указанные средства необходимо отключать от линии связи и убирать в опечатываемые хранилища. В противном случае по согласо-ванию с ответственным пользователем криптосредств необходимо предусмотреть организационно-технические меры, исключающие возможность использования криптосредств посторонними лицами.

3.15. Вскрытие системного блока ПЭВМ, на которой установлено криптосредство, для проведения ремонта или технического обслуживания должно осуществляться в присутствии ответственного пользователя криптосредств, который осуществляет контроль за криптосредствами во время проведения работ и производит опечатывание после окончания работ.

3.16. При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования криптосредств, указанные сообщения необходимо передавать только с использованием криптосредств.

3.17. Передача по техническим средствам связи криптоключей не допуска-ется, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

3.18. Передача криптосредств, эксплуатационной и технической докумен-тации к ним, ключевых документов допускается только между пользователями криптосредств и (или) ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. Такая передача между пользователями криптосредств должна быть санкционирована ответственным пользователем криптосредств.

3.19. Криптосредства и ключевые документы могут доставляться курьер-ской, фельдъегерской (в том числе ведомственной) связью или со специально выделенными руководителем сотрудниками при соблюдении мер, исключа-ющих бесконтрольный доступ к криптосредствам и ключевым документам во время доставки. Эксплуатационную и техническую документацию к криптосредствам можно пересылать заказными или ценными почтовыми отправлениями.

3.20. Для пересылки криптосредств и ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физи-ческого повреждения и внешнего воздействия, в особенности на записанную ключевую информацию. Криптосредства пересылают отдельно от ключевых документов к ним. На упаковках указывают организацию или ответственного сотрудника, для которых эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати. До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

3.21. Для пересылки криптосредств, эксплуатационной и технической документации к ним, ключевых документов следует подготовить сопроводи-тельное письмо, в котором необходимо указать, что посылается и в каком количестве, учетные номера изделий или документов, а также при необхо-димости – назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

3.22. Полученные упаковки вскрывает только ответственный пользователь криптосредств или ответственный сотрудник, для которого они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопро-водительном письме или сама упаковка и печать – их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к ее содержимому, то получатель составляет акт, который высылает отправителю. Полученные с такими отправлениями криптосредства и ключевые документы до получения указаний от отправителя применять не разрешается.

3.23. При обнаружении бракованных ключевых документов или крипто-ключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

3.24. Получение криптосредств, эксплуатационной и технической доку-ментации к ним, ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправи-тель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

4. Изготовление и перевыпуск криптографических ключей

4.1. Криптографические ключи изготавливаются в соответствии с эксплу-атационно-технической документацией на используемые криптосредства.

4.2. Криптографический ключ невозможно использовать если истек срок его действия.

4.3. Заказ на изготовление очередных ключевых документов, их изготов-ление и рассылку на места использования для своевременной замены действу-ющих ключевых документов следует производить заблаговременно.

4.4. Переход на новые криптографические ключи осуществляется в сроки, указанные в сертификате ключа подписи по заявлению пользователя криптосредств.

4.5. При замене криптографических ключей используют программное обеспечение в соответствии с эксплуатационной документацией на крипто-средства.

5. Мероприятия при компрометации криптографических ключей

5.1. К обстоятельствам, указывающим на возможную компрометацию криптографических ключей относится, включая, но не ограничиваясь, следующее:

- потеря ключевых носителей с криптографическими ключами;

- потеря ключевых носителей с криптографическими ключами с их после-дующим обнаружением;

- увольнение сотрудника, имевшего доступ к ключевым носителям с криптографическими ключами;

- исключение сотрудника из перечня лиц, допущенных к работе со сред-ствами криптографической защиты информации;

- возникновение подозрений на утечку информации;

- нарушение печати (пломбы) шкафов (ящиков, хранилищ), аппаратных средств, с которыми осуществляется штатное функционирование крипто-средств, а также аппаратных и аппаратно-программных криптосредств, где производилось опечатывание (опломбирование);

- неподконтрольный доступ посторонних лиц к ключевым носителям с криптографическими ключами (осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения);

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

5.2. В случае возникновения вышеуказанных обстоятельств пользователь криптосредств обязан незамедлительно прекратить работу с криптосредствами, в том числе обмен электронными документами, и уведомить ответственного пользователя криптосредств о возможной компрометации криптографических ключей.

5.3. Криптоключи, в отношении которых возникло подозрение в компро-метации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорен в эксплуатационной и технической документации к криптосредствам. В чрезвы-чайных случаях, когда отсутствуют криптоключи для замены скомпрометиро-ванных, допускается по решению ответственного пользователя криптосредств использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

5.4. О нарушениях, которые могут привести к компрометации крипто-ключей, их составных частей или передававшихся (хранящихся) с их использо-ванием конфиденциальных данных, пользователи криптосредств обязаны сообщать ответственному пользователю криптосредств.

5.5. Мероприятия по локализации последствий компрометации ключевых документов организует ответственный пользователь криптосредств.

6. Уничтожение криптографических ключей

6.1. Неиспользованные или выведенные из действия ключевые документы подлежат возвращению ответственному пользователю криптосредств или по его указанию должны быть уничтожены на месте.

6.2. При уничтожении криптографических ключей, находящихся на ключевых носителях, необходимо:

- установить наличие оригинала и количество копий криптографических ключей;

- проверить внешним осмотром целостность каждого ключевого носителя;

- установить наличие на оригинале и всех копиях ключевых носителей реквизитов путем сверки с записями в журнале поэкземплярного учета;

- убедиться, что криптографические ключи, находящиеся на ключевых носителях, действительно подлежат удалению;

- произвести уничтожение ключевой информации на оригинале и на всех копиях носителей.

6.3. В журнале поэкземплярного учета ответственным пользователем криптосредств производится отметка об уничтожении соответствующих криптографических ключей.

6.4. 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).

6.5. Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее приме-нение соответствующих ключевых носителей многократного использования регламентируются эксплуатационной и технической документацией к соответ-ствующим криптосредствам.

6.6. Бумажные и прочие сгораемые ключевые носители, а также эксплуата-ционная и техническая документация к криптосредствам уничтожаются путем сжигания или с помощью любых бумагорезательных машин.

6.7. Намеченные к уничтожению (утилизации) криптосредства подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документа-цией к криптосредствам процедура удаления программного обеспечения криптосредств и они полностью отсоединены от аппаратных средств. Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной реализации криптографических алгоритмов или иных функций криптосредств, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и тому подобное), разрешается использовать после уничтожения криптосредств без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

6.8. Ключевые документы должны быть уничтожены в сроки, указанные в эксплуатационной и технической документации к соответствующим крипто-средствам. Если срок уничтожения эксплуатационной и технической докумен-тацией не установлен, то ключевые документы должны быть уничтожены не позднее 10 суток после вывода их из действия (окончания срока действия). Факт уничтожения оформляется в соответствующих журналах поэкземпляр-ного учета. В эти же сроки с отметкой в техническом (аппаратном) журнале подлежат уничтожению разовые ключевые носители и ранее введенная и хранящаяся в криптосредствах или иных дополнительных устройствах ключевая информация, соответствующая выведенным из действия крипто-ключам. Хранящиеся в криптографически защищенном виде данные следует перешифровать на новых криптоключах.

6.9. Разовые ключевые носители, а также электронные записи ключевой информации, соответствующей выведенным из действия криптоключам, непосредственно в криптосредствах или иных дополнительных устройствах уничтожаются пользователями криптосредств самостоятельно под расписку в техническом (аппаратном) журнале.

6.10. Ключевые документы уничтожаются либо пользователями крипто-средств, либо ответственным пользователем криптосредств под расписку в соответствующих журналах поэкземплярного учета. При этом пользователям криптосредств разрешается уничтожать только использованные непосредственно ими (предназначенные для них) криптоключи. После уничтожения пользователи криптосредств должны уведомить об этом (телефонограммой, устным сообщением по телефону и тому подобное) ответственного пользователя криптосредств.

Уничтожение большого объема ключевых документов производит комиссия с оформлением акта. 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 доку-ментов, инсталлирующих криптосредства 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 соответству-ющих журналах поэкземплярного учета.

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

7.1. Размещение, специальное оборудование, охрана и организация режима в помещениях, где установлены криптосредства или хранятся ключевые документы к ним (далее – режимные помещения), должны обеспечивать сохранность конфиденциальных данных, криптосредств и ключевых документов к ним.

7.2. Режимные помещения должны иметь прочные входные двери с замками, гарантирующими надежное закрытие помещений в нерабочее время.

7.3. Окна помещений, расположенных на первых или последних этажах зданий, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение в режимные помещения посторонних лиц, необходимо оборудовать металлическими решетками, или ставнями, или охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в режимные помещения.

7.4. Размещение, специальное оборудование, охрана и организация режима в режимных помещениях должны исключить возможность неконтролируемого проникновения или пребывания в них посторонних лиц, а также просмотра посторонними лицами ведущихся там работ.

7.5. Двери режимных помещений должны быть закрыты на замок и могут открываться только для санкционированного прохода сотрудников и посетителей. Ключи от входных дверей нумеруют, учитывают и выдают сотрудникам, имеющим право допуска в режимные помещения, под расписку в журнале учета хранилищ. Дубликаты ключей от входных дверей таких помещений следует хранить в сейфе.

7.6. Для предотвращения просмотра извне режимных помещений их окна должны быть защищены.

7.7. Режимные помещения, как правило, должны быть оснащены охранной сигнализацией, связанной со службой охраны здания. Исправность сигнали-зации периодически необходимо проверять представителям службы охраны с отметкой в соответствующих журналах.

7.8. Для хранения ключевых документов, эксплуатационной и технической документации, инсталлирующих криптосредства носителей, должно быть предусмотрено необходимое число надежных металлических хранилищ, обору-дованных внутренними замками с двумя экземплярами ключей и кодовыми замками или приспособлениями для опечатывания замочных скважин. Дубликаты ключей от хранилищ сотрудники хранят в сейфе ответственного пользователя криптосредств.

7.9. По окончании рабочего дня режимное помещение и установленные в нем хранилища должны быть закрыты, хранилища опечатаны. Находящиеся в пользовании ключи от хранилищ должны быть сданы под расписку в соот-ветствующем журнале.

7.10. При утрате ключа от хранилища или от входной двери в режимное помещение замок необходимо заменить или переделать его секрет с изготов-лением к нему новых ключей с документальным оформлением. Если замок от хранилища переделать невозможно, то такое хранилище необходимо заменить. Порядок хранения ключевых и других документов в хранилище, от которого утрачен ключ, до изменения секрета замка устанавливает ответственный пользователь криптосредств.

7.11. В обычных условиях режимные помещения, находящиеся в них опеча-танные хранилища могут быть вскрыты только сотрудниками, имеющими доступ в данные помещения, или руководителем.

7.12. При обнаружении признаков, указывающих на возможное несанкцио-нированное проникновение в эти помещения или хранилища посторонних лиц, о случившемся должно быть немедленно сообщено ответственному пользова-телю криптосредств или руководителю. Прибывший ответственный пользователь криптосредств должен оценить возможность компрометации хранящихся ключевых и других документов, составить акт и принять при необ-ходимости меры к локализации последствий компрометации конфиден-циальных данных и к замене скомпрометированных криптоключей.

7.13. Размещение и монтаж криптосредств, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными криптосредствами.

Приложение 6

к постановлению Администрации города

от \_\_\_\_\_\_\_\_\_\_\_\_\_ № \_\_\_\_\_\_\_\_\_

Руководство

пользователя в части обеспечения безопасности персональных данных

при их обработке в информационных системах персональных данных

1. Общие положения

1.1. Пользователи получают допуск к работам в информационной системе персональных данных (далее – ИСПДн) на основании регламентов разгра-ничения прав доступа в ИСПДн, принятых у оператора.

1.2. Пользователи ИСПДн в пределах своих функциональных обязанностей обеспечивают безопасность информации, обрабатываемой, передаваемой и хранимой в ИСПДн.

1.3. Пользователи ИСПДн руководствуются положениями настоящего руководства и других руководящих документов по защите информации и персональных данных (далее – ПДн), принятых у оператора, а также требова-ниями эксплуатационных документов на используемые средства защиты информации (далее – СЗИ), технические и программные средства ИСПДн.

1.4. Методическое руководство деятельностью пользователей ИСПДн осуществляется уполномоченной организацией по обеспечению безопасности персональных данных при их обработке в муниципальных ИСПДн (далее – уполномоченная организация).

2. Обязанности пользователей в части обеспечения информационной безопасности при работе в ИСПДн

2.1. Каждый пользователь ИСПДн, участвующий в рамках своих функцио-нальных обязанностей в процессах автоматизированной обработки информации и имеющий доступ к аппаратным средствам, программному обеспечению и данным ИСПДн, несет персональную ответственность за свои действия и обязан:

2.1.1. Хранить в тайне сведения о ПДн субъектов, ставшие известными ему в соответствии с родом работы.

2.1.2. Хранить в тайне свой пароль (пароли).

2.1.3. В соответствии с требованиями инструкции по организации парольной защиты менять свой пароль (пароли) с установленной периодичностью.

2.1.4. Выполнять требования инструкции по организации антивирусной защиты в части, касающейся действий пользователей рабочих станций ИСПДн.

2.1.5. Строго соблюдать:

- требования настоящего руководства;

- требования документов по защите информации и ПДн, принятых у оператора;

- правила работы с общесистемным и прикладным программным обеспе-чением, средствами защиты информации, используемыми у оператора.

2.1.6. Для хранения ПДн использовать только учтенные установленным порядком машинные носители информации, соблюдать порядок учета, обращения и хранения учтенных машинных носителей информации (гибкие машинные носители, оптические диски, flash-диски и другие носители) согласно правилам работы с носителями персональных данных.

2.1.7. При выходе в течение рабочего дня из помещения, в котором располагаются элементы ИСПДн, убирать документы и машинные носители информации, содержащие ПДн, в предназначенные для этого хранилища (запираемые шкафы, ящики столов, тумбочки), закрывать и при необходимости опечатывать, а также закрывать само помещение.

2.1.8. Располагать экран видеомонитора в помещении во время работы так, чтобы исключалась возможность ознакомления посторонними лицами с отображаемой на нем информацией.

2.1.9. Немедленно оповещать сотрудников уполномоченной организации и ставить в известность ответственного за организацию обработки персо-нальных данных в случае утери индивидуального устройства идентификации (при наличии) или при подозрении компрометации личного пароля, а также при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на системном блоке или иных фактов совершения в его отсут-ствие попыток несанкционированного доступа;

- несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств;

- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ПЭВМ, выхода из строя или неустой-чивого функционирования узлов ПЭВМ или периферийных устройств (дисководов, принтера и тому подобное), а также перебоев в системе электроснабжения;

- некорректного функционирования установленных на ПЭВМ технических средств защиты, не предусмотренных формуляром ПЭВМ (техническим паспортом ИСПДн) отводов кабелей и подключенных устройств.

2.1.10. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленной за ним ПЭВМ в подразделении.

2.2. Пользователям категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ИСПДн в неслужебных целях;

- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств рабочих станций или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами рабочих станций (техническим паспортом ИСПДн);

- осуществлять обработку ПДн в присутствии посторонних (не допущенных к данной информации) лиц;

- записывать и хранить информацию, содержащую сведения о ПДн, на неучтенных машинные носителях информации;

- оставлять включенной без присмотра свою рабочую станцию, не активи-зировав временную блокировку экрана и клавиатуры;

- передавать кому-либо свое индивидуальное устройство идентификации (при наличии) или другие реквизиты разграничения доступа (кроме сотруд-ников уполномоченной организации или ответственного за организацию обработки персональных данных установленным порядком);

- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации (при наличии), машинные носители и распечатки, содержащие сведения ПДн;

- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. При обнаружении такого рода ошибок ставить в известность сотрудников уполномоченной организации;

- использовать нештатные технические средства и системы;

- самостоятельно вносить изменения в состав, конфигурацию и размещение технических средств;

- использовать нештатные программные средства;

- проводить обработку ПДн при неисправно работающих средствах защиты информации;

- вносить изменения в средства защиты информации, используемые на объекте информатизации;

- допускать к работам в ИСПДн лиц, не имеющих допуска к этим работам;

- обрабатывать информацию в случае, если имеют место неисправности, создающие предпосылки для утечки ПДн.

3. Права пользователей ИСПДн

3.1. Обрабатывать ПДн в соответствии и в рамках полученного служебного задания на выполнение работ.

3.2. Обращаться к сотрудникам уполномоченной организации с просьбой об оказании методической помощи.

4. Ответственность пользователей ИСПДн

4.1. Пользователи ИСПДн несут ответственность в полном объеме в соответствии с действующим законодательством Российской Федерации за разглашение сведений, содержащих ПДн, ставших известными им в соответствии с родом работы, а также утрату носителей информации и выходных документов, содержащих ПДн.

5. Правила работы в сетях связи общего пользования и (или) сетях между-народного информационного обмена

5.1. Работа в сетях связи общего пользования и (или) международного информационного обмена (сети Интернет и других) (далее – сеть) на элементах ИСПДн должна проводиться при служебной необходимости с соблюдением правил, установленных настоящим руководством.

5.2. При работе в сети запрещается:

- осуществлять работу при отключенных средствах защиты информации (антивирусов и других);

- передавать по сети защищаемую информацию без использования средств защиты каналов связи;

- скачивать из сети программное обеспечение;

- посещение сайтов сомнительной репутации (порно-сайты, сайты, содер-жащие нелегально распространяемое ПО, и другие);

- нецелевое использование подключения к сети.

5.3. При работе с ресурсами сети запрещается:

- разглашать коммерческую информацию и ПДн, ставшие известными по служебной необходимости либо иным путем;

- распространять защищаемые авторскими правами материалы, затраги-вающие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

- публиковать, загружать и распространять материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети, а также размещать ссылки на вышеука-занную информацию;

- загружать и запускать исполняемые либо иные файлы без предвари-тельной проверки на наличие вирусов установленным антивирусным пакетом;

- использовать анонимные прокси-серверы;

- использовать программные и аппаратные средства, позволяющие получить доступ к ресурсу, запрещенному к использованию политикой оператора.

5.4. Возможность получить доступ к ресурсу не является гарантией того, что запрошенный ресурс является разрешенным политиками оператора.

6. Правила работы с корпоративной электронной почтой

6.1. Электронная почта является собственностью оператора и может быть использована только в служебных целях. Использование электронной почты в иных целях категорически запрещено.

6.2. При работе с корпоративной системой электронной почты пользова-телям запрещается:

- использовать адрес корпоративной почты для оформления подписок без предварительного согласования;

- публиковать свой адрес либо адреса других сотрудников на общедоступных интернет-ресурсах (форумы, конференции и тому подобное) без предваритель-ного согласования;

- открывать вложенные файлы во входящих сообщениях без предвари-тельной проверки антивирусными средствами, даже если отправитель письма хорошо известен;

- рассылать через электронную почту материалы, содержащие вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в сети, а также ссылки на вышеуказанную информацию;

- распространять защищаемые авторскими правами материалы, затрагива-ющие какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ними права третьей стороны;

- распространять информацию, содержание и направленность которой запрещены международным законодательством и законодательством Российской Федерации, включая материалы, носящие вредоносную, угрожающую, клеветни-ческую, непристойную информацию, а также информацию, оскорбляющую честь и достоинство других лиц, материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, и так далее;

- распространять информацию ограниченного доступа, представляющую коммерческую тайну или информацию со сведениями ПДн, ставшей известной по служебной необходимости либо иным путем;

- предоставлять, кому бы то ни было пароль доступа к своему почтовому ящику.

7. Выдержки из статей Уголовного кодекса Российской Федерации

Статья 183. Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну

1. Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз, а равно иным незаконным способом в целях разглашения либо незаконного использования этих сведений – наказываются штрафом в размере от ста до двухсот мини-мальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев либо лишением свободы на срок до двух лет.

2. Незаконные разглашение или использование сведений, составляющих коммерческую или банковскую тайну, без согласия их владельцев, совершенные из корыстной или иной личной заинтересованности и причи-нившие крупный ущерб, – наказывается штрафом в размере от двухсот до пятисот минимальных окладов оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев либо лишением свободы на срок до трех лет со штрафом в размере до пятидесяти минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период до одного месяца либо без такового.

Статья 272. Неправомерный доступ к компьютерной информации

1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование инфор-мации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказываются штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, – наказывается штрафом в размере от пятисот до восьмисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от пяти до восьми месяцев, либо исправительным работам на срок от одного года до двух лет, либо арестом на срок от трех до шести месяцев, либо лишением свободы на срок до пяти лет.

Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ

1. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сетей, а равно использование либо распро-странение таких программ или машинных носителей с такими программами – наказывается лишением свободы на срок до трех лет со штрафом в размере от двухсот до пятисот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от двух до пяти месяцев.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия, – наказывается лишением свободы на срок от трех до семи лет.

Статья 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

1. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – наказывается лишением права занимать определенные должности или заниматься определенной деятельно-стью на срок до пяти лет, либо обязательными работами на срок от ста восьми-десяти до двухсот сорока часов, либо ограничением свободы на срок до двух лет.

2. То же деяние, повлекшее по неосторожности тяжкие последствия, – наказывается лишением свободы на срок до четырех лет.

Статья 293. Халатность

Халатность, то есть неисполнение или ненадлежащее исполнение должно-стным лицом своих обязанностей вследствие недобросовестного или небреж-ного отношения к службе, если это повлекло существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства, – наказывается штрафом в размере от ста до двухсот минимальных размеров оплаты труда или в размере заработной платы или иного дохода осужденного за период от одного до двух месяцев, либо обязательными работами на срок от ста двадцати до ста восьмидесяти часов, либо исправительными работами на срок от шести месяцев до одного года, либо арестом на срок до трех месяцев.