Положение

по организации и проведению работ

по защите персональных данных при их обработке

в информационных системах в зоне ответственности

ООО МИКС

(Редакция 1)

Чита

2017 г.

Приложение № ___

УТВЕРЖДЕНО

приказом генерального директора ООО Микс

от «28_»_июня_2017 г. №_3.6.17__

Положение по организации и проведению работ по защите персональных данных при их обработке в информационных системах в зоне ответственности ООО МИКС

Оглавление

1 Назначение....4

2 Общие положения....4

2.1 Область применения....4

2.2 Нормативные ссылки....4

2.3 Термины, определения и сокращения....5

3 Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн....9

3.1 Порядок определения защищаемой информации и классификации ИСПДн....11

3.2 Порядок разработки, ввода в действие и эксплуатацию СЗПДн....12

4 Основные требования и правила по обеспечению безопасностиПДн при их обработке в ИСПДн Общества....20

4.1 Требования по организации разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации....22

4.2 Требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где размещены средства ИСПДн....25

4.3 Правила обеспечения безопасности ПДн при использовании съемных носителей ПДн....26

4.4 Требования к резервированию ИР....27

4.6 Требования по обеспечению безопасности при работе в сети Интернет....30

4.7 Правила использования ПО и аппаратных средств ИСПДн....31

4.8 Требования по обеспечению безопасности при применении средств криптографической защиты информации....35

5. Порядок организации внутреннего обучения персонала правилам и мерам защиты ПДн....36

5.2 Самостоятельное изучение....38

6. Ответственность должностных лиц за обеспечениебезопасности ПДн, своевременность и качество формирования требований по защите информации, за качество и научно- технический уровень разработки СЗПДн....38

7 Порядок контроля обеспечения уровня защищенности ПДн и оценки соответствия ИСПДн....39

7.1 Внутренний контроль режима безопасности ПДн и оценки соответствия ИСПДн требованиям безопасности ПДн....40

7.2 Обследование защищенности ПДн внешней специализированной организацией....41

7.3 Порядок оценки соответствия ИСПДн требованиям безопасности ПДн....42

8 Хранение и архивирование....42

9 Рассылка и актуализация....42

1 Назначение

Данное Положение по организации и проведению работ по защите

персональных данных при их обработке в информационных системах в зоне ответственности ООО МИКС(Далее –Положение) регламентирует вопросы обеспечения безопасности персональныхданных при их обработке в информационных системах в зоне ответственности

ООО МИКС(Далее – ОБЩЕСТВО) и определяет порядок организации работ по созданию и эксплуатации системы защиты персональных данных (СЗПДн).

Данное Положение разработано с целью обеспечения защиты персональных данных работников, абонентов и иных категорий граждан в соответствии с требованиями действующего законодательства Российской Федерации.

Данное Положение вводится в действие впервые с момента его утверждения.

2 Общие положения

2.1 Область применения

Требования данного Положения распространяются на всех работников

ООО МИКС(далее – Общество).

2.2 Нормативные ссылки

В данном Положении использованы ссылки на следующие нормативные

документы:

— Федеральный закон от 27.07.2006 г. № 152-ФЗ «О персональных данных»

(ред. от 25.07.2011 г.);

— Требования к материальным носителям биометрических персональных

данных и технологиям хранения таких данных вне информационных систем

персональных данных (Постановление Правительства РФ от 6 июля 2008 г.

№512);

— Положение об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации (Постановление Правительства РФ от 15 сентября 2008 г. №687);

— Требования к защите персональных данных при их обработке в информационных системах персональных данных (Постановление Правительства РФ от 1 ноября 2012 г. №1119);

— Положение о методах и способах защиты информации в информационных системах персональных данных (утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58);

— Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282);

2.3 Термины, определения и сокращения

Для целей Положения в нем используются термины и сокращения, определенные в Глоссарии терминов и определений ООО МИКС, а также следующие:

Автоматизированная обработка персональных данных – обработка персональных данных (ПДн) с помощью средств вычислительной техники.

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

Администратор безопасности информации (администратор безопасности) – Сотрудник ООО МИКС, ответственный за защиту информационных систем персональных данных (ИСПДн) от несанкционированного доступа (НСД) к информации.

Администратор информационной системы персональных данных – администратор автоматизированной системы, администратор локальной

вычислительной сети, администратор баз данных, администратор информационного ресурса (ИР) – ответственный за функционирование ИСПДн в установленном штатном режиме работы.

Блокирование персональных данных – временное прекращение обработки ПДн (за исключением случаев, если обработка необходима для уточнения ПДн).

Владелец информации (информационного ресурса) – структурное подразделение ООО МИКС, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец устанавливает в пределах своей компетенции режим и правила обработки информации, защиты ИР, доступа к ИР, условия копирования и тиражирования ИР (в распоряжении на создание ИР или в виде отдельных регламентов).

Доступ к информации – возможность получения информации и ее использования.

Информационная система персональных данных (ИСПДн) – совокупность содержащихся в базах данных ПДн и обеспечивающих их обработку информационных технологий и технических средств (ТС).

Инцидент информационной безопасности – появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности (отказ в обслуживании, сбор информации, НСД и т.д.).

Использование персональных данных – действия (операции) с ПДн, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПДн или других лиц либо иным образом затрагивающих права и свободы субъекта ПДн или других лиц.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с

ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

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

Общество – ООО МИКС.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции),

совершаемые с ПДн (в данном Положении – ООО МИКС).

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту ПДн).

Распространение персональных данных – действия, направленные на раскрытие ПДн неопределенному кругу лиц.

Технические средства, позволяющие осуществлять обработку персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие ТС обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационной системе.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Угроза безопасности персональных данных – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение ПДн, а также иных несанкционированных действий при их обработке в ИСПДн.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание ПДн в ИСПДн и (или) в результате которых уничтожаются материальные носители ПДн.

АРМ – автоматизированное рабочее место.

АС – автоматизированная система.

ВП – вредоносная программа.

ИБ – информационная безопасность.

ИР – информационный ресурс.

ИС – информационная система.

ИСПДн – информационная система персональных данных.

ИТ – информационная технология.

НСД – несанкционированный доступ.

ОРД – организационно-распорядительные документы.

ОС – операционная система.

ОТСС – основные технические средства и системы.

ПДн – персональные данные.

ПО – программное обеспечение.

СВТ – средство вычислительной техники.

СЗИ – средство защиты информации.

СЗПДн – система защиты персональных данных.

СКЗИ – средство криптографической защиты информации.

СТР-К – «Специальные требования и рекомендации по технической защите конфиденциальной информации», утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

СУБД – система управления базами данных.

ТС – техническое средство.

ФСБ России – Федеральная служба безопасности России.

ФСТЭК России – Федеральная служба по техническому и экспортному контролю России.

3 Порядок организации и проведения работ по обеспечению безопасности ПДн при их обработке в ИСПДн

Под организацией обеспечения безопасности ПДн при их обработке в ИСПДн понимается формирование совокупности мероприятий, осуществляемых на всех стадиях жизненного цикла ИСПДн, согласованных по цели, задачам, месту и времени, направленных на предотвращение (нейтрализацию) и парирование угроз безопасности ПДн в ИСПДн, восстановление нормального функционирования ИСПДн после нейтрализации угрозы, с целью минимизации как непосредственного, так и опосредованного ущерба от возможной реализации таких угроз.

Организация работ по защите ПДн предусматривает определение:

— на основании законодательства и других нормативных актов, регулирующих

деятельность Общества, перечня ПДн, обрабатываемых в информационных системах (ИС) Общества;

— порядка классификации ИС Общества как ИСПДн;

— порядка разработки, ввода в действие и эксплуатацию ИСПДн в части реализации мероприятий по обеспечению безопасности ПДн;

— порядка взаимодействия между ответственными за обеспечение безопасности ПДн и эксплуатирующими подразделениями (администраторами) по вопросам обеспечения безопасности ПДн;

— порядка привлечения структурных подразделений Общества и специализированных сторонних организаций к разработке и эксплуатации СЗПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн;

— ответственности должностных лиц за обеспечение безопасности ПДн, своевременность и качество формирования требований по защите информации, за качество и научно-технический уровень разработки СЗПДн;

— порядка контроля обеспечения требуемого уровня защищенности ПДн.

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн назначается приказом лицо, ответственное за обеспечение безопасности ПДн.

Непосредственно исполнение работ по защите информации (ПДн) в ИСПДн с использованием средств автоматизации возлагается на руководителей соответствующих структурных подразделений ОБЩЕСТВО.

Для проведения классификации ИСПДн соответствующим приказом назначается специальная внутренняя комиссия (рабочая группа).

Для придания необходимого статуса рабочей группе могут издаваться

соответствующие распоряжения, в которых, в частности, даются указания всем руководителям структурных подразделений ОБЩЕСТВО об оказании содействия и необходимой помощи в работе комиссии (рабочей группе) при проведении работ.

Для оказания помощи на время работы группы в подразделениях руководителями этих структурных подразделений должны выделяться сотрудники, владеющие детальной информацией по вопросам обработки ПДн в данных подразделениях.

Проведение предпроектного обследования ИСПДн, разработка и реализация СЗПДн может осуществляться как сотрудниками ОБЩЕСТВО (специалистом по ИБ, сотрудниками подразделения ИТ, так и на договорной основе другими специализированными организациями, имеющими соответствующие лицензии.

Научно-техническое и методическое руководство, непосредственная организация работ по созданию (модернизации) СЗПДн и контроль за эффективностью использования предусмотренных мер возлагается на специалиста по ИБ (подразделение ИБ).

В случае разработки СЗПДн или ее отдельных компонент специализированными организациями, подразделение ИТ отвечает за организацию и проведение мероприятий по защите информации. Разработка, внедрение и эксплуатация СЗПДн осуществляется во взаимодействии разработчика с подразделением ИТ.

Контроль за реализацией проектных решений возлагается на руководителя подразделения ИТ.

3.1 Порядок определения защищаемой информации и классификации ИСПДн

На основании законодательства и других нормативных актов, регулирующих деятельность Общества, внутренней комиссией (рабочей группой), назначенной приказом для каждой ИСПДн определяется перечень ПДн, уточняются цели и основание обработки ПДн, а также срок хранения и условия прекращения обработки.

Целью классификации ИС Общества как ИСПДн является определение по еѐ результатам перечня обоснованных организационных и технических мероприятий, позволяющих выполнить требования по обеспечению безопасности ПДн с учѐтом особенностей конкретной ИСПДн. Классификация может проводиться на этапе создания ИС или в ходе их эксплуатации (для ранее введенных в эксплуатацию и (или) модернизируемых ИС).

Классификация ИСПДн проводится внутренней комиссией (рабочей группой) и включает в себя следующие этапы:

— сбор и анализ исходных данных по ИС;

— присвоение ИС соответствующего уровня защищенности и его документальное оформление.

— при проведении классификации ИСПДн внутренней комиссией (рабочей

группой) определяется:

— заданные оператором характеристики безопасности ПДн, обрабатываемых в ИС;

— структура ИС;

— наличие подключений ИС к сетям связи общего пользования и (или) сетям международного информационного обмена;

— режим обработки ПДн;

— режим разграничения прав доступа пользователей ИС;

— местонахождение ТС ИС.

В случае выделения в составе ИС подсистем, каждая из которых является ИС, ИС в целом присваивается уровень защищенности, соответствующий наиболее высокому уровню защищенности входящих в нее подсистем.

Предложения комиссии (рабочей группы) по отнесению ИС к определенному уровню защищенности, согласовываются с владельцами ИСПДн.

Результаты классификации ИСПДн Общества оформляются актом.

Сформированные по результатам классификации материалы являются неотъемлемой частью организационно-распорядительной документации (ОРД) ИСПДн и относятся к информации конфиденциального характера. Оригиналы ОРД ИСПДн хранятся у лица, ответственного за организацию работ по защите ПДн Уровень защищенности ИСПДн может быть пересмотрен комиссией (рабочей группой) в установленном порядке в следующих случаях:

— на основе результатов проведенного анализа и оценки угроз безопасности

ПДн с учетом особенностей и (или) изменений конкретной ИС;

— по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности ПДн при их обработке в ИС.

3.2 Порядок разработки, ввода в действие и эксплуатацию СЗПДн

Предусматриваются следующие стадии разработки и сопровождения СЗПДн:
— предпроектная стадия – включает предпроектное обследование ИСПДн и

разработку технического (частного технического) задания на создание СЗПДн;

— стадия проектирования (разработки проектов) и реализации ИСПДн – включает разработку СЗПДн в составе ИСПДн;

— стадия ввода в действие СЗПДн – включает предварительные испытания, опытную эксплуатацию и приемо-сдаточные испытания средств защиты, а также оценку соответствия ИСПДн требованиям безопасности информации.

3.2.1 Предпроектная стадия

На предпроектной стадии проводится предпроектное обследование ИСПДн и разработка технического (частного технического) задания на создание СЗПДн.

Выполнение данных работ может быть поручено на договорной основе специализированной сторонней организации, имеющей соответствующую лицензию.

Условия соблюдения конфиденциальности специалистами привлекаемой сторонней организации при проведении работ оформляются в соответствии с установленным в Обществе порядком.

При проведении предпроектного обследования ИСПДн осуществляются следующие работы:

— определяется перечень ПДн, подлежащих защите;

— определяются условия расположения ИСПДн относительно границ

контролируемой зоны;

— определяются конфигурация и топология ИСПДн и ее компонент;

— определяются физические, функциональные и технологические связи как

между компонентами ИСПДн, так и между ИСПДн и другими системами;

— определяется состав ТС и систем ИСПДн;

— определяется состав общесистемных и программных средств ИСПДн;

— определяются режимы обработки ПДн в ИСПДн в целом и в отдельных

компонентах;

— определяется степень участия персонала в обработке ПДн и характер

их взаимодействия между собой;

— определяется класс ИСПДн;

— определяются (уточняются) угрозы безопасности и модель вероятного

нарушителя применительно к конкретным условиям функционирования

ИСПДн;

— определяются мероприятия по обеспечению безопасности ПДн в процессе

проектирования СЗПДн.

По результатам предпроектного обследования с учетом установленного уровня защищенности ИСПДн задаются конкретные требования по обеспечению безопасности ПДн, включаемые в техническое (частное техническое) задание на разработку СЗПДн.

Техническое (частное техническое) задание на разработку СЗПДн должно содержать:

— обоснование разработки СЗПДн;

— исходные данные о создаваемой (модернизируемой) ИСПДн в техническом, программном, информационном и организационном аспектах;

— класс ИСПДн;

— ссылку на нормативные документы, с учетом которых будет разрабатываться

СЗПДн и приниматься в эксплуатацию ИСПДн;

— конкретизацию мероприятий и требований к СЗПДн;

— перечень предполагаемых к использованию сертифицированных средств

защиты информации (СЗИ);

— обоснование проведения разработок собственных СЗИ при невозможности или нецелесообразности использования имеющихся на рынке сертифицированных СЗИ;

— состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн.

3.2.2 Стадия проектирования и реализации СЗПДн

Проектирование и реализация СЗПДн проводится на основании требований, изложенных в техническом (частном техническом) задании на разработку СЗПДн.

При разработке СЗПДн в составе ИСПДн проводятся следующие мероприятия:

— разработка задания и проекта на строительные, строительно-монтажные работы (или реконструкцию) ИСПДн в соответствии с требованиями технического (частного технического) задания на разработку СЗПДн;

— разработка раздела технического проекта на ИСПДн в части защиты информации;

— проведение строительно-монтажных работ в соответствии с проектной документацией;

— использование серийно выпускаемых ТС обработки, передачи и хранения информации;

— разработка мероприятий по защите информации в соответствии с предъявляемыми требованиями;

— использование сертифицированных технических, программных и программно-технических СЗИ и их установка;

— сертификация по требованиям безопасности информации программных СЗИ

в случае, если на рынке отсутствуют требуемые сертифицированные СЗИ;

— разработка и реализация разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации;

— определение подразделений и назначение лиц, ответственных за эксплуатацию СЗИ, с их обучением по направлению безопасности ПДн;

— разработка рабочей, эксплуатационной документации на СЗПДн, а также ОРД

по защите информации (приказов, инструкций и других документов);

— выполнение других мероприятий, характерных для конкретных ИСПДн и направлений обеспечения безопасности ПДн.

Проектная документация подлежит согласованию с руководителем

подразделения ИБ и ИТ.

3.2.3 Стадия ввода в действие СЗПДн

На стадии ввода в действие СЗПДн выполняются следующие мероприятия:

— опытная эксплуатация средств защиты в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн и отработки технологического процесса обработки (передачи) информации;

— приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;

— организация охраны и физической защиты помещений ИСПДн, исключающих НСД к ТС ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации;

— оценка соответствия ИСПДн требованиям безопасности ПДн.

Ввод в эксплуатацию СЗПДн осуществляется на основании приказа, который издается на основании положительных результатов оценки соответствия ИСПДн Общества требованиям безопасности ПДн.

Эксплуатация СЗПДн осуществляется в полном соответствии с утвержденной организационно-распорядительной и эксплуатационной документацией с учетом требований и положений, изложенных в настоящем документе.

При определении порядка проведения технического обслуживания и ремонтных работ в СЗПДн должно быть учтено требование исполнения данных работ только уполномоченными сотрудниками Общества (или в их присутствии), назначенными ответственными за обслуживание (сопровождение) СЗПДн.

Все процедуры, связанные с изменением конфигурации СЗПДн, проведением технического обслуживания и ремонтных работ на ТС СЗПДн должны предусматривать документирование объемов и сроков выполненных работ, а также лиц (организаций), проводивших эти работы.

3.3 Порядок привлечения структурных подразделений Общества и специализированных сторонних организаций к разработке и эксплуатации ИСПДн, их задачи и функции на различных стадиях создания и эксплуатации ИСПДн

Для организации и обеспечения безопасности ПДн при их обработке в ИСПДн ответственным структурным подразделением за обеспечение безопасности ПДн соответствующим приказом назначается подразделение ИБ.

3.3.1 Функции подразделения ИТ

Подразделение ИТ обеспечивает методическое руководство, разработку

требований к мерам защиты ИСПДн Общества и контроль за эффективностью

использования предусмотренных мер защиты информации.

Подразделение ИТ обеспечивает подготовку предложений по совершенствованию и реализации положений Политики безопасности информации и контролирует выполнение установленных требований в структурных подразделениях Общества.

В целом, Подразделение ИТ осуществляет следующие функции:

— разрабатывает предложения по определению уровня защищенности объектов ИСПДн и автоматизированной системы (АС);

— участвует в организации работ по выявлению актуальных угроз безопасности ПДн;

— осуществляет методическое руководство и участвует в разработке (согласовании) конкретных требований по защите ПДн и разработке технического (частного технического) задания на создание СЗПДн;

— согласовывает выбор конкретных средств обработки ПДн, технических и программных средств защиты;

— осуществляет контроль реализации проектных решений на создание СЗПДн;

— участвует в организации работ по оценке соответствия ИСПДн предъявляемым требованиям по обеспечению безопасности ПДн;

— участвует в организации разработки ОРД по защите информации в ИСПДн;

— проводит контроль требуемого уровня обеспечения защищенности ПДн при эксплуатации СЗПДн, в том числе контроль соблюдения условий

использования СЗИ;

— участвует в организации обучения должностных лиц Общества, ответственных за эксплуатацию СЗИ, по направлению обеспечения безопасности ПДн;

— участвует в организации охраны и физической защиты помещений Общества, в которых размещаются средства обработки ПДн, исключающих НСД к ТС ИСПДн, их хищение и нарушение работоспособности, хищение носителей информации.

3.3.2 Функции подразделения ИТ

Подразделение ИТ осуществляет следующие функции:

— устанавливает правила работы с информацией, ТС и правила использованияПДн в рамках своей ответственности согласно возможностям, функциям, предназначению и степени защищенности этих средств, ресурсов и требованиям к защите и доступности ПДн;

— осуществляет предоставление ИТ-сервисов всем структурным

подразделениям Общества, отвечает за их целостность и доступность;

— обеспечивает разграничение доступа к ПДн в процессе их использования,

контроль над ходом информационных процессов.

3.3.3 Функции сторонних специализированных организаций

Привлечение для разработки СЗПДн или ее отдельных компонент сторонних специализированных организаций осуществляется в соответствии с порядком, устанавливаемым нормативными ОРД Общества.

В случае привлечения для обеспечения безопасности ПДн сторонних специализированных организаций должны выполняться следующие условия:

— наличие у организации лицензии на право проведения работ по технической защите конфиденциальной информации;

— оформление соглашения о неразглашении конфиденциальных сведений;

— проведение инструктажа исполнителей работ по вопросам ИБ;

— другие условия, устанавливаемые соответствующими нормативными и ОРД Общества.

На предпроектной стадии на сторонние специализированные организации возлагаются следующие функции:

— уточнение перечня ПДн, подлежащих защите;

— определение условий расположения ИСПДн относительно границ контролируемой зоны;

— определение конфигурации и топологии ИСПДн в целом, и ее отдельных компонент, физические, функциональные и технологические связи как внутри ИСПДн, так и с другими системами различного назначения;

— определение ТС и систем, включаемых в состав ИСПДн, условий их расположения, общесистемных и прикладных программных средств;

— определение режимов обработки ПДн в ИСПДн;

— разработка предложений по уточнению уровня защищенности ИСПДн;

— уточнение степени участия персонала в обработке ПДн, характера их взаимодействия между собой;

— определение (уточнение) угроз безопасности ПДн с учѐтом конкретных условий функционирования ИСПДн, разработка проекта частной модели угроз;

— участие в разработке (согласовании) конкретных требований по защите ПДн и разработке технического (частного технического) задания на создание СЗПДн.

На стадии проектирования на сторонние специализированные организации возлагаются следующие функции:

— разработка технического проекта на создание СЗПДн в соответствии с требованиями российского законодательства;

— монтажные работы в соответствии с проектной документацией;

— использование сертифицированных технических, программных и программно-технических СЗИ и их установка;

— организация сертификации по требованиям безопасности информации программных СЗИ в случае, когда на рынке отсутствуют; требуемые сертифицированные СЗИ;

— разработка разрешительной системы доступа пользователей к ПДн, обрабатываемым в ИСПДн;

— разработка (в согласованном объеме) эксплуатационной документации на СЗПДн.

На стадии ввода СЗПДн в эксплуатацию на сторонние специализированные организации возлагаются следующие функции:

— установка СЗИ;

— предварительные испытания и опытная эксплуатация СЗИ в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе ИСПДн;

— приемо-сдаточные испытания СЗИ по результатам опытной эксплуатации;

— оценка соответствия ИСПДн требованиям безопасности ПДн.

4 Основные требования и правила по обеспечению безопасностиПДн при их обработке в ИСПДн Общества

Обеспечение безопасности ПДн при их обработке в ИСПДн Общества достигается применением организационных и технических мер, причем в интересах обеспечения безопасности в обязательном порядке подлежат защите технические и программные средства, используемые при обработке ПДн, и носители информации.

Основными направлениями защиты информации (ПДн) являются:

— обеспечение защиты информации (ПДн) от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД и специальных воздействий;

— обеспечение защиты информации (ПДн) от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи.

Основными мерами защиты информации (ПДн) являются:

— назначение ответственного за организацию обработки ПДн;

— разработка документов, определяющих политику Общества в отношении обработки ПДн, локальных актов по вопросам обработки ПДн, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства РФ в области обеспечения безопасности ПДн, устранение последствий таких нарушений;

— оценка вреда, который может быть причинен субъектам ПДн в случае нарушения требований настоящего Положения и нормативных актов РФ;

— реализация разрешительной системы допуска пользователей (обслуживающего персонала) к ИР, ИС и связанным с ее использованием работам, документам;

— ограничение доступа пользователей в помещения, где размещены ТС, позволяющие осуществлять обработку ПДн, а также хранятся носители информации;

— разграничение доступа пользователей и обслуживающего персонала к ИР, программным средствам обработки (передачи) и защиты информации;

— регистрация действий пользователей и обслуживающего персонала, контроль НСД и действий пользователей, обслуживающего персонала и посторонних лиц;

— учет и хранение съемных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;

— резервирование ТС, дублирование массивов и носителей информации;

— использование СЗИ, прошедших в установленном порядке процедуру оценки соответствия требованиям безопасности информации;

— использование защищенных каналов связи;

— размещение ТС, позволяющих осуществлять обработку ПДн, в пределах охраняемой территории;

— размещение дисплеев и других средств отображения информации, исключающее ее несанкционированный просмотр;

— организация физической защиты помещений и собственно ТС, позволяющих осуществлять обработку ПДн;

— предотвращение внедрения в ИС вредоносных программ (программ-вирусов) и программных закладок.

Для обеспечения безопасности ПДн от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа к ней за счет НСД в зависимости от уровня защищенности ИСПДн, заданных характеристик безопасности обрабатываемых ПДн, угроз безопасности ПДн, структуры ИСПДн, наличия межсетевого взаимодействия и режимов обработки ПДн в рамках СЗИ от НСД реализуются функции управления доступом, регистрации и учѐта, обеспечения целостности, анализа защищѐнности, обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений.

4.1 Требования по организации разрешительной системы доступа пользователей к обрабатываемой в ИСПДн информации

Данный подраздел Положения регламентирует порядок взаимодействия

подразделений Общества по обеспечению безопасности ПДн при организации разрешительной системы доступа к сервисам и ресурсам ИСПДн Общества.

Разрешительная система доступа к обрабатываемой в ИСПДн информации должна предусматривать установление единого порядка обращения со сведениями, содержащими ПДн клиентов и сотрудников Общества, и их носителями, определять степень ограничения на доступ к данной информации и степень ответственности за сохранность предоставленной информации.

Организация разрешительной системы доступа относится к основным вопросам управления обеспечением безопасности ПДн и включает:

— распределение функций управления доступом к данным и их обработкой

между должностными лицами;

— определение порядка изменения правил доступа к защищаемой информации;

— определение порядка изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

— контроль функционирования разрешительной системы доступа и расследование фактов неправомерного доступа лиц к защищаемой информации, в случае выявления таковых;

— оценку эффективности проводимых мер по исключению утечки информации;

— организацию деятельности должностных лиц, ответственных за подготовку предложений о внесении изменений в должностные обязанности и иные документы, определяющие задачи и функции персонала ИСПДн Общества;

— разработку ВНД, определяющих порядок реализации и функционирования разрешительной системы доступа.

Основные условия правомерного доступа сотрудников Общества к обрабатываемой в ИСПДн Общества информации включают в себя:

— подписание сотрудником Общества Обязательства о неразглашении конфиденциальной информации либо включение обязательства о неразглашении работником конфиденциальной информации в Трудовой договор;

— наличие у сотрудника Общества, оформленного в установленном порядке права допуска к ПДн, обрабатываемым в ИСПДн Общества;

— наличие утвержденных руководством Общества должностных (функциональных) обязанностей сотрудника, определяющих круг его задач и объем необходимой для их решения информации.

Лица, доступ которых к ПДн, обрабатываемым в ИСПДн, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим ПДн на основании утвержденного Перечня должностей работников, допущенных к обработке ПДн.

Для обеспечения персональной ответственности за свои действия каждому пользователю ИСПДн, допущенному к работе с защищаемой информацией в ИСПДн, присваивается уникальное имя (учетная запись пользователя), под которым он регистрируется и осуществляет работу в системе. В случае производственной необходимости пользователю ИСПДн могут быть сопоставлены несколько уникальных имен (учетных записей). Использование несколькими сотрудниками при работе в ИСПДн одного и того же имени пользователя («группового имени») запрещается.

При регистрации и назначении прав доступа пользователей ИСПДн Общества должны быть выполнены следующие требования:

— каждому пользователю должен быть присвоен уникальный идентификатор пользователя, по которому его можно однозначно идентифицировать;

— учетные записи всех пользователей должны быть привязаны к конкретным автоматизированным рабочим местам (АРМ), за исключением учетных записей технического персонала, обслуживающего компоненты ИСПДн Общества;

— при регистрации пользователей должна быть проведена проверка соответствия уровня доступа возложенным на пользователя задачам (вмененным обязанностям);

— назначенные пользователю права доступа должны быть документированы;

— пользователь должен быть ознакомлен под роспись с предоставленными ему правами доступа и порядком его осуществления;

— в ИСПДн должно быть предусмотрено разрешение доступа к сервисам только аутентифицированным пользователям;

— должен быть разработан и обновляться при внесении нового пользователя формальный список всех пользователей, зарегистрированных для работы

в ИСПДн;

— при изменении должностных обязанностей (увольнении) пользователя должно проводиться немедленное исправление (аннулирование) прав его доступа;

— администраторами ИСПДн должно проводиться удаление всех неиспользуемых учетных записей. Предусмотренные в системе запасные идентификаторы должны быть недоступны другим пользователям.

Контроль выполнения требований разрешительной системы доступа к ПДн возлагается на Администратора безопасности информации (администратора

ИТ).

Допуск к ИР ИСПДн сторонних организаций (правоохранительных органов, судебных органов, органов статистики, органов исполнительной и законодательной власти субъектов РФ) регламентируется законодательством РФ, приказами и распоряжениями министерств и служб, законодательно наделенных полномочиями на получение информации, а также настоящим Положением.

Порядок допуска к ИР ИСПДн сторонних организаций, выполняющих работы на договорной основе, определяется в договоре на выполнение работ (оказание услуг). Обязательным условием договора должно являться заключение соглашения о конфиденциальности.

4.2 Требования к проведению мероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где размещены средства ИСПДн

Данный подраздел Положения содержит общие требования к проведениюмероприятий по размещению, специальному оборудованию, охране и режиму допуска в помещения, где размещены ИСПДн Общества.

Должен быть организован контроль доступа персонала и посетителей в помещения Общества, в которых установлены ТС ИСПДн и осуществляется обработка ПДн, а также хранятся носители ПДн.

Доступ должностных лиц структурных подразделений Общества в помещения, в которых осуществляется обработка ПДн, организовывается на основании списков, утверждаемых руководством ООО МИКС. Доступ другого персонала Общества и посетителей в эти помещения должен осуществляться в сопровождении ответственных должностных лиц.

Посетители должны получать доступ только в соответствии с необходимостью и должны быть ознакомлены с инструкциями по безопасности и по действиям в аварийных ситуациях.

Для защиты помещений, в которых расположены ТС ИСПДн, должны быть приняты меры для минимизации воздействий огня, дыма, воды, пыли, взрыва, химических веществ, а также кражи.

ТС ИСПДн и размещенное совместно с ними вспомогательное оборудование должны подвергаться регулярным осмотрам с целью выявлений изменения конфигурации средств вычислительной техники (СВТ) (замки на коммутационных шкафах, использование специальных защитных знаков, пломбирование, опечатывание и др.).

Должно быть обеспечено размещение устройств вывода информации СВТ, дисплеев АРМ ИСПДн таким образом, чтобы была исключена возможность просмотра посторонними лицами текстовой и графической видовой информации, содержащей ПДн.

4.3 Правила обеспечения безопасности ПДн при использовании съемных носителей ПДн

4.3.1 Правила обращения со съемными носителями ПДн

При обращении со съемными носителями ПДн должны выполняться следующие основные правила:

— носители ПДн должны быть учтены, выданы пользователям под роспись и защищены;

— носители ПДн, срок эксплуатации которых истек, должны уничтожаться в установленном порядке;

— для выноса носителей ПДн за пределы объектов Общества должно быть получено специальное разрешение, а факт выноса – зафиксирован в специальной базе данных;

— все носители ПДн должны храниться в безопасном месте в соответствии с требованиями по их эксплуатации.

Ответственным за хранение, учет и выдачу съемных носителей ПДн является ответственный сотрудник структурного подразделения, ответственного за конфиденциальное делопроизводство.

4.3.2 Порядок учета носителей информации

Все находящиеся на хранении и в обращении съемные носители ПДн должны быть учтены в Журнале учета носителей ПДн.

Каждый носитель, с записанными на нем ПДн, должен иметь этикетку, на которой указывается метка съемного носителя и гриф.

Пользователи ИСПДн для выполнения работ получают учтенный съемный носитель от ответственного работника структурного подразделения, ответственного за конфиденциальное делопроизводство. При получении делаются соответствующие записи в Журнале учета.

После окончания работ пользователь ИСПДн сдает съемный носитель в помещение для хранения, о чем делается соответствующая запись в Журнале учета.

При наличии личного сейфа у пользователя ИСПДн допускается хранение учтенных съемных носителей в личных сейфах, опечатанных печатью пользователя ИСПДн.

4.3.3 Порядок уничтожения носителей ПДн

Носители ПДн, пришедшие в негодность, или отслужившие установленный срок, подлежат уничтожению.

Уничтожение носителей ПДн осуществляется комиссией по уничтожению, назначенной приказом по представлению руководителя структурного подразделения, ответственного за конфиденциальное делопроизводство .

Уничтожение магнитных, оптических и магнитооптических носителей информации производится путем их физического разрушения. Перед уничтожением носителя информация с него должна быть стерта (уничтожена), если это позволяют физические принципы работы носителя.

Бумажные носители данных уничтожаются на специальных бумагорезательных устройствах (шредерах).

Перед утилизацией оборудования, участвующего в обработке ПДн, сотрудником подразделения ИТ осуществляется проверка всех его компонентов, включая носители информации (жесткие диски) на отсутствие ПДн и лицензированного программного обеспечения (ПО).

По результатам уничтожения комиссией составляется Акт уничтожения носителей ПДн, который хранится в помещении для хранения носителей ПДн, уничтоженные носители ПДн (утилизированное оборудование) снимается с материального учета.

4.4 Требования к резервированию ИР

Резервное копирование защищаемой информации (ПДн) применяется для оперативного восстановления данных в случае утери или по другим причинам.

В состав ИР, подлежащих резервному копированию, в обязательном порядке включаются ИР, являющиеся объектом защиты в Обществе.

При организации резервирования ИР необходимо обеспечить выполнение следующих требований:

— резервные копии ИР и инструкции по их восстановлению должны храниться в специально выделенном месте, территориально отдаленном от места хранения основной копии информации;

— к резервным копиям должен быть применен комплекс физических и организационных мер защиты;

— носители, на которые осуществляется резервное копирование, должны

регулярно проверяться на отсутствие сбоев;

— применяемая система резервного копирования должна обеспечивать производительность, достаточную для сохранения информации, в установленные сроки и с заданной периодичностью;

— должны быть предусмотрены регулярная проверка процедур восстановления и практический тренинг персонала по восстановлению данных.

Резервное копирование информации осуществляется работниками подразделения ИТ в пределах своих полномочий в соответствии с графиком резервного копирования. Допускается осуществление резервного копирования в автоматизированном режиме.

График резервного копирования составляется для каждого вида информации, подлежащей периодическому резервному копированию, утверждается руководителем подразделения .

Периодичность проведения резервного копирования устанавливается Графиком резервного копирования не реже одного раза в неделю и может осуществляться ежедневно (в автоматизированном режиме).

Резервное копирование информации производится в соответствии с документацией на используемое ПО.

Программно-аппаратные средства, обеспечивающие проведение резервного копирования и носители, на которые осуществляется резервное копирование, не реже одного раза в месяц проверяются на отсутствие сбоев сотрудниками подразделения ИТ в соответствии с документацией на программно-аппаратные средства.

Резервные копии данных хранятся вместе с инструкцией по восстановлению данных из резервных копий в отдельном помещении от используемых данных.

Восстановление данных из резервной копии производится сотрудниками подразделения ИТ на основании Заявки руководителя структурного подразделения – владельца ИР.

Восстановление данных из резервных копий осуществляется в соответствии с документацией на используемое ПО в максимально сжатые сроки, ограниченные техническими возможностями системы, но не более одного рабочего дня.

4.5 Правила защиты ИСПДн от вредоносных программ

При использовании в ИСПДн средств антивирусной защиты и защиты от вредоносных программ, должны выполняться следующие организационные меры:

— использование съемных носителей ПДн пользователя ИСПДн на других компьютерах только с механической защитой от записи;

— запрет на использование посторонних съемных носителей ПДн при работе в ИСПДн;

— запрет на передачу съемных носителей ПДн посторонним лицам

— запрет на запуск программ с внешних съемных носителей информации при работе в ИСПДн;

— запрет на несанкционированное использование отчуждаемых носителей информации (оптических дисков, флэш-карт и т. п.);

— использование в ИСПДн только дистрибутивов программных продуктов, приобретенных у официальных дилеров фирм-разработчиков этих продуктов;

— обязательная проверка всех программных продуктов;

— проверка всех программных файлов и файлов документов, полученных по электронной почте, специальными антивирусными средствами;

— систематическая проверка содержимого дисков файловых хранилищ обновленными версиями антивирусных программ;

— контроль и обновление списка разрешенных ссылок на веб-ресурсы сети Интернет.

Ответственность за эксплуатацию средств антивирусной защиты и защиты от вредоносных программ возлагается:

— на сотрудников подразделения ИТ в части наличия антивирусного ПО на клиентских рабочих станциях и использования данного ПОпользователями;

4.6 Требования по обеспечению безопасности при работе в сети Интернет

Доступ в сеть Интернет и другие глобальные сети пользователям предоставляется исключительно в целях повышения эффективности выполнения ими свои служебных обязанностей.

Организация доступа пользователей ИСПДн к сети Интернет осуществляется сотрудником подразделения ИТ на основании мотивированного запроса руководителя подразделения Общества. Установка дополнительного оборудования и ПО для осуществления доступа пользователей ИСПДн Общества осуществляется в порядке, установленным настоящим Положением для внесения изменений в ПО и аппаратные средства Общества.

Пользователю может быть ограничен доступ к ресурсам сети Интернет, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены международным и Российским законодательством, включая материалы, носящие вредоносную, угрожающую, клеветническую, 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 т.д.

При работе с ресурсами сети Интернет запрещается:

— разглашение сведений конфиденциального характера Общества, ставшие известными сотруднику Общества по служебной необходимости либо иным путем;

— распространение защищаемых авторскими правами материалов, затрагивающих какой-либо патент, торговую марку, коммерческую тайну, копирайт или прочие права собственности и/или авторские и смежные с ним права третьей стороны;

— публикация, загрузка и распространение материалов, содержащих вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программ, для осуществления НСД, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и

прочие средства для получения НСД к платным ресурсам в сети Интернет, а также размещение ссылок на вышеуказанную информацию;

— загрузка и запуск исполняемых либо иных файлов без предварительной проверки на наличие вирусов установленным антивирусным пакетом;

— использование анонимных прокси-серверов;

— доступ к ресурсам сети Интернет, содержащим развлекательную (в том числе музыкальные, видео, графические и другие файлы, не связанные с производственной деятельностью), эротическую или порнографическую информацию.

При нарушении сотрудником Общества правил работы в сети Интернет либо возникновении нештатных ситуаций доступ к ресурсам сети Интернет может быть блокирован.

4.7 Правила использования ПО и аппаратных средств ИСПДн

Настоящий подраздел регламентирует взаимодействие подразделений Общества по обеспечению безопасности информации при проведении модификаций ПО, технического обслуживания и ремонта СВТ ИСПДн Общества.

4.7.1 Права на внесение изменений в ПО и аппаратные средства ИСПДн Общества

Все изменения конфигурации ТС и программных средств АРМ и серверов ИСПДн, обрабатывающих ПДн, должны производиться только на основании заявок руководителей структурных подразделений, согласованных с подразделением ИТ.

Право внесения изменений в конфигурацию программно-аппаратных средств информационных узлов (АРМ, серверов) и телекоммуникационного оборудования, обрабатывающего ПДн, предоставляется:

— в отношении системных и прикладных программных средств, а также в отношении аппаратных средств – уполномоченным сотрудникам подразделения ИТ;

— в отношении программно-аппаратных СЗИ – администратору ИТ и уполномоченным сотрудникам подразделения ИТ;

— в отношении программно-аппаратных средств телекоммуникаций – уполномоченным сотрудникам подразделения ИТ.

Изменение конфигурации аппаратно-программных средств защищенных АРМ и серверов кем-либо, кроме уполномоченных сотрудников перечисленных подразделений, запрещено.

Право внесения изменений в конфигурацию программно-аппаратных средств АРМ (серверов) локальной вычислительной сети, не обрабатывающих ПДн, предоставляется сотрудникам подразделения ИТ (на основании служебных записок руководителей структурных подразделений на имя руководителя подразделения ИТ).

4.7.2 Порядок внесения изменений в ПО и аппаратные средства ИСПДн Общества

Для внесения изменений в конфигурацию аппаратных и программных средств защищенных серверов и АРМ ИСПДн руководитель структурного подразделения, в котором необходимо внести изменения, подает заявку на имя руководителя подразделения ИТ, которая им рассматривается и утверждается.

При необходимости планового проведения изменений (обновлений версий) ПО, заявка выпускается руководителем подразделения ИТ и, направляется уполномоченному сотруднику подразделения ИТ.

В заявках могут быть указаны следующие виды необходимых изменений в составе программных и аппаратных средств рабочих станций (АРМ) и серверов подразделения:

— установка в подразделении новой рабочей станции (АРМ) или сервера;

— замена рабочей станции (АРМ) или сервера подразделения;

— изъятие рабочей станции (АРМ) или сервера подразделения;

— добавление устройства (узла, блока) в состав конкретной рабочей станции (АРМ) или сервера подразделения;

— замена устройства (узла, блока) в составе конкретной рабочей станции (АРМ) или сервера подразделения;

— изъятие устройства (узла, блока) из состава конкретной рабочей станции (АРМ) или сервера;

— установка (развертывание) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данной рабочей станции или сервере);

— обновление (замена) на конкретной рабочей станции (АРМ) или сервере программных средств, необходимых для решения определенной задачи (обновление версий используемых для решения определенной задачи программ);

— удаление с конкретной рабочей станции (АРМ) или сервера программных средств, использовавшихся для решения определенной задачи (исключение возможности решения данной задачи на данной рабочей станции).

В заявке указываются условные наименования развернутых рабочих станций (АРМ) и серверов в соответствии с их паспортами. Программные средства указываются в соответствии с перечнем программных средств фонда алгоритмов и программ, которые должны использоваться в ИСПДн.

Подразделение ИТ при согласовании заявки учитывает возможность совмещения решения новых задач (обработки информации) на указанных в заявке рабочих станциях (АРМ) или серверах в соответствии с требованиями по безопасности.

Руководитель структурного подразделения, в котором установлены аппаратно- программные средства, подлежащие модернизации, допускает уполномоченных исполнителей подразделения ИТ и внесению изменений в состав аппаратных средств и ПО только по предъявлении последними подписанного задания (в заявке) на осуществление данных изменений.

Установка, изменение (обновление) и удаление системных и прикладных программных средств производится уполномоченными сотрудниками подразделения ИТ.

Если рабочая станция (АРМ) или сервер обрабатывают ПДн, то установка, снятие, и внесение необходимых изменений в настройки СЗИ от НСД и средств контроля целостности файлов на рабочих станциях осуществляется уполномоченным сотрудником подразделения ИТ под контролем администратора безопасности. Работы производятся в присутствии пользователя данной рабочей станции.

Подготовка модификаций ПО защищенных серверов и рабочих станций, тестирование, стендовые испытания и передача исходных текстов, документации и дистрибутивных носителей программ в фонд алгоритмов и программ и другие необходимые действия производится уполномоченным сотрудником подразделения ИТ.

Установка или обновление подсистем ИСПДн должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

Модификация ПО на сервере осуществляется уполномоченными сотрудниками подразделения ИТ по согласованию с администратором безопасности.

После установки модифицированных модулей на сервер Администратор безопасности в присутствии уполномоченных сотрудников подразделения ИТ устанавливает защиту целостности модулей на сервере (производит пересчет контрольных сумм эталонов модулей на файл-сервере с помощью специальных программных средств, прошедших оценку соответствия).

После проведения модификации ПО на рабочих станциях уполномоченный сотрудник подразделения ИТ проводит антивирусный контроль.

Установка и обновление общего ПО (системного, тестового) на рабочие станции (АРМ) и серверы производится с оригинальных лицензионных дистрибутивных носителей (компакт дисков и др.), полученных установленным порядком, а прикладного ПО – с эталонных копий программных средств, полученных из фонда алгоритмов и программ.

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность, контроль наличия проверок работоспособности осуществляет подразделение ИБ.

После установки (обновления) ПО уполномоченный работник подразделения ИТ (при использовании специализированных СЗИ от НСД – Администратор безопасности) должен произвести настройку средств управления доступом к данному программному средству и проверить работоспособность ПО и правильность настройки СЗИ.

После завершения работ по внесению изменений в состав аппаратных средств рабочей станции (АРМ), обрабатывающей ПДн, ее системный блок закрывается уполномоченным сотрудником подразделения ИТ на ключ (при наличии штатных механических замков) и опечатывается (пломбируется,

защищается специальной наклейкой) с возможностью постоянного визуального контроля за ее целостностью .

При изъятии рабочей станции (сервера), обрабатывающей ПДн, из состава рабочих станций (серверов) структурного подразделения ее передача на склад, в ремонт или в другое структурное подразделение для решения иных задач осуществляется только после того, как уполномоченный сотрудник подразделения ИТ снимет с данной рабочей станции (сервера) СЗИ и предпримет необходимые меры для затирания защищаемой информации, которая хранилась на дисках компьютера.

Факт уничтожения данных, находившихся на диске компьютера, оформляется Актом о затирании остаточной информации, хранившейся на диске компьютера.

Оригиналы заявок (документов), на основании которых производились изменения в составе ТС или программных средств рабочих станций с отметками о внесении изменений в состав программно-аппаратных средств, должны храниться вместе с оригиналами паспортов рабочих станций (серверов) Копии заявок и актов

хранятся в подразделении ИТ. Они используются:

— для восстановления конфигурации рабочих станций (серверов) после аварий;

— для контроля правомерности установки на конкретной рабочей станции (сервере) средств для решения соответствующих задач при разборе конфликтных ситуаций;

— для проверки правильности установки и настройки СЗИ рабочих станций (серверов).

4.8 Требования по обеспечению безопасности при применении средств криптографической защиты информации

Криптографическая защита в ИСПДн Общества создаѐтся на основе сертифицированных СКЗИ, встраивание которых в ИСПДн должно происходить с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

В Обществе должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению

функционирования и безопасности СКЗИ. Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководителем ООО МИКС, с учетом эксплуатационной документации на СКЗИ.

К работе с СКЗИ допускаются только сотрудники, знающие правила его эксплуатации, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

Ответственное должностное лицо, уполномоченное на руководство заявленными видами деятельности со средствами СКЗИ, должно иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и СЗИ.

Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее - помещения), должны обеспечивать безопасность информации, СКЗИ и криптоключей, должны быть сведены к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

Порядок допуска в помещения определяется локальными нормативными актами Общества.

Для хранения криптоключей, нормативной и эксплуатационной документации, инсталлирующих криптосредство носителей, помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ. Системные блоки АРМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.

5. Порядок организации внутреннего обучения персонала правилам и мерам защиты ПДн

Решение основных вопросов обеспечения защиты ПДн должно предусматривать соответствующую подготовку кадров. Проведение обучения сотрудников Общества позволит организовать обработку информации в соответствии с требованиями законодательства и нормативно-методических документов в области обеспечения безопасности ПДн при их обработке в ИСПДн и реализовать установленный комплекс организационных и технических мер по защите ПДн.

Систему внутреннего обучения персонала в области защиты ПДн составляет:

— проведение инструктажа пользователей ИСПДн;

— самостоятельное изучение сотрудниками Общества необходимых для работы

документов, средств и продуктов.

В результате прохождения обучения сотрудники Общества получат необходимые знания и навыки в отношении:

— правил использования СЗИ;

— содержания основных нормативных правовых актов, руководящих и нормативно-методических документов в области обеспечения безопасности ПДн при их обработке в ИСПДн;

— основных мероприятий по организации и техническому обеспечению безопасности ПДн при их обработке в ИСПДн Общества;

— планирования, организации и контроля выполнения мероприятий по обеспечению безопасности ПДн при их обработке в ИСПДн.

5.1 Проведение инструктажа пользователей ИСПДн Пользователи ИСПДн, допущенные к работе с ПДн, обязаны пройти инструктаж по вопросам обеспечения безопасности ПДн с целью подтверждения своих знаний и уяснения своих обязанностей по поддержанию установленного режима защиты ПДн.

Инструктаж представляет собой ознакомление сотрудников Общества, допущенных к работе в ИСПДн, с положениями настоящего Положения и действующих нормативных документов по обеспечению безопасности информации при ее обработке в ИСПДн.

Ознакомление с положениями нормативной документации сотрудник Общества подтверждает своей личной подписью в журнале инструктажа, что свидетельствует о прохождении инструктажа.

Контроль проведения инструктажа и периодическая проверка знания пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн возлагается на администратора безопасности совместно с руководителями структурных подразделений Общества, использующих ИСПДн. Ответственность за непосредственное проведение

инструктажа возлагается на руководителей структурных подразделений Общества.

Сотрудники Общества, не прошедшие инструктаж, к работе в ИСПДн не допускаются. Инструктаж проводится перед началом работы в ИСПДн новых сотрудников Общества, а также не реже одного раза в год для всех пользователей ИСПДн.

Проверка знаний пользователями ИСПДн положений нормативной документации по вопросам обеспечения безопасности ПДн проводится администратором безопасности не реже одного раза в год в ходе периодического контроля соблюдения режима безопасности информации.

5.2 Самостоятельное изучение

При данном виде подготовки сотрудниками Общества, осуществляющими обработку ПДн, а также сотрудниками подразделения ИТ и подразделения ИБ самостоятельно изучаются (в части касающейся):

— руководящие и нормативно-методические документы в области обеспечения безопасности ПДн;

— правила (инструкции) по использованию программных и аппаратных СЗИ.

— внутренние положения (локальные акты), устанавливающие порядок обращения с ПДн и их защиты.

Время для самостоятельного изучения определяется руководителями соответствующих структурных подразделений Общества.

6. Ответственность должностных лиц за обеспечениебезопасности ПДн, своевременность и качество формирования требований по защите информации, за качество и научно- технический уровень разработки СЗПДн

Ответственность за обеспечение безопасности ПДн распределяется между должностными лицами Общества на основании настоящего Положения.

Ответственность за организацию режима обеспечения безопасности ПДн возлагается на руководителей структурных подразделений Общества.

Ответственность за своевременность и качество формирования требований по защите ПДн, за качество и научно-технический уровень разработки СЗПДн, а также контроль исполнения правил и требований, направленных на обеспечение безопасности ПДн, возлагается на подразделение ИТ.

Ответственность за выполнение обязанностей по обеспечению режима безопасности ПДн, возложенных на структурные подразделения Общества, эксплуатирующие ИСПДн, несут руководители соответствующих структурных подразделений.

Средства информатизации, входящие в состав ИСПДн, должны быть закреплены за ответственными должностными лицами (владельцами). Владельцем средств информатизации может быть руководитель структурного подразделения или специально назначаемое должностное лицо Общества. На владельца средств информатизации возлагается ответственность за выполнение установленных мероприятий по защите закрепленных средств информатизации и обрабатываемых ими ПДн.

Руководители и сотрудники Общества, виновные в нарушении режима защиты ПДн, несут дисциплинарную, гражданскую, административную, уголовную и иную предусмотренную законодательством РФ ответственность.

7 Порядок контроля обеспечения уровня защищенности ПДн и оценки соответствия ИСПДн

Контроль обеспечения требуемого уровня защищенности ПДн заключается в проверке выполнения требований нормативных документов по защите ПДн, а также в оценке обоснованности и эффективности принятых мер. Мероприятия по контролю защищенности ПДн могут проводиться как уполномоченными сотрудниками подразделения ИБ, так и на договорной основе сторонней организацией, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Мероприятия по контролю защищенности ПДн и оценке соответствия ИСПДн включают:

— внутренний контроль режима безопасности ПДн (оперативный и периодический);

— обследование защищенности ПДн с привлечением сторонней организации;

— оценку соответствия ИСПДн требованиям безопасности ПДн.

7.1 Внутренний контроль режима безопасности ПДн и оценки соответствия ИСПДн требованиям безопасности ПДн

Внутренний оперативный контроль соблюдения режима безопасности ПДн проводится специалистом по ИБ (администратором безопасности) ежедневно в режиме «реального времени». Внутренний контроль заключается в анализе защищенности ПДн посредством используемых в составе ИСПДн программных и программно-аппаратных средств (систем) анализа защищенности.

В ходе проведения контроля соблюдения режима безопасности ПДн специалист по ИБ (администратор безопасности):

— осуществляет анализ лог-файлов, производимых средствами защиты и другими элементами ИСПДн (ОС, прикладные программы);

— просматривает оповещения средств защиты ИСПДн;

— принимает меры по результатам анализа полученных оповещений и лог файлов.

Внутренний периодический контроль заключается в оценке выполнения требований нормативных документов по обеспечению безопасности ПДн, обрабатываемых в ИСПДн.

В ходе проведения внутреннего периодического контроля проверяются следующие вопросы:

— соответствие состава и структуры программно-технических средств, обрабатывающих защищаемую информацию (ПДн), документированному составу и структуре средств, разрешенных для обработки такой информации;
— знание персоналом руководящих документов, технологических инструкций, предписаний, актов, заключений и уровень овладения персоналом технологией безопасной обработки информации, описанной в этих инструкциях;

— проверка наличия документов, подтверждающих возможность применения технических и программных СВТ для обработки ПДн и применения СЗИ (сертификатов соответствия и других документов);

— проверка правильности применения СЗИ;

— проверка выполнения требований по условиям размещения АРМ в рабочих

помещениях;

— соответствие реального уровня полномочий по доступу к защищаемой информации (ПДн) различных пользователей установленному в списке лиц, допущенных к обработке ПДн, уровню полномочий;

— знание инструкций по обеспечению безопасности информации пользователями ИСПДн;

— организация хранения носителей ПДн и допуска в помещения, где размещены средства обработки и осуществляется обработка ПДн;

— прохождение инструктажа пользователей по вопросам обеспечения безопасности ПДн и выполнение ими установленных требований.

По фактам несоблюдения условий хранения носителей ПДн, использования СЗИ, которые могут привести к нарушению конфиденциальности ПДн или другим

нарушениям, приводящим к снижению уровня защищенности ПДн, проводится разбирательство и составляется соответствующее заключение, на основе которого впоследствии осуществляется разработка и реализация мер по предотвращению возможных опасных последствий подобных нарушений.

Результаты контроля оформляются Актом, в котором делаются выводы о состоянии обеспечения безопасности ПДн на проверяемом объекте информатизации и приводятся рекомендации по его совершенствованию.

7.2 Обследование защищенности ПДн внешней специализированной организацией

Обследование защищенности ПДн внешней специализированной организацией проводится при создании ИСПДн (предпроектное обследование) или при доработке (модернизации) СЗПДн в случае, если:

— изменился состав или структура ИСПДн или технические особенности его

построения (состав или структура ПО, ТС обработки ПДн, топологии и т.п.);

— изменился состав угроз безопасности ПДн;

— изменился класс защищѐнности ИСПДн.

Привлекаемая для проведения обследования внешняя специализированная организация должна иметь лицензию на деятельность по технической защите конфиденциальной информации.

7.3 Порядок оценки соответствия ИСПДн требованиям безопасности ПДн

Оценка соответствия ИСПДн требованиям безопасности ПДн проводится в форме проверки готовности СЗИ к использованию или добровольной аттестации.

Проверка готовности СЗИ к использованию осуществляется в ходе приѐмо-сдаточных испытаний СЗПДн с составлением протоколов проверки и заключений о возможности их эксплуатации.

Проверка готовности СЗИ к использованию проводится в соответствии с разрабатываемой программой и методикой испытаний соответствующих СЗИ, определяющих порядок проверки выполнения СЗИ заявленных функций защиты.

8 Хранение и архивирование

Подлинник данного Положения во время срока действия хранится у Генерального директора общества

9 Рассылка и актуализация

Периодическая проверка данного Положения проводится подразделением ИТ

по мере необходимости, но не реже 1 раза в 12 месяцев.

Решение об инициации процесса внесения изменений в Положени принимает

Генеральный директор на основании предложений других

подразделений, результатов применения документа в ОБЩЕСТВЕ , анализа зарегистрированных и устраненных несоответствий, а также рекомендаций внутренних или внешних аудитов.

Актуальная версия утвержденного Положения размещена на интернет-сайте общества