


СОГЛАСОВАНО

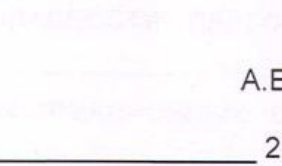
Директор Департамента научно-технического и стратегического развития отрасли Министерства связи и массовых коммуникаций Российской Федерации

 О.В. Чутов

«__» _____ 2010 г.

УТВЕРЖДАЮ

Президент
Инфокоммуникационного союза

 А.Е. Крупнов

«__» _____ 2010 г.

СОГЛАСОВАНО


Первый заместитель начальника 8-го центра Федеральной службы безопасности Российской Федерации

 А.П. Баранов

«__» _____ 2010 г.

СОГЛАСОВАНО

Начальник 2-го управления Федеральной службы по техническому и экспортному контролю

 А.В. Куц

«30» МАРТА 2010 г.



КОНЦЕПЦИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА СВЯЗИ

ОГЛАВЛЕНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ	5
1. ОБЩИЕ ПОЛОЖЕНИЯ	7
1.1 Назначение концепции	7
1.2 Правовые основы обеспечения безопасности ПДн в ИСПДн Оператора связи.....	8
2. СФЕРА ДЕЙСТВИЯ И ОБЛАСТЬ РАСПРОСТРАНЕНИЯ КОНЦЕПЦИИ	9
3. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ	10
4. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОПЕРАТОРОВ СВЯЗИ	11
4.1 Категории субъектов персональных данных	11
4.2 Цели обработки персональных данных	11
4.3 Категории персональных данных субъектов персональных данных	12
4.4 Характеристики безопасности персональных данных	12
5. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПД В ИСПДН ОПЕРАТОРА СВЯЗИ	13
5.1 Законность	13
5.2 Системность	13
5.3 Комплексность	13
5.4 Непрерывность.....	14
5.5 Своевременность	14
5.6 Преемственность и непрерывность совершенствования	15
5.7 Разумная достаточность и адекватность.....	15
5.8 Персональная ответственность.....	15
5.9 Минимизация полномочий	16
5.10 Гибкость	16
5.11 Открытость алгоритмов и механизмов защиты.....	16
5.12 Научная обоснованность и техническая реализуемость	16
5.13 Специализация и профессионализм.....	17
5.14 Знание своих партнеров и работников	17
5.15 Наблюдаемость и оцениваемость обеспечения безопасности персональных данных	17
5.16 Обязательность контроля и оценки.....	17
6. ОБЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ	18
6.1 Классификация методов обеспечения безопасности персональных данных.....	18
6.2 Административно-правовые методы	18
6.3 Организационно-технические методы	19
6.4 Экономические методы	20
6.5 Превентивные методы.....	20
6.6 Восстановительные методы	20
6.7 Основные этапы работ по обеспечению безопасности персональных данных.....	21
7. ОБЩИЕ ХАРАКТЕРИСТИКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА СВЯЗИ	23
8. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДн В ИСПДН ОПЕРАТОРА СВЯЗИ	27
8.1 Модель угроз безопасности персональных данных	27

8.2	Модель нарушителя безопасности персональных данных.....	27
9.	ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ	29
9.1	Идентификация и аутентификация	31
9.2	Физическая защита	31
9.3	Регистрация и учет.....	32
9.4	Обеспечение целостности	32
9.5	Антивирусная защита	32
9.6	Обеспечение безопасного межсетевого взаимодействия	33
9.7	Анализ защищенности	33
9.8	Обнаружение вторжений	33
9.9	Криптографическая защита	34
9.10	Обеспечение безопасности мобильных рабочих мест.....	34
9.11	Обеспечение безопасного доступа к сетям международного информационного обмена ..	35
10.	ПРИНЦИПЫ ОЦЕНКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА СВЯЗИ.....	37
10.1	Внутренний контроль	37
10.2	Государственный контроль	38
11.	ПОРЯДОК ПЕРЕСМОТРА КОНЦЕПЦИИ.....	39
Приложение 1.	НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ.....	40

ПРИНЯТЫЕ СОКРАЩЕНИЯ

ИСПДн – информационная система персональных данных

ИТ – инфраструктура – информационно-технологическая инфраструктура

КИС – корпоративная информационная система

МРМ – мобильное рабочее место

НСД – несанкционированный доступ

ПДн – персональные данные

ПТК – программно-технический комплекс

СЗПДн – система защиты персональных данных

СКЗИ – средство криптографической защиты информации

УБПДн – угрозы безопасности персональных данных

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Абонент - пользователь услугами связи, с которым заключен договор об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации.

Доверенная среда эксплуатации ИСПДн - среда, в которой обеспечение необходимого уровня безопасности персональных данных, гарантируется выполнением требований разрешительных документов уполномоченных федеральных органов, включая ФСБ России и (или) ФСТЭК России.

Доверенный канал – средство взаимодействия между функциями безопасности объекта и удаленным доверенным продуктом ИТ, обеспечивающее необходимую степень уверенности в поддержании политики безопасности объекта

Доверие - основание для уверенности в том, что сущность отвечает своим целям безопасности.

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационная система персональных данных - информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Линии связи - линии передачи, физические цепи и линейно-кабельные сооружения связи.

Нарушитель безопасности персональных данных - физическое лицо случайно или преднамеренно совершающее действия, следствием которых

является нарушение заданных характеристик безопасности персональных данных при их обработке в информационной системе персональных данных.

Обработка персональных данных - действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Оператор связи - юридическое лицо или индивидуальный предприниматель, оказывающие услуги связи на основании соответствующей лицензии.

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Пользователь услугами связи - лицо, заказывающее и (или) использующее услуги связи.

Сеть связи - технологическая система, включающая в себя средства и линии связи и предназначенная для электросвязи.

Система защиты персональных данных – совокупность организационных мер и средств защиты информации, включающих средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных, а также используемые в информационной системе информационные технологии.

Средства связи - технические и программные средства, используемые для формирования, приема, обработки, хранения, передачи, доставки сообщений электросвязи или почтовых отправлений, а также иные технические и программные средства, используемые при оказании услуг связи или обеспечении функционирования сетей связи.

Услуга связи - деятельность по приему, обработке, хранению, передаче, доставке сообщений электросвязи.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Назначение концепции

Концепция защиты персональных данных в информационных системах персональных данных Оператора связи (далее – Концепция) является отраслевым документом, определяющим общие принципы обеспечения безопасности персональных данных (далее – ПДн) и организационно-технические меры по защите ПДн в информационных системах персональных данных (далее – ИСПДн) Оператора связи.

Настоящая Концепция разработана на основе анализа требований действующего законодательства Российской Федерации и нормативных документов, регламентирующих вопросы защиты ПДн, с учетом современного состояния и стратегии развития информационных технологий, целей, задач и правовых основ создания и эксплуатации информационных систем Операторов связи, режимов функционирования, а также на основе анализа угроз безопасности ПДн (далее – УБПДн).

Концепция служит основой для разработки комплекса организационных и технических мер по обеспечению защиты персональных данных в ИСПДн Операторов связи, а также нормативных и методических документов, обеспечивающих жизненный цикл системы защиты персональных данных (далее – СЗПДн) Оператора связи

Обязанности по реализации необходимых организационных и технических мероприятий для защиты ПДн ИСПДн Оператора связи от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними, возлагаются на Оператора связи.

Настоящая Концепция развивает положения Концепции информационной безопасности Сетей связи общего пользования взаимосвязанной сети связи Российской Федерации в отношении информационных систем персональных данных Операторов связи.

1.2 Правовые основы обеспечения безопасности ПДн в ИСПДн Оператора связи

Концепция разработана в целях реализации требований Федерального закона № 152-ФЗ от 27.07.2006 года «О персональных данных» по обеспечению безопасности ПДн, обрабатываемых в ИСПДн Оператора связи и выполнения международных обязательств РФ.

Правовую основу Концепции составляют Конституция Российской Федерации, Концепция национальной безопасности Российской Федерации, Доктрина информационной безопасности Российской Федерации, Федеральные законы РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ, нормативные правовые акты (приказы, распоряжения) федеральных органов исполнительной власти, уполномоченных в областях связи, обеспечения безопасности и технической защиты информации, а также международные договоры РФ.

2. СФЕРА ДЕЙСТВИЯ И ОБЛАСТЬ РАСПРОСТРАНЕНИЯ КОНЦЕПЦИИ

Сфера действия Концепции распространяется на Операторов связи, оказывающих услуги связи в сети связи общего пользования взаимосвязанной сети связи Российской Федерации.

При обеспечении технологического процесса оказания услуг связи используются как ресурсы корпоративной информационной системы Оператора связи, так и технологической сети связи.

ИСПДн интегрированы в корпоративную информационную систему (далее – КИС) Оператора связи.

Технологические сети связи Операторов связи состоят из средств связи и линий связи и предназначены для обеспечения приема, обработки, хранения, передачи и доставки потоков информации (сообщений, данных) абонентов на основании только абонентского номера или уникального кода идентификации.

Областью распространения Концепции являются информационные системы персональных данных Операторов связи.

Технологические сети связи не являются областью распространения Концепции.

3. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Основной целью обеспечения безопасности персональных данных является минимизация ущерба (как непосредственного, так и опосредованного), возникающего вследствие возможной реализации угроз безопасности персональных данных.

Непосредственный ущерб связан с причинением физического, материального, финансового или морального вреда непосредственно субъекту персональных данных и может проявляться в виде:

- нанесения вреда здоровью субъекта персональных данных;
- незапланированных и (или) непроизводительных финансовых или материальных затрат субъекта;
- потери субъектом свободы действий вследствие шантажа и угроз, осуществляемых с использованием персональных данных;
- нарушения конституционных прав субъекта вследствие вмешательства в его личную жизнь.

Опосредованный ущерб связан с причинением вреда обществу и (или) государству вследствие нарушения нормальной деятельности государственных органов, органов местного самоуправления, муниципальных органов, организаций различных форм собственности за счет неправомерных действий с персональными данными.

Основной задачей обеспечения безопасности персональных данных, при их обработке в информационных системах персональных данных Операторов связи, является предотвращение утечки персональных данных по техническим каналам, несанкционированного доступа к ним, предупреждение преднамеренных программно-технических воздействий с целью их разрушения (уничтожения) или искажения в процессе обработки, передачи и хранения.

4. ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОПЕРАТОРОВ СВЯЗИ

4.1 Категории субъектов персональных данных

Субъекты, персональные данные которых обрабатываются в информационных системах Операторов связи, подразделяются на две категории:

1) Пользователи услугами связи – физические лица, заказывающее и (или) использующее услуги связи. К данной категории относятся абоненты – пользователи услугами связи, с которыми заключены договоры об оказании таких услуг при выделении для этих целей абонентского номера или уникального кода идентификации.

2) Физические лица, обработка персональных данных которых осуществляется в целях выполнения технологического процесса оказания услуг связи. К данной категории относятся:

- работники – физические лица, вступившие в трудовые отношения с работодателем (Оператором связи);
- другие физические лица, обработка персональных данных которых необходима в целях выполнения технологического процесса оказания услуг связи. К таким физическим лицам, в частности, могут относиться работники сторонних организаций, осуществляющие функции по профессиональной поддержке бесперебойной работоспособности отдельных систем и информационно-технологической инфраструктуры Оператора связи, физические лица, в отношении которых осуществляются мероприятия по контролю доступа на защищаемые объекты Оператора связи.

4.2 Цели обработки персональных данных

В основе определения целей обработки персональных данных лежит принцип законности их обработки.

Целью обработки персональных данных абонентов является исполнение договоров об оказании услуг связи.

Целями обработки персональных данных работников являются содействие в трудоустройстве, обучение и продвижение по службе, обеспечение личной

безопасности работников, контроль количества и качества выполняемой работы и обеспечение сохранности имущества.

При определении целей обработки персональных данных иных категорий субъектов персональных данных, необходимо соблюдать законы и иные нормативно-правовые акты.

4.3 Категории персональных данных субъектов персональных данных

Состав персональных данных должен соответствовать принципу их достаточности для достижения целей обработки (персональные данные не должны быть избыточными по отношению к целям обработки).

Категория персональных данных, таких категорий субъектов как абонент и работник, не должна быть выше второй.

4.4 Характеристики безопасности персональных данных

Персональные данные, обрабатываемые в информационных системах Операторов связи, должны обладать свойством конфиденциальности, а также могут рассматриваться и другие характеристики безопасности. В частности, к таким характеристикам относятся: целостность, доступность, неотказуемость, учетность (подконтрольность), аутентичность (достоверность), адекватность.

Для обеспечения заданных характеристик безопасности персональных данных необходимо реализовать минимальный и достаточный набор организационно-технических мер.

5. ОБЩИЕ ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПД В ИСПДН ОПЕРАТОРА СВЯЗИ

Построение СЗПДн Оператора связи и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

- законность;
- системность;
- комплексность;
- непрерывность;
- своевременность;
- преемственность и непрерывность совершенствования;
- разумная достаточность и адекватность;
- персональная ответственность;
- минимизация полномочий;
- гибкость;
- открытость алгоритмов и механизмов защиты;
- научная обоснованность и техническая реализуемость;
- специализация и профессионализм;
- знание своих партнеров и работников;
- наблюдаемость и оцениваемость;
- обязательность контроля и оценки.

5.1 Законность

Защита ПДн в ИСПДн Оператора связи основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите ПДн и учитывает лучшие мировые практики.

5.2 Системность

Системный подход к построению СЗПДн предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности ПДн Оператором связи.

5.3 Комплексность

Безопасность ПДн обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер, реализованных Оператором связи.

Применение различных средств и технологий защиты информации должно перекрывать все существенные (значимые) каналы реализации угроз безопасности ПДн и не содержать слабых мест в согласовании применяемых средств и технологии защиты информации.

Должен быть обеспечен отраслевой подход к разработке рекомендаций (требований) по защите ПДн с учетом особенностей обработки ПД в ИСПДн Операторов связи.

СЗПДн должна строиться с учетом не только всех известных каналов проникновения и несанкционированного доступа (далее – НСД) к ПДн, но и с учетом возможности повышения уровня защиты по мере выявления новых источников УБПДн, развития способов и средств их реализации в ИСПДн.

СЗПДн Оператора связи строится на основе единой технической политики, с использованием функциональных возможностей информационных технологий, реализованных в информационной системе и имеющихся систем и средств защиты в соответствии с разработанными типовыми моделями угроз и профилями защиты. При создании СЗПДн могут использоваться системы и средства защиты информации, используемые в организации для обеспечения безопасности коммерческой тайны и иной конфиденциальной информации.

5.4 Непрерывность

Защита ПДн должна обеспечиваться на всех технологических этапах обработки ПДн и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

5.5 Своевременность

Принимаемые меры по обеспечению безопасности ПДн должны носить упреждающий характер.

Оператор связи принимает необходимые меры по защите ПДн до начала обработки ПДн, которые должны обеспечить надлежащий уровень безопасности ПДн.

СЗПДн разрабатывается одновременно с разработкой и развитием ИСПДн Оператора связи, что позволяет учитывать требования по безопасности ПДн при проектировании и модернизации ИСПДн.

5.6 Преемственность и непрерывность совершенствования

Предполагают постоянное совершенствование мер и средств защиты ПДн на основе результатов анализа функционирования ИСПДн и СЗПДн с учетом выявления новых способов и средств реализации УБПДн, отечественного и зарубежного положительного опыта в сфере защиты информации.

Оператор связи должен определять действия, необходимые для устранения причин потенциальных несоответствий требованиям по безопасности ПДн с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать возможным негативным последствиям.

5.7 Разумная достаточность и адекватность

Состояние и стоимость реализации мер защиты должно быть соизмеримо с рисками, связанными с обработкой и характером защищаемых ПДн.

Анализ рисков нарушения безопасности ПДн проводится в целях определения влияния системы защиты информации на вероятность реализации угроз безопасности ПДн с учетом уязвимостей (дефектов) ИТ - инфраструктуры Оператора связи.

Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики и производительность ИСПДн Оператора связи.

5.8 Персональная ответственность

Ответственность за обеспечение безопасности ПДн и ИСПДн Оператора связи возлагается на каждого работника в пределах его полномочий.

Распределение обязанностей и полномочий работников Оператора связи должно обеспечивать выявление виновных лиц в случаях нарушения безопасности ПДн.

Роли и обязанности сотрудников должны быть определены и документально подтверждены в соответствии с организационной политикой в области защиты информации.

5.9 Минимизация полномочий

Предоставление и использование прав доступа к ПДн должно быть ограничено и управляемо.

Пользователям должны предоставляться минимальные права доступа к ПДн и ИСПДн только в соответствии с производственной необходимостью.

Доступ к ПДн должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

Пользователю должны быть запрещены все операции с ПДн за исключением тех, которые разрешены явно.

5.10 Гибкость

В процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категория обрабатываемых Оператором связи ПДн.

Для обеспечения возможности варьирования уровня защищенности ПДн, СЗПДн Оператора связи должна обладать определенной гибкостью.

5.11 Открытость алгоритмов и механизмов защиты

Защита ПДн не должна осуществляться только за счет сокрытия структуры, технологий и алгоритмов функционирования СЗПДн.

Знание указанных характеристик СЗПДн не должно давать возможности преодоления защиты возможными нарушителями безопасности ПДн, включая разработчиков средств защиты.

5.12 Научная обоснованность и техническая реализуемость

Уровень рекомендаций и требований по защите ПДн должен соответствовать имеющемуся уровню развития информационных технологий и средств защиты информации.

При создании и эксплуатации СЗПДн необходимо ориентироваться на лучшие современные отечественные и зарубежные технические решения и практику защиты информации.

5.13 Специализация и профессионализм

Реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн должна осуществляться профессионально подготовленными специалистами Оператора связи.

5.14 Знание своих партнеров и работников

Оператор связи должен обладать информацией о своих партнерах, позволяющей минимизировать вероятность реализации УБПДн, источники которых связаны с человеческим фактором.

Оператор связи должен реализовывать кадровую политику (тщательный подбор персонала и мотивация работников), позволяющую исключить или минимизировать возможность нарушения безопасности ПДн своими работниками.

5.15 Наблюдаемость и оцениваемость обеспечения безопасности персональных данных

Предлагаемые Оператором связи меры по обеспечению безопасности ПДн должны быть спланированы так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен федеральными органами исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

5.16 Обязательность контроля и оценки

Неотъемлемой частью работ по защите ПДн является оценка эффективности системы защиты.

С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн Оператором связи должны быть определены процедуры для постоянного контроля использования систем обработки и защиты ПДн, а результаты контроля должны регулярно анализироваться.

6. ОБЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Классификация методов обеспечения безопасности персональных данных

Методы обеспечения безопасности ПДн разделяются на:

- административно-правовые;
- организационно-технические;
- экономические.

По времени применения методы обеспечения безопасности ПДн разделяются на:

- превентивные;
- восстановительные.

6.2 Административно-правовые методы

К административно-правовым методам защиты относятся нормы действующего законодательства Российской Федерации в области персональных данных и внутренние организационно-распорядительные документы Оператора связи, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе обработки и использования ПДн, а также устанавливающие ответственность за нарушения этих правил, препятствуя неправомерной обработке ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

Основными направлениями этой деятельности Оператора связи являются:

- разработка, внесение изменений и дополнений в политику информационной безопасности в части защиты ПДн и поддерживающие ее документы;
- регламентация процессов обработки ПДн;
- определение ответственности за нарушения в области обеспечения безопасности ПДн;
- назначение и подготовка должностных лиц (работников), ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности ПДн;

- закрепление в должностных инструкциях установленного разграничения полномочий в области обеспечения безопасности ПДн;
- разработка и принятие документов, устанавливающих ответственность структурных подразделений и сотрудников, а также взаимодействующих юридических лиц, за несанкционированный доступ к ПДн, противоправное копирование, искажение и противозаконное использование, преднамеренное распространение недостоверных ПДн, противоправное их раскрытие или использование в преступных и корыстных целях;
- контроль знания и соблюдения пользователями ИСПДн, требований организационно-распорядительных документов по вопросам обеспечения безопасности ПДн;
- проведение постоянного анализа эффективности и достаточности принимаемых мер и применяемых средств защиты ПДн, разработка и реализация предложений по совершенствованию СЗПДн.

6.3 Организационно-технические методы

Организационно-технические методы защиты основаны на использовании организационных мер, различных программных, аппаратных и программно - аппаратных средств, входящих в состав СЗПДн и выполняющих функции защиты информации, направленных на решение следующих задач:

- строгий учет всех подлежащих защите ресурсов (персональных данных, сервисов, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- своевременного обнаружения фактов НСД к ПДн;
- недопущения воздействия на технические средства автоматизированной обработки ПДн, в результате которого может быть нарушено их функционирование;
- возможности незамедлительного восстановления ПДн, модифицированных или уничтоженных вследствие НСД к ним;
- постоянного контроля за обеспечением уровня защищенности ПДн.

6.4 Экономические методы

Экономические методы обеспечения безопасности ПДн включают в себя:

- разработку Оператором связи программ обеспечения безопасности ПДн и определение порядка их финансирования.
- разработку Оператором связи мер поощрения и наложения штрафных санкций за соблюдение или не соблюдение установленных правил и процедур обработки ПДн.

6.5 Превентивные методы

Превентивные методы противодействия угрозам безопасности ПДн осуществляются на основе эффективного применения в процессе эксплуатации ИСПДн комплекса организационных, технических и технологических мероприятий, а также методов и средств обеспечения функциональной устойчивости и безопасности работы ИСПДн.

Организационные мероприятия по обеспечению безопасности ПДн являются мероприятиями общего характера по организации деятельности персонала, эксплуатирующего ИСПДн, порядку применения информационных технологий в зданиях и сооружениях, систематическому применению мер по недопущению вывода ИСПДн из строя.

Технические мероприятия по обеспечению безопасности ПДн заключаются в обслуживании, поддержании и управлении требуемым составом технических средств, обеспечивающих обработку ПДн в защищенном режиме.

Технологические мероприятия по обеспечению безопасности ПДн направлены на правильную реализацию функций и заданных алгоритмов работы ИСПДн, технологий обработки ПДн и защиту программ и ПДн от преднамеренных и непреднамеренных нарушений.

6.6 Восстановительные методы

Планирование восстановительных методов определяется системой документов, устанавливающих требования к обязательным мероприятиям, проводимым заблаговременно и после возникновения нарушений, угрожающих штатному функционированию ИСПДн.

6.7 Основные этапы работ по обеспечению безопасности персональных данных

В число основных этапов работ по обеспечению безопасности персональных данных входят, в частности, следующие:

- определение объектов защиты;
- установление целей защиты объектов защиты;
- определение угроз объектам защиты;
- установление требований к системе защиты персональных данных;
- определение порядка контроля и надзора.

Основным объектом защиты являются персональные данные.

Персональные данные могут иметь различные формы представления (бумажная, файлы, записи и поля записей баз данных, электромагнитные волны и поля, излучения и т.д.), каждая из которых является объектом защиты.

Формы представления персональных данных связаны с различными ресурсами информационной системы персональных данных, которые в свою очередь могут порождать объекты защиты.

Используемые в информационной системе персональных данных средства защиты информации являются объектами защиты.

Информация о методах и средствах обеспечения безопасности персональных данных содержит сведения, которые являются объектами защиты, в частности, к таким объектам могут быть обнесены парольная и аутентифицирующая информация, ключевая информация

Установление целей защиты объектов защиты связано с установлением характеристик безопасности для каждого из определенных объектов защиты.

Определение угроз объектам защиты проводится путем формирования модели угроз и модели нарушителя (см. п. 8 настоящей Концепции). При этом модель нарушителя формируется как составная часть модели угроз, определяющая возможные специфические угрозы – атаки.

Установление требований к системе защиты персональных данных основано на формировании моделей угроз и нарушителя.

В первую очередь устанавливаются общие требования к организационным мерам.

Далее на основе моделей угроз и нарушителя, сформированных в соответствии с нормативными и методическими документами ФСТЭК России, определяются требования к средствам защиты информации, входящим в зону ответственности ФСТЭК России, а также требования к поддерживающим эти средства организационным мерам.

Процесс формирования требований к системе защиты персональных данных заканчивается, если выполнение установленных требований нейтрализует все угрозы, перечисленные в моделях угроз и нарушителя.

Если выполнение установленных требований нейтрализует не все угрозы, перечисленные в моделях угроз и нарушителя, сформированных в соответствии с нормативными и методическими документами ФСТЭК России, на основе моделей угроз и нарушителя, сформированных в соответствии с нормативными документами ФСБ России, определяются требования к средствам защиты информации, входящих в зону ответственности ФСБ России., а также требования к поддерживающим эти средства организационным мерам.

Вопросы контроля и надзора рассмотрены в п. 10 настоящей Концепции.

7. ОБЩИЕ ХАРАКТЕРИСТИКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА СВЯЗИ

Информационные системы персональных данных Оператора связи функционируют в рамках корпоративной информационной системы (КИС) и являются её частью.

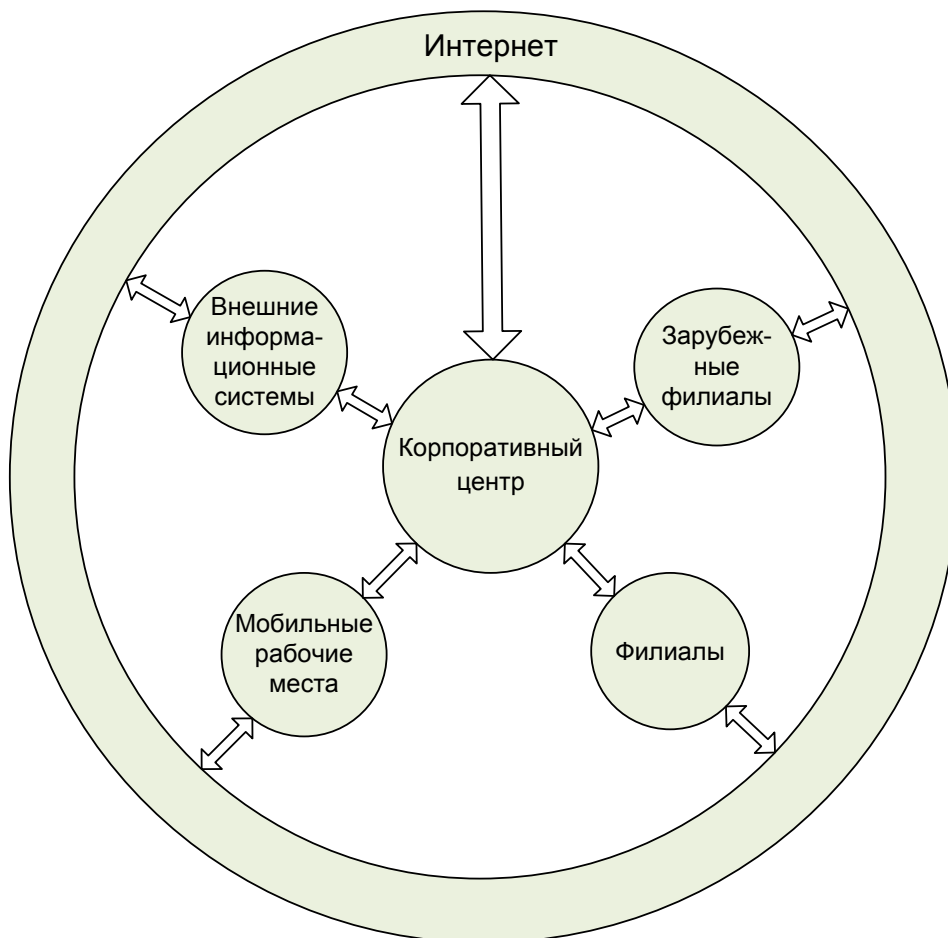


Схема организации КИС Оператора связи

КИС является основой информационно-технологической инфраструктуры (далее – ИТ – инфраструктура), поддерживающей решение актуальных задач и обеспечивающая достижение бизнес-целей Оператора связи. Она представляет собой территориально распределенную совокупность программно-технических комплексов (ПТК), объединенных с помощью каналов связи, в том числе доверенных, расположенных на всех уровнях управления Оператора связи:

1. Корпоративный центр;
2. Филиалы;
3. Зарубежные филиалы;

4. Внешние информационные системы (дилеры Оператора связи, другие внешние организации, имеющие доступ к ИСПДн Оператора связи);
5. Мобильные пользователи.

Управление представляет собой совокупность целенаправленных действий, включающих планирование и проведение мероприятий по защите персональных данных и осуществляется централизованно из корпоративного центра, в подчинении которого находятся филиалы Оператора связи.

Для связи между ПТК используются:

- собственные оптоволоконные каналы связи;
- спутниковые каналы связи;
- радиоканалы (в т.ч. радиорелейные);
- проводные каналы связи;
- каналы связи Операторов связи;
- физические носители информации (съёмные носители информации, бумажные носители).

При этом каналы связи по наличию контроля со стороны Оператора связи могут быть следующих типов:

- контролируемые – каналы связи, защищенные от НСД к информации режимными, организационно-техническими и техническими мерами, направленными на обеспечение заданных характеристик безопасности, использование которых контролируется оператором связи;
- неконтролируемые – каналы связи, использование которых контролируется сторонними организациями (сторонние организации гарантируют безопасность ПДн на основе договора);

По уровню защищенности каналы связи могут быть следующих типов:

- защищенные каналы:
 - доверенные каналы – каналы связи, которые обеспечивают конфиденциальность и (или) целостность информации, а также реализуют взаимную аутентификацию ПТК или их компонент;

- защищенные волоконно-оптические линии связи, безопасность передаваемой информации в которых определяется физической средой распространения и значительной сложностью перехвата передаваемого в ней информационного сигнала;
- открытые каналы – сети связи общего пользования и (или) сети международного информационного обмена (Интернет), не обеспечивающие безопасность передаваемой информации.

В состав средств защиты ПДн при использовании доверенного канала, входят следующие механизмы:

- механизмы взаимной аутентификации компонент ПТК;
- механизмы обеспечения конфиденциальности передаваемой в рамках доверенного канала информации;
- механизмы обеспечения целостности передаваемой в рамках доверенного канала информации.

По структуре информационные системы персональных данных Операторов связи являются локальными информационными системами, состоящими из комплекса технических и программных средств, предназначенных для обработки персональных данных, и функционирующих в доверенной среде эксплуатации.

Классификация информационных систем персональных данных Операторов связи осуществляется в соответствии с Отраслевым классификатором.

Информационные системы персональных данных Операторов связи подразделяются на два типа:

- к первому типу относятся автоматизированные рабочие места, являющиеся локальными информационными системами, не имеющими подключений к сетям связи общего пользования и (или) сетям международного информационного обмена;
- ко второму типу относятся локальные информационные системы и (или) комплексы локальных информационных систем, объединенных в единую информационную систему средствами связи, не имеющими подключений к сетям

связи общего пользования и (или) сетям международного информационного обмена.

Класс автоматизированного рабочего места определяется по его функционально-технологическому принципу:

АРМ.А – специальная информационная система персональных данных Оператора связи, представляющая собой автоматизированное рабочее место администратора, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, может привести к негативным последствиям для субъектов персональных данных;

АРМ.П – специальная информационная система персональных данных Оператора связи, представляющая собой автоматизированное рабочее место пользователя, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, может привести к незначительным негативным последствиям для субъектов персональных данных.

Локальной информационной системе и (или) комплексу локальных информационных систем, объединенных в единую информационную систему средствами связи, присваивается один из следующих классов:

ИСПДНОС2с – специальная информационная система персональных данных Оператора связи, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, может привести к негативным последствиям для субъектов персональных данных;

ИСПДНОС3с – специальная информационная система персональных данных Оператора связи, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, может привести к незначительным негативным последствиям для субъектов персональных данных;

ИСПДНОС4с – специальная информационная система персональных данных Оператора связи, для которой нарушение заданных характеристик безопасности персональных данных, обрабатываемых в ней, не приводит к негативным последствиям для субъектов персональных данных.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите персональных данных.

8. МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДН В ИСПДН ОПЕРАТОРА СВЯЗИ

8.1 Модель угроз безопасности персональных данных

В информационных системах персональных данных Операторов связи рассматриваются угрозы связанные:

- с перехватом (съемом) персональных данных по техническим каналам с целью их копирования или неправомерного распространения;
- с несанкционированным, в том числе случайным, доступом в ИСПДн с целью изменения, копирования, неправомерного распространения ПДн или деструктивных воздействий на элементы ИСПДн и обрабатываемых в них ПДн с использованием программных и программно-аппаратных средств с целью уничтожения или блокирования ПДн.

Конечный перечень угроз безопасности персональных данных определяется частными моделями угроз, разрабатываемыми применительно к конкретным ИСПДн на этапах их создания и (или) эксплуатации и зависит от характеристик ИСПДн, обуславливающих возникновение угроз безопасности персональных данных. К таким характеристикам относятся: категория и объем обрабатываемых в ИСПДн персональных данных, структура ИСПДн, наличие подключений ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, характеристики подсистемы безопасности ПДн, обрабатываемых в ИСПДн, режимы обработки персональных данных, режимы разграничения прав доступа пользователей ИСПДн, местонахождение и условия размещения технических средств ИСПДн.

Частные модели угроз безопасности ПДн рекомендуется разрабатывать на основе «Отраслевой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных Операторов связи» или «Модели угроз и нарушителя безопасности персональных данных, обрабатываемых в специальных информационных системах персональных данных отрасли связи».

8.2 Модель нарушителя безопасности персональных данных

Основным источником угроз безопасности персональных данных является нарушитель.

В качестве нарушителя безопасности персональных данных могут выступать физические лица или организации, которые преднамеренно или случайно совершают действия, в результате которых нарушаются заданные характеристики безопасности персональных данных.

Нарушитель может быть как законным абонентом (принадлежать к персоналу Оператора связи), так и посторонним лицом, пытающимся непосредственно или с помощью имеющихся у него технических и программных средств получить доступ к информационным ресурсам и инфраструктуре сети Оператора связи.

В зависимости от прав доступа к ресурсам ИСПДн нарушители подразделяются на два типа: внешние и внутренние.

Внешними нарушителями могут являться:

- конкурирующие организации и структуры;
- организованные преступные группы, сообщества;
- взломщики программных продуктов информационных технологий, использующихся в системах связи;
- бывшие сотрудники Оператора связи;
- недобросовестные сотрудники и партнеры;
- пользователи услугами связи.

Внутренние (потенциальные) нарушители определяются в зависимости от организационно-штатной структуры Оператора связи и полномочий доступа к ресурсам ИСПДн.

Основными мотивами нарушения безопасности персональных данных могут быть:

- месть;
- достижение денежной выгоды, в том числе за счет продажи полученной информации;
- хулиганство и любопытство;
- профессиональное самоутверждение.

9. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для разработки и осуществления мероприятий по организации и обеспечению безопасности ПДн при их обработке в ИСПДн Оператором связи или уполномоченным им лицом назначается структурное подразделение или должностное лицо (работник), ответственное за обеспечение безопасности ПДн.

Основными мероприятиями по организации и техническому обеспечению безопасности ПДн в ИСПДн являются:

- мероприятия по организации обеспечения безопасности ПДн, включая классификацию ИСПДн;
- мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн, включающие мероприятия по размещению, специальному оборудованию, охране и организации режима допуска в помещения, где ведется работа с ПДн;
- мероприятия по защите ПДн от несанкционированного доступа и определению порядка выбора средств защиты ПДн при их обработке в ИСПДн.

Обеспечение безопасности ПДн осуществляется путем выполнения комплекса организационных и технических мероприятий, реализуемых в рамках создаваемой СЗПДн. Структура, состав и основные функции СЗПДн определяются с учетом класса ИСПДн Оператора связи.

Перечень реализуемых мероприятий по защите ПДн при их обработке в специальных ИСПДн Оператора связи определяется на основании анализа актуальности угроз, рисков безопасности ПДн и профилей защиты ПДн для ИСПДн Оператора связи, в соответствии с нормативными и методическими документами ФСБ России и ФСТЭК России.

ИСПДн по своим характеристикам и номенклатуре угроз безопасности ПДн близки к наиболее распространенным информационным системам, поэтому целесообразно при их защите максимально использовать традиционные подходы к технической защите информации в автоматизированных системах.

Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю

и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

В соответствии с нормативными документами Федеральной службы по техническому и экспортному контролю:

- осуществляется обеспечение защиты (некриптографическими методами) информации;
- проводятся мероприятия по предотвращению утечки информации по техническим каналам;
- проводятся мероприятия по предотвращению несанкционированного доступа к информации, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, и блокирования доступа к ней.

В соответствии с нормативными документами Федеральной службы безопасности Российской Федерации:

- устанавливаются особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах;
- проводятся мероприятия по обнаружению компьютерных атак.

Мероприятия по обеспечению безопасности ПДн включают в себя:

- управление доступом:
 - идентификация и аутентификация;
 - физическая защита;
- регистрацию и учет;
- обеспечение конфиденциальности;
- обеспечение целостности;
- обеспечение доступности;
- обеспечение достоверности (аутентичности);
- антивирусную защиту;
- обеспечение безопасного межсетевого взаимодействия;
- анализ защищенности;

- обнаружение вторжений;
- обеспечение безопасности мобильных рабочих мест;
- обеспечение безопасного доступа к сетям международного информационного обмена.

9.1 Идентификация и аутентификация

Управление доступом к ПДн должно осуществляться на основе принципа минимизации полномочий. Стандартным методом доступа является ролевой доступ, для чего определяются совокупности типов доступа - групповых прав и полномочий доступа пользователей (ролей), предоставляемых пользователям. Количество таких ролей должно быть ограниченным и подразумевать возможность эффективного управления. Назначение прав и полномочий конкретным пользователям осуществляется путем назначения им соответствующих ролей.

Каждый пользователь для получения соответствующих прав доступа при подключении к ИСПДн должен пройти процедуру идентификации, при этом должны использоваться уникальные признаки и имена. При этом подлинность личности пользователя должна быть проверена. Стандартное средство проверки подлинности (аутентификации) – пароль. Для обеспечения более высокой надежности аутентификации возможно использование таких средств как токены, смарт-карты и другие носители аутентифицирующей информации.

9.2 Физическая защита

Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации.

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

9.3 Регистрация и учет

В ИСПДн должны вестись контрольные журналы, регистрирующие действия пользователей с ПДн. Должны быть установлены процедуры применения мониторинга действий с ПДн, а результаты действий пользователей должны регулярно просматриваться.

В целях повышения эффективности контроля действий возможных нарушителей настоящая Концепция предлагает использование средств и методов активного мониторинга и аудита, направленных на выявление и регистрацию подозрительных действий в реальном масштабе времени.

9.4 Обеспечение целостности

Оператор связи обеспечивает целостность программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонентов СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ.

Обеспечение целостности реализуется преимущественно операционными системами и системами управления базами данных. Средства повышения достоверности и обеспечения целостности передаваемых данных и надежности транзакций, встраиваемые в операционные системы и системы управления базами данных, основаны на расчете контрольных сумм, уведомлении о сбое в передаче пакета сообщения, повторе передачи не принятого пакета.

9.5 Антивирусная защита

Для обеспечения безопасности ПДн и программно-аппаратной среды ИСПДн, осуществляющей обработку этой информации, необходимо применять специальные средства антивирусной защиты, выполняющие:

- обнаружение и (или) блокирование деструктивных вирусных воздействий на общесистемное и прикладное программное обеспечение, реализующее обработку ПДн, а также на ПДн;
- обнаружение и удаление неизвестных вирусов;
- обеспечение самоконтроля (предотвращение инфицирования) данного антивирусного средства при его запуске.

9.6 Обеспечение безопасного межсетевого взаимодействия

Для осуществления разграничения доступа к ресурсам ИСПДн при межсетевом взаимодействии должно применяться межсетевое экранирование, которое реализуется программными и программно-аппаратными межсетевыми экранами. Межсетевой экран устанавливается между защищаемой сетью, называемой внутренней, и внешней сетью. Межсетевой экран входит в состав защищаемой сети. Для него путем настроек отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю и наоборот.

Межсетевое экранирование должно обеспечивать:

- скрывание внутренней сетевой структуры ИСПДн;
- разрешение только такого входящего и исходящего трафика, который является необходимым для работы ИСПДн;
- блокирование любого входящего и исходящего трафика, не разрешенного явно.

9.7 Анализ защищенности

Анализ защищенности реализуется на основе использования средств тестирования (анализа защищенности) и контроля (аудита) безопасности информации.

Для гарантии того, что СЗИ успешно выполняют свои функции, должны быть разработаны процедуры контроля изменений конфигураций СЗИ и сетевых устройств. Для выполнения этих процедур в информационно-телекоммуникационной среде Оператора связи должна быть создана система анализа защищенности, выполняющая следующие функции:

- контроль настроек сетевых устройств, СЗИ и программно-технического обеспечения ИСПДн;
- анализ уязвимостей настроек СЗИ, сетевых устройств или уязвимостей операционных систем или прикладного программного обеспечения.

9.8 Обнаружение вторжений

Обнаружение вторжений реализуется с использованием в составе СЗПДн Оператора связи программных и (или) программно-аппаратных средств (систем)

обнаружения вторжений, использующих комбинированные методы обнаружения атак, включающие в себя сигнатурные методы и методы выявления аномалий.

9.9 Криптографическая защита

Для защиты ПДн, передаваемых между ИСПДн по каналам связи, выходящим за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, включая доверенные каналы и защищенные волоконно-оптические линии связи.

При использовании открытых и неконтролируемых каналов связи для защиты ПДн необходимо применять средства криптографической защиты информации (далее – СКЗИ). Как отдельно, так и комплексно, используются следующие криптографические методы:

- шифрование, как средство обеспечения конфиденциальности информации;
- электронная цифровая подпись, как средство обеспечения подлинности и юридической значимости электронного документа;
- криптографическая аутентификация, как средство подтверждения санкционированности доступа субъекта к объекту;
- управление ключами, как необходимая составная часть систем с СКЗИ, которая применяется в целях изготовления, учета, распределения, хранения и уничтожения ключевых элементов.

9.10 Обеспечение безопасности мобильных рабочих мест

В случае необходимости Оператор связи может организовывать доступ к ПДн с АРМ, расположенных за пределами контролируемой зоны (мобильных рабочих мест).

При использовании мобильных рабочих мест (МРМ) Оператор связи реализует ряд дополнительных организационно-технических мер обеспечения безопасности ПДн:

- обеспечение доверенной загрузки операционной среды МРМ;
- обеспечение доверенной среды эксплуатации МРМ;
- обеспечение доверенного (защищенного) канала взаимодействия с ИСПДн Оператора связи;

- очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти МРМ и накопителей информации.

Обеспечение доверенной загрузки основывается на загрузке операционных систем только с заранее определенных постоянных носителей в комплексе с использованием специальных средств контроля над составом аппаратных средств ПЭВМ, целостности программных модулей операционных систем и средств усиленной аутентификации.

Доверенная среда эксплуатации и доверенный (защищенный) канал взаимодействия обеспечивается путем использования специальных СЗИ и средств криптографической защиты информации.

По окончании информационного взаимодействия на МРМ должно производиться удаление ПДн и другой информации, которая может быть использована для осуществления НСД к ПДн Оператора связи.

9.11 Обеспечение безопасного доступа к сетям международного информационного обмена

Доступ ИСПДн к сетям связи общего пользования и (или) сетям международного информационного обмена, в том числе к международной компьютерной сети «Интернет» допускается только с использованием специально предназначенных для этого средств защиты информации.

При принятии Оператором связи решений об использовании сети «Интернет» необходимо учитывать следующие положения:

- сеть «Интернет» не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение).
- провайдеры (посредники) сети «Интернет» могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством сети «Интернет»;

- существует вероятность атаки злоумышленников на оборудование, программное обеспечение и информационные ресурсы, подключенные/доступные из сети «Интернет»;
- гарантии по обеспечению безопасности ПДн при использовании сети «Интернет» никаким органом/учреждением/организацией не предоставляются.

10. ПРИНЦИПЫ ОЦЕНКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА СВЯЗИ

В соответствии с принципом обязательности контроля (раздел 5.16) выполняются следующие виды контроля эффективности системы защиты персональных данных:

- внутренний контроль;
- государственный контроль.

10.1 Внутренний контроль

Внутренний контроль эффективности системы защиты ПДн осуществляется Оператором связи с целью поддержания заданного уровня эффективности СЗПДн, в соответствии с документированными методиками. Внутренний контроль включает:

- мониторинг состояния технических и программных средств, входящих в состав СЗПДн;
- контроль соблюдения требований по обеспечению безопасности ПДн (требований законодательства в области защиты ПДн, требований внутренних нормативно-методических и организационно-распорядительных документов Оператора связи, сформулированных на основе анализа рисков нарушения безопасности ПДн, договорных требований).

Оценка эффективности СЗПДн реализуется в виде аттестации или декларирования соответствия требованиям по безопасности ПДн.

Декларирование производится по факту ввода в эксплуатацию ИСПДн. Ввод в эксплуатацию ИСПДн производится в соответствии с документально оформленными требованиями по безопасности ПДн (техническими условиями¹), разрабатываемыми Оператором в соответствии с требованиями законодательства и нормативно-методических документов федеральных органов исполнительной власти, осуществляющими функции по контролю и надзору в пределах своих полномочий.

¹ Технические условия разрабатываются в соответствии с требованиями ГОСТ 2.114-95 и должны содержать в своем составе методику оценки соответствия требованиям по безопасности ПДн.

Факт ввода в эксплуатацию ИСПДн в соответствии с техническими условиями оформляется Актом ввода в эксплуатацию и утверждается приказом по организации Оператора связи.

Внутренний контроль проводится периодически, либо инициируется по мере необходимости Оператором связи.

10.2 Государственный контроль

Государственный контроль и надзор за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных осуществляется Роскомнадзором.

Контроль и надзор за выполнением требований безопасности персональных данных при их обработке в ИСПДн осуществляются ФСБ России и ФСТЭК России, в пределах их полномочий.

11. ПОРЯДОК ПЕРЕСМОТРА КОНЦЕПЦИИ

Положения настоящей Концепции пересматриваются в установленном порядке не реже одного раза в 2 года.

Внеплановый пересмотр Концепции проводится в случае существенных изменений международного или национального законодательства в сфере защиты ПД.

При внесении изменений в положения Концепции учитываются:

- уровень развития и внедрения информационных технологий в телекоммуникационной отрасли;
- рекомендации российских и международных профильных организаций по информационной безопасности и защите ПДн;
- рекомендации Консультационного совета при уполномоченном органе по защите прав субъектов ПДн.

Приложение 1. НОРМАТИВНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

- 1) Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 09.09.2000 г. № Пр-1895
- 2) Концепция национальной безопасности Российской Федерации. Утверждена указом Президента Российской Федерации от 17.12.1997 г. №1300
- 3) Закон Российской Федерации от 05.03.1992 г. № 2446-1 "О безопасности"
- 4) Федеральный закон от 27.07.2006 г. №152-ФЗ «О персональных данных»
- 5) Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»
- 6) Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи»
- 7) Указ Президента Российской Федерации от 06.03.1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»
- 8) Трудовой кодекс Российской Федерации
- 9) Гражданский кодекс Российской Федерации
- 10) Постановление Правительства Российской Федерации от 17.11.2007 г. №781 «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- 11) Постановление Правительства Российской Федерации от 15.09.2008 г. № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- 12) Постановление Правительства Российской Федерации от 06.07.08 №512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
- 13) Приказ Федеральной службы по техническому и экспортному контролю, Федеральной службы безопасности Российской Федерации,

Министерства информационных технологий и связи Российской Федерации от 13.02.2008 г. №55/86/20 "Об утверждении порядка проведения классификации информационных систем персональных данных"

14) Приказ Федеральной службы по техническому и экспортному контролю от 5.02.2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»

15) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008 г.

16) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14.02.2008 г.

17) Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/5-144.

18) 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 обработке в информационных системах персональных данных. Утверждены руководством 8 Центра ФСБ России 21.02.2008 г. №149/6/6-622.

19) ГОСТ Р 52448-2005. Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

20) ГОСТ Р 53110-2008. Система обеспечения информационной безопасности сети связи общего пользования. Общие положения.