ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«АСТРАХАНЬ-ПЕЙДЖ»

УТВЕРЖДАЮ

Генеральный директор

_____ /Курьянов С.В./

«_____» _____ 20__г.

ПОЛОЖЕНИЕ
О ЗАЩИТЕ И ОБРАБОТКЕ
ОПЕРАТОРОМ СВЯЗИ ПЕРСОНАЛЬНЫХ ДАННЫХ АБОНЕНТОВ

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.

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, 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.

ОБЩИЕ ПОЛОЖЕНИЯ

Назначение положения

Положение о защите персональных данных в информационных системах персональных данных Оператора связи (далее – Концепция) является отраслевым нормативным 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 Оператора связи, режима 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 Оператора 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.
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.

СФЕРА ДЕЙСТВИЯ И ОБЛАСТЬ РАСПРОСТРАНЕНИЯ КОНЦЕПЦИИ

Технологические сети связи Оператора 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.

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.

Основной задачей обеспечения безопасности персональных данных, при их обработке в информационных системах персональных данных Оператора 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.

ПЕРСОНАЛЬНЫЕ ДАННЫЕ, ОБРАБАТЫВАЕМЫЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ОПЕРАТОРОВ СВЯЗИ

Категории субъектов персональных данных

Субъекты, персональные данные которых обрабатываются в информационных системах Оператора 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:

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.

Персональные данные Абонентов не распространяются, а также не предоставляются третьим лицам без письменного согласия Абонента и используются Оператором связи исключительно для исполнения и заключения указанного договора с Абонентом.

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.

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

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.

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.

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.

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.

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.

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.

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.

Разумная достаточность и адекватность
Состояние и стоимость реализации мер защиты должно быть соизмеримы с рисками, связанными с обработкой и характером защищаемых ПДн.
Программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики и производительность ИСПДн Оператора связи.

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

Минимизация полномочий
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.

Гибкость
В процессе функционирования ИСПДн могут меняться ее характеристики, а также объем и категория обрабатываемых Оператором связи ПДн.
Специализация и профессионализм
Реализация мер по обеспечению безопасности ПДн и эксплуатация СЗПДн должна осуществляться профессионально подготовленными специалистами Оператора связи.

ОБЩИЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Административно-правовые методы
К административно-правовым методам защиты относятся нормы действующего законодательства 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 неправомерному использованию ПДн и являющиеся сдерживающим фактором для реализации угроз безопасности потенциальными нарушителями.

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.

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.

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

МОДЕЛЬ УГРОЗ И НАРУШИТЕЛЯ БЕЗОПАСНОСТИ ПДН В ИСПДН ОПЕРАТОРА СВЯЗИ

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.

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.

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

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.
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:

Идентификация и аутентификация
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.

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.

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.

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.

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.

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 раздельно, 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.

ПРИНЦИПЫ ОЦЕНКИ И КОНТРОЛЯ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОПЕРАТОРА СВЯЗИ

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

Государственный контроль
Обеспечение государственного контроля и надзора за соответствием обработки ПДн требованиям законодательства Российской Федерации в области защиты ПДн осуществляется федеральными органами исполнительной власти.
В соответствии с действующим законодательством распределение полномочий между федеральными органами исполнительной власти Роскомнадзором, ФСБ России и ФСТЭК России при осуществлении государственного контроля и надзора за соблюдением требований законодательства Российской Федерации в области защиты персональных данных осуществляется в пределах их компетенции.

ПОРЯДОК ПЕРЕСМОТРА КОНЦЕПЦИИ

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.