



ПТВЕРЖДАЮ
Директор
ООО «Санрайз»
И.М. Рясина

И.М. Рясина 2026 г.

ПОЛИТИКА
информационной безопасности
при работе с персональными данными в ООО «Санрайз»

СОДЕРЖАНИЕ

Содержание.....	2
Определения.....	3
Обозначения и сокращения.....	11
Введение.....	12
1. Общие положения.....	14
2. Область действия.....	15
3. Система защиты персональных данных.....	16
4. Требования к подсистемам СЗПДн.....	18
Подсистемы управления доступом, регистрации и учета.....	18
Подсистема обеспечения целостности и доступности.....	19
Подсистема антивирусной защиты.....	19
Подсистема межсетевое экранирование.....	20
Подсистема анализа защищенности.....	21
5. Пользователи ИСПДн.....	22
6. Требования к персоналу по обеспечению защиты ПДн.....	25
Должностные обязанности пользователей ИСПДн.....	26
Ответственность сотрудников ИСПДн.....	27
7. Список использованных источников.....	29

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

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

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

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

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на

персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

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

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

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

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

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

нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанному в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными

данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

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

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

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

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

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, заблокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) заблокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

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

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы 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 персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в

результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства

АРМ – автоматизированное рабочее место

ВТСС – вспомогательные технические средства и системы

ИСПДн – информационная система персональных данных

КЗ – контролируемая зона

ЛВС – локальная вычислительная сеть

МЭ – межсетевой экран

НСД – несанкционированный доступ

ОС – операционная система

ПДн – персональные данные

ПМВ – программно-математическое воздействие

ПО – программное обеспечение

ПЭМИН – побочные электромагнитные излучения и наводки

САЗ – система анализа защищенности

СЗИ – средства защиты информации

СЗИПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Настоящая Политика информационной безопасности (далее – Политика) в ООО «Санрайз», является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных, изложенных в Положении информационной безопасности ИСПДн ООО «Санрайз».

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных», на основании:

~ Требованиям к защите персональных данных при их обработке в информационных системах персональных данных, утвержденных Постановлением Правительства РФ от 01.11.2012 г. № 1119;

~ Приказа ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

~ Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае из использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников,

ответственных за обеспечение безопасности персональных данных в ИСПДн
ООО «Санрайз».

1. Общие положения

Целью настоящей Политики является обеспечение безопасности объектов защиты ООО «Санрайз» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в «Перечне персональных данных, подлежащих защите».

Состав ИСПДн подлежащих защите, представлен в «Перечне ИСПДн».

2.Область действия

Требования настоящей Политики распространяются на всех сотрудников ООО «Санрайз» (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

3. Система защиты персональных данных

Система защиты персональных данных (СЗПДн), строится на основании:

- ~ Итогового отчета об обследовании ИСПДн;
- ~ Отчета о результатах проведения внутренней проверки защиты ПДн на бумажных носителях.
- ~ Перечня персональных данных, подлежащих защите;
- ~ Акта классификации информационной системы персональных данных;
- ~ Модели угроз безопасности персональных данных;
- ~ Матрицы доступа пользователей к защищаемым информационным ресурсам ИСПДн;
- ~ Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн ООО «Санрайз». На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн. Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

Для ИСПДн должен быть составлен список используемых технических средств защиты (далее - Список), а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- ~ АРМ пользователей;
- ~ Сервера приложений;
- ~ СУБД;
- ~ Граница ЛВС;
- ~ Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

- ~ антивирусные средства для рабочих станций пользователей и серверов;
- ~ средства межсетевого экранирования;
- ~ средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Также в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- ~ управление и разграничение доступа пользователей;
- ~ регистрацию и учет действий с информацией;
- ~ обеспечивать целостность данных;
- ~ производить обнаружений вторжений.

Список используемых технических средств отражается в «Плане мероприятий по обеспечению защиты персональных данных». Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены руководителем ООО «Санрайз» или лицом, ответственным за обеспечение защиты ПДн.

4. Требования к подсистемам СЗПДн

СЗПДн включает в себя следующие подсистемы:

- ~ управления доступом, регистрации и учета;
- ~ обеспечения целостности и доступности;
- ~ антивирусной защиты;
- ~ межсетевое экранирование;
- ~ анализа защищенности;
- ~ обнаружения вторжений;
- ~ криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в «Акте классификации информационной системы персональных данных». Список соответствия функций подсистем СЗПДн классу защищенности представлен в техническом задании по созданию системы защиты информации информационной системы персональных данных.

Подсистемы управления доступом, регистрации и учета

Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций:

- ~ идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
- ~ идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- ~ идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- ~ регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- ~ регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

~ регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн ООО «Санрайз», а так же средств защиты, при случайной или намеренной модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.

Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн ООО «Санрайз».

Средства антивирусной защиты предназначены для реализации следующих функций:

- ~ резидентный антивирусный мониторинг;
- ~ антивирусное сканирование;
- ~ скрипт-блокирование;

~ централизованную/удаленную установку/деинсталляцию антивирусного
~ продукта, настройку, администрирование, просмотр отчетов и
~ статистической информации по работе продукта;

~ автоматизированное обновление антивирусных баз;

~ ограничение прав пользователя на остановку исполняемых задач и
~ изменения настроек антивирусного программного обеспечения;

~ автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

Подсистема межсетевого экранирования

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

~ фильтрации открытого и зашифрованного (закрытого) IP-трафика;

~ фиксации во внутренних журналах информации о проходящем
~ открытом и закрытом IP-трафике;

~ идентификации и аутентификацию администратора межсетевого экрана
~ при его локальных запросах на доступ;

~ регистрации входа (выхода) администратора межсетевого экрана в
~ систему (из системы) либо загрузки и инициализации системы и ее
~ программного останова;

~ контроля целостности своей программной и информационной части;

~ фильтрации пакетов служебных протоколов, служащих для диагностики
~ и управления работой сетевых устройств;

~ фильтрации с учетом входного и выходного сетевого интерфейса как
~ средство проверки подлинности сетевых адресов;

~ регистрации и учета запрашиваемых сервисов прикладного уровня;

~ блокирования доступа не идентифицированного объекта или субъекта,
~ подлинность которого при аутентификации не подтвердилась, методами,
~ устойчивыми к перехвату;

контроля за сетевой активностью приложений и обнаружения сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе ЛВС, классом не ниже 4.

Подсистема анализа защищенности

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема обнаружения вторжений

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн ООО «Санрайз», при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрения криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн

В Положении информационной безопасности определены основные категории пользователей. На основании этих категории должна быть

произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн ООО «Санрайз» можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- ~ Администратора ИСПДн;
- ~ Администратора безопасности;
- ~ Оператора АРМ;

Данные о группах пользователей, уровне их доступа и информированности должен быть отражен в Матрице доступа пользователей к защищаемым информационным ресурсам.

Администратор ИСПДн

Администратор ИСПДн, сотрудник ООО «Санрайз», ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- ~ обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;
- ~ обладает полной информацией о технических средствах и конфигурации ИСПДн;
- ~ имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;
- ~ обладает правами конфигурирования и административной настройки технических средств ИСПДн.

Администратор безопасности

Администратор безопасности, сотрудник ООО «Санрайз», ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- ~ обладает правами Администратора ИСПДн;
 - ~ обладает полной информацией об ИСПДн;
 - ~ имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;
- Администратор безопасности уполномочен:
- ~ реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
 - ~ осуществлять аудит средств защиты;

Оператор АРМ

Оператор АРМ, сотрудник ООО «Санрайз», осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- ~ обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;
- ~ располагает конфиденциальными данными, к которым имеет доступ.

6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники ООО «Санрайз», являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники ООО «Санрайз», использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники ООО «Санрайз» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники ООО «Санрайз» должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами, третьим лицам.

При работе с ПДн в ИСПДн сотрудники ООО «Санрайз» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.

При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ООО «Санрайз» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- ~ Инструкция администратора ИСПДн;
- ~ Инструкция администратора безопасности ИСПДн;
- ~ Инструкция пользователя ИСПДн;

Инструкция пользователя при возникновении внештатных ситуаций;

Ответственность сотрудников

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

Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ).

Администратор ИСПДн и администратор безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками ООО «Санрайз» – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в Положениях о подразделениях ООО «Санрайз», осуществляющих обработку ПДн в ИСПДн и должностных инструкциях сотрудников ООО «Санрайз».

Необходимо внести в Положения о подразделениях ООО «Санрайз», осуществляющих обработку ПДн в ИСПДн сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.