ПОЛИТИКА
БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ ООО «ТРЭВЕЛ ЛАЙН СИСТЕМС»

1. Область применения

Настоящая Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции безопасности персональных данных, обрабатываемых в информационных системах персональных данных ООО «ТРЭВЕЛ ЛАЙН СИСТЕМС» (далее – Общество).

В Настоящей Политике определены требования к работникам Общества, степень ответственности работников, структура и необходимый уровень защищенности, статус и должностные обязанности работников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных Общества.

Настоящая Политика разработана с учетом требований Конституции Российской Федерации, а также в соответствии с федеральными законами и подзаконными актами Российской Федерации, определяющими порядок обработки персональных данных, обеспечения безопасности и конфиденциальности такой информации.

Настоящая Политика разработана в целях обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных в Обществе.

Положения настоящей Политики служат основой для разработки локальных нормативных актов Общества, регламентирующих вопросы обработки и защиты персональных данных работников Общества и других субъектов персональных данных, оператором которых является Общество.

Положения настоящей Политики являются обязательными для исполнения работниками Общества, имеющими доступ к персональным данным.

2. Термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

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.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Доступ к информации – возможность получения информации и её использования.

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.

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

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

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

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 распространять их без согласия субъекта персональных данных или наличия иного законного основания.

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.

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 невозможно 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.

Объект вычислительной техники – стационарный или подвижный объект, который представляет собой комплекс средств вычислительной техники, предназначенный для выполнения определенных функций обработки информации. К объектам вычислительной техники относятся автоматизированные системы, автоматизированные рабочие места, информационно-вычислительные центры и другие комплексы средств вычислительной техники. К объектам вычислительной техники могут быть отнесены также отдельные средства вычислительной техники, выполняющие самостоятельные функции обработки информации.

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.

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

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.

Предоставление персональных данных – действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц.

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

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.

Система защиты персональных данных – совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты персональных данных.

Средство криптографической защиты информации – средство защиты информации, реализующее алгоритмы криптографического преобразования информации.

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

Субъект персональных данных – физическое лицо, которое прямо или косвенно определено или определяемо с помощью персональных данных.

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

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие 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.

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 ИСПДн.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных 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.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность

информации в условиях случайного и/или преднамеренного искажения (разрушения).

3. Сокращения

В настоящем документе используются следующие сокращения.

Общество	ООО «ТРЭВЕЛ ЛАЙН СИСТЕМС».
ПДн	персональные данные
ИСПДн	информационная система персональных данных
ИБ	информационная безопасность
СЗПДн	система защиты персональных данных

4. Общие положения

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

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей. В ИСПДн должно осуществляться своевременное обнаружение угроз и реагирование на угрозы безопасности ПДн.

В ИСПДн необходимо исключить возможность преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Перечень ПДн, подлежащих защите, определяется в Положении об обработке ПДн Общества.

5. Система защиты персональных данных

СЗПДн строится на основании:

- Перечня ПДн, подлежащих защите;
- Перечня ИСПДн;
- Акта определения уровня защищенности ПДн при их обработке в ИСПДн;
- Частной модели угроз и нарушителя безопасности ПДн;
- Положения о разграничении прав доступа к обрабатываемым ПДн;
- Руководящих документов ФСТЭК России и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн данных в каждой ИСПДн Общества. Для каждой ИСПДн должен быть составлен список используемых технических средств, а также программного обеспечения участвующего в обработке ПДн, подлежащих защите.

В зависимости от уровня защищенности ПДн в ИСПДн и актуальных угроз, система защиты ПДн может включать следующие технические и программные средства:

– антивирусные средства для объектов вычислительной техники;
– средства межсетевого экранирования;
– средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами ИСПДн и операционных систем, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты.

Список функций защиты может включать:
– управление доступом и разграничение доступа пользователей;
– регистрацию и учет действий с информацией;
– обеспечение целостности данных;
– обнаружение вторжений.

Список используемых средств должен поддерживаться в актуальном состоянии. Все изменения состава СЗПДн или элементов ИСПДн должны быть согласованы с Администратором ИБ.

6. Требования к подсистемам системы защиты персональных данных

СЗПДн включает в себя следующие подсистемы:
– управления доступом, регистрации и учета;
– обеспечения целостности и доступности;
– антивирусной защиты;
– межсетевого экранирования;
– анализа защищенности;
– обнаружения вторжений;
– криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от уровня защищенности ПДн при их обработке в ИСПДн, определенного в Акте определения уровня защищенности ПДн при их обработке в ИСПДн.

6.1. 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 регистрации 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). 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.

6.2. Подсистема обеспечения целостности и доступности

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн Общества, 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.

6.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты объектов вычислительной техники Общества.

Средства антивирусной защиты предназначены для реализации следующих функций:

– резидентный антивирусный мониторинг;

– антивирусное сканирование;

– скрипт-блокирование;

– централизованная/удаленная установка/деинсталляция антивирусного продукта, настройка, 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 во все элементы ИСПДн.

6.4. 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 аутентификации Администратора ИБ или Администратора ИСПДн при его локальных запросах на доступ;

– регистрации входа (выхода) Администратора ИБ или Администратора ИСПДн 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 неидентифицированного 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 сети.

6.5. Подсистема анализа защищенности

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

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

6.6. 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.

6.7. Подсистема криптографической защиты

Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в ИСПДн Общества, при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

7. Пользователи информационной системы персональных данных

В Концепции безопасности ПДн определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.

В ИСПДн Общества можно выделить следующие группы пользователей, участвующих в обработке ПДн:

- Администратор ИСПДн;
- Оператор ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в Положении о разграничении прав доступа к обрабатываемым персональным данным.

7.1. Администратор информационной системы персональных данных

Администратор ИСПДн, работник Общества, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора ИСПДн) 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 в ИСПДн;

– обладает возможностями внесения изменений в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

– обладает правами конфигурирования и административной настройки технических средств ИСПДн.

7.2. Оператор информационной системы персональных данных

Оператор ИСПДн, работник Общества, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в ИСПДн, формирование справок и отчетов по информации, полученной из ИСПДн.

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.

8. Администратор информационной безопасности

Администратор ИБ, работник Общества, назначаемый приказом генерального директора Общества, ответственный за функционирование

СЗПДн, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор ИБ обладает следующим уровнем доступа и знаний:

– обладает полной информацией об ИСПДн;

– имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн;

– не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор ИБ уполномочен:

– реализовывать политики безопасности в части настройки средств защиты информации, межсетевых экранов и систем обнаружения вторжений, в соответствии с которыми пользователь (Оператор ИСПДн) получает возможность работать с элементами ИСПДн;

– осуществлять аудит средств защиты информации;

– осуществлять контроль за действиями пользователей ИСПДн при их работе с персональными данными;

– устанавливать доверительные отношения своей защищенной сети с сетями других организаций и учреждений.

Должностные обязанности Администратора ИБ описаны в Инструкции Администратора ИБ.

9. Требования к работникам по обеспечению защиты персональных данных

Все работники Общества, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению установленного режима безопасности персональных данных.

При вступлении в должность нового работника непосредственный руководитель структурного подразделения 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.

Работник должен быть ознакомлен с настоящей Политикой, установленными процедурами работы с элементами ИСПДн и СЗПДн.

Работники Общества, использующие технические средства аутентификации, должны обеспечивать сохранность персональных идентификаторов (электронных ключей) и не допускать несанкционированный доступ к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники Общества должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства идентификации и аутентификации).

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

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

Работникам запрещается разглашать защищаемую информацию, которая стала им известна в силу выполнения ими своих должностных обязанностей.

При работе с ПДн в ИСПДн работники Общества обязаны исключить возможность просмотра персональных данных третьими лицами с мониторов объектов вычислительной техники.

При завершении работы с ИСПДн работники обязаны защитить объекты вычислительной техники с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Работники Общества 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 работников, нарушающих принятые политику и процедуры безопасности ПДн.

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

10. Должностные обязанности пользователей ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция Администратора ИСПДн;
- Инструкция Оператора ИСПДн.

11. Ответственность пользователей ИСПДн

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

Действующее законодательство Российской Федерации 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).

Пользователи ИСПДн 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 работниками Общества – Пользователями 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 локальных нормативных и правовых актах Общества.