«У Т В Е Р Ж Д А Ю»

Нотариус Видновского нотариального округа Московской области

Мурыгина Олеся Семеновна

_____ /О.С. Мурыгина/

“01” июня 2021 г.

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ НОТАРИУСА ВИДНОВСКОГО НОТАРИАЛЬНОГО ОКРУГА МОСКОВСКОЙ ОБЛАСТИ МУРЫГИНОЙ ОЛЕСИ СЕМЕНОВНЫ

2021 г.

СОДЕРЖАНИЕ

1 ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение безопасности объектов защиты нотариуса Мурыгиной Олеси Семеновны 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 Отчете о результатах проведения внутренней проверки.

2 ОБЛАСТЬ ДЕЙСТВИЯ

Субъектами настоящей Политики информационной безопасности являются все лица, вовлеченные в организационные и технологические процессы сбора, систематизации, накопления, хранения, уточнения (обновления, изменения), использования, распространения (в том числе передачу), обезличивания, блокирования, уничтожения персональных данных, обрабатываемых ИСПДн нотариуса Мурыгиной Олеси Семеновны.

3 СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (СЗИ ПДн), строится на основании:

3.1 Отчета о результатах обследования.

3.2 Модели угроз безопасности персональных данных.

3.3 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3.4 Федерального закона от 30.12.2001 г. №197 ФЗ «Трудовой Кодекс Российской Федерации».

3.5 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных Постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119.

3.6 Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности ПДн ИСПДн нотариуса Мурыгиной Олеси Семеновны. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчета о результатах обследования, делается заключение о необходимости использования средств защиты и организационных мероприятий для обеспечения безопасности ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗИ ПДн 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.

Так же в список могут быть включены СЗИ, обеспечивающие функции защиты:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечение целостности данных;
- обнаружение вторжений.

4 СОСТАВ И СОДЕРЖАНИЕ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

Для обеспечения 4 уровня защищенности персональных данных применяются:

- средства вычислительной техники не ниже 6 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;
- межсетевые экраны 5 класса.

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

4.1 идентификация и аутентификация субъектов доступа и объектов доступа - меры по идентификации и аутентификации субъектов доступа и объектов доступа должны

обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности;

4.2 управление доступом субъектов доступа к объектам доступа - меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил;

4.3 защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных) - меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных;

4.4 регистрация событий безопасности – меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них;

4.5 антивирусная защита – меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации;

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

4.6 контроль (анализ) защищенности персональных данных – меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных;

4.7 обеспечение целостности информационной системы и персональных данных - меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных;

4.8 защита технических средств - меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

Меры по защите технических средств включает в себя в том числе:

- контроль и управление доступом в помещения;
- физическую защиту;
- контроль доступа и разграничения полномочий пользователей.

Контроль и управление доступом в помещения

Контроль и управление доступом в помещения осуществляется с использованием совокупности организационных мероприятий и средств физической защиты - систем инженерно-технических средств охраны объектов.

Физическая защита

Физическая защита объектов осуществляется с целью своевременного обнаружения фактов несанкционированного проникновения на охраняемую территорию, в выделенные помещения, а также для обеспечения сохранности средств информатизации.

Физическая защита охраняемых территорий, помещений и средств осуществляется путем реализации организационных мер (пропускной режим, дислокация) в сочетании с построением систем инженерно-технических средств охраны, предотвращающими проникновение в здания, выделенные помещения посторонних лиц, хищение документов и информационных носителей, самих средств информатизации и исключающими нахождение внутри контролируемой (охраняемой) зоны средств технической разведки.

Основными задачами физической защиты объектов являются:

- реализация организационных и инженерно-технических мер на объектах по построению и обеспечению функционирования систем охраны, с комплексным применением современных технических средств, видео наблюдения, сбора и обработки информации, обеспечивающих надежное обнаружение фактов несанкционированного проникновения в охраняемую зону, достоверное отображение и объективное документирование событий;
- ограничение несанкционированного доступа посторонних лиц в здания и помещения, где размещены средства вычислительной техники, на которых обрабатывается информация о персональных данных.

В целях обеспечения комплексной безопасности информации физической защите подлежат следующие объекты ИСПДн:

- помещения, в которых установлены компьютеры нотариуса, входящие в Единую информационную систему нотариата РФ (ЕИС РФ);
- помещения, в которых хранятся носители информации;
- коммуникации ИСПДн;
- системы электропитания (автономные источники электропитания).

Помещения ИСПДн должны размещаться в контролируемой зоне

4.9 защита информационной системы, ее средств, систем связи и передачи данных - меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных;

Меры по реализации межсетевого экранирования

Межсетевое экранирование предназначено для реализации следующих функций:

- фильтрации открытого и зашифрованного (закрытого) IP-трафика по заданным параметрам;
- 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 неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

4.10 выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них - меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в

информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

4.11 Меры криптографической защиты

Криптографическая защита предназначена для исключения НСД к защищаемой информации в ИСПДн нотариуса при ее передачи по каналам связи сетей общего пользования и (или) международного обмена.

Криптографическая защита предназначена для реализации функций криптографического преобразования данных, в том числе:

- генерация и распределение ключевой информации между элементами ИСПДн;
- управление ключевой информацией;
- шифрование/дешифрование информации;
- взаимодействие с подсистемами управления процессами обеспечения безопасности информации, контроля доступа к ресурсам и аудита.

Криптографическая защита может быть реализована модулем криптографической защиты.

Модуль криптографической защиты

Функциональное предназначение:

- шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, а также на съемные портативные носители данных (дискеты, usb - носители и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа;
- создание каналов связи, обеспечивающих защиту передаваемой информации;
- принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию.
- аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;
- обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;
- обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя;

5 ПОЛЬЗОВАТЕЛИ ИСПДн

В ИСПДн нотариуса Мурыгиной Олеси Семеновны можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратор ИСПДн;
- Администратор безопасности ИСПДн;
- Пользователь ИСПДн.

5.1. Администратор ИСПДн

Администратор ИСПДн – сотрудник нотариуса Мурыгиной Олеси Семеновны, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и осуществляет предоставление и разграничение доступа конечного пользователя (пользователя ИСПДн) к элементам, хранящим персональные данные.

Администратор ИСПДн обладает следующим уровнем доступ:

- 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.

5.2. Администратор безопасности ИСПДн

Администратор безопасности, ИСПДн – сотрудник нотариуса Мурыгиной Олеси Семеновны, ответственный за функционирование СЗИ ПДн, включая обслуживание и настройку административной ПО.

Администратор безопасности обладает следующим уровнем доступа:

- обладает правами Администратора ИСПДн;
- обладает полной информацией об ИСПДн;
- имеет доступ к средствам защиты информации;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать настройки межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИСПДн;

– осуществлять аудит средств защиты.

5.3. Пользователь ИСПДн

Пользователь ИСПДн нотариуса Мурыгиной Олеси Семеновны – работник, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование выходных документов по информации, полученной из ИСПДн Оператор не имеет полномочий для управления подсистемами обработки данных и СЗИ ПДн.

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 работники нотариуса Мурыгиной Олеси Семеновны, 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 работника нотариус обязан организовать его ознакомление с должностными инструкциями и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Работник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗИ ПДн.

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

Работники нотариуса Мурыгиной Олеси Семеновны, должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники 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.

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 при работе с информационными системами нотариуса Мурыгиной Олеси Семеновны третьим лицам.

При работе с ПДн в ИСПДн работники Мурыгиной Олеси Семеновны обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами информации с мониторов АРМ.

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

Работники Мурыгиной Олеси Семеновны 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, которые нарушили принятые политику и процедуры безопасности ПДн.

Работники 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, нотариусу и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

7 ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн.

8 ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ ИСПДн НОТАРИУСА

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).

При нарушениях работниками Мурыгиной Олеси Семеновны – 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 Положениях об обработке ПДн в ИСПДн и должностных инструкциях работников нотариуса Мурыгиной Олеси Семеновны.

ПРИЛОЖЕНИЕ 1

9 ПЕРЕЧЕНЬ НОРМАТИВНЫХ НОРМАТИВНО-ПРАВОВЫМИ И МЕТОДИЧЕСКИХ ДОКУМЕНТОВ, НА КОТОРЫХ БАЗИРУЕТСЯ НАСТОЯЩАЯ ПОЛИТИКА

9.1 Указ Президента Российской Федерации от 6 марта 1997 года № 188 «Об утверждении перечня сведений конфиденциального характера»;

9.2 Федеральный закон от 19 декабря 2005 г. № 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»;

9.3 Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

9.4 Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

9.5 «Требования к защите персональных данных при их обработке в информационных системах персональных данных», утверждены Постановлением Правительства Российской Федерации от 01 ноября 2013 года № 1119;

9.6 Постановление Правительства Российской Федерации от 15 сентября 2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

9.7 Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации по обеспечению безопасности ПДн при их обработке в ИСПДн:

9.8 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.;

9.9 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.;

9.10 Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», зарегистрирован в Минюсте России 14 мая 2013 г. № 28375.

9.11 Руководящий документ ГТК при Президенте РФ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от НСД к информации».

9.12 Руководящий документ ГТК при Президенте РФ «Средства вычислительной техники. Межсетевые Экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

9.13 Нормативно-методические документы Федеральной службы безопасности России:

9.14 Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации ФСБ (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/54–144);

9.15 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 их обработке в информационных системах персональных данных (утверждены руководством 8 Центра ФСБ России 21 февраля 2008 года № 149/6/6-622).

ПРИЛОЖЕНИЕ 2

10 СПИСОК ИСПОЛЬЗОВАННЫХ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

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

СВТ – средства вычислительной техники

СЗИ – средства защиты информации

СЗИ ПДн – система (подсистема) защиты персональных данных

СОВ – система обнаружения вторжений

ТКУ И – технические каналы утечки информации

УБПДн – угрозы безопасности персональных данных

ПРИЛОЖЕНИЕ 3

11 ТЕРМИНЫ И 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 сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

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.

Информационная система персональных данных (ИСПДн) – 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.

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 описанным 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 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;

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.

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, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать 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 на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу

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).