«Утверждаю»

Директор МБОУ Школы № 52 г.о. Самары

_____ И.Ю. Преина

Приказ № 192 от 01.09.16 года

ПОЛИТИКА

В ОТНОШЕНИИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ РАБОТНИКОВ УЧРЕЖДЕНИЯ МБОУ Школы № 52, А ТАК ЖЕ ОБУЧАЮЩИХСЯ И ИХ ЗАКОННЫХ ПРЕДСТАВИТЕЛЕЙ

Самара 2016

Введение

Настоящая Политика информационной безопасности (далее - Политика) Муниципального бюджетного общеобразовательного учреждения «Школы № 52 имени Ф.Ф. Селина» г. о. Самара (Далее – МБОУ Школа № 52 г.о. Самара)разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных МБОУ Школы № 52 г.о. Самара.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 12-ФЗ «О персональных данных», Постановления Правительства РФ от 11.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» на основании:

- «Положения о методах и способах защиты информации в информационных системах персональных данных», утверждённого приказом ФСТЭК России от 05.02.2010 г. № 58;
- «Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащих сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при обработке в информационных системах персональных данных», утверждённых руководством 8 Центра ФСБ РФ 21.02.2008 г. № 149/6/6-622.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищённости ИСПДн МБО Школы № 52 г. о. Самара.

1. Общие положения.

1. Целью настоящей Политики является обеспечение безопасности объектов защиты МБОУ Школы № 52 г. о. Самара от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн).

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

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

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

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

6. Состав ИСПДн подлежащих защите, представлен в Отчёте о результатах проведения внутренней проверки.

7. Эта Политика информационной безопасности была утверждена руководителем МБОУ Школы № 52 г.о. Самара Преиной Ириной Юрьевной и введена в действие приказом № 55 от 27.03.2013 г.

2. Область действия.

Требования настоящей Политики распространяются на всех сотрудников МБОУ Школы № 52 г. о. Самара (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:

- Отчёта о результатах проведения внутренней проверки;
- Перечня персональных данных, подлежащих защите;
- Акта классификаций информационной системы персональных данных;

- Модели угроз безопасности персональных данных;
- Положении о разграничении прав доступа к обрабатываемым персональным данным;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищённости ПДн каждой ИСПДн Муниципального бюджетного образовательного учреждения «Школы № 52 имени Ф.Ф. Селина» г. о. Самара. На основании анализа актуальных угроз безопасности ПДн описанного в Модели угроз и Отчёта о результатах проведения внутренней проверки, 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 каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- сервера приложений;
- граница ЛВС;

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

- антивирусные средств для рабочих станций, пользователей и серверов.
- средства криптографической защиты информации, при передачи защищаемой информации по каналам связи;

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учёт действий с информацией;
- обеспечение целостности данных;
- обнаружение 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 МБОУ Школы № 52 г. о. Самара или лицом, ответственным за обеспечение защиты ПДн.

4. Требования к подсистемам СЗПДн.

СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учёта;
- обеспечения целостности и доступности;
- антивирусной защиты;
- межсетевого экранирования;
- анализа защищённости;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определённого в Акте классификации информационной системы персональных данных.

4.1. Подсистемы управления доступом, регистрации и учёта.

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

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
- идентификации технических средств, узлов сети, каналов связи, внешних устройств по логическим именам;

- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам.

- контроль доступа пользователей к защищаемым ресурсам в соответствии с матрицей доступа;

- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и её установка;

- регистрация выдачи печатных (графических) материалов на бумажный носитель;

- регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки персональных данных;

- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

- регистрация 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 ос3уществляющие дополнительные меры по аутентификации и контролю.

4.2. Подсистема обеспечения целостности и доступности.

Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн МБОУ Школы № 52 г. о. Самара, а так же средств защиты, при случайной или намеренной модификации.

Подсистема обеспечения целостности и доступности предназначена для реализации следующих функций:

- резервное копирование обрабатываемых данных;

- обеспечение целостности программных средств защиты персональных данных, обрабатываемой информации, а так же неизменность программной среды;

- периодическое тестирование функций системы защиты персональных данных с помощью тест-программ, имитирующих попытки несанкционированного доступа;

- наличие средств восстановления системы защиты персональных данных.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, проверок при загрузки системы контрольных сумм компонентов средств защиты информации и их периодическим обновлением и контролем работоспособности, а так же резервированием ключевых элементов ИСПДн.

4.3. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты сервером и АРМ пользователей ИСПДн МБОУ Школы № 52 г.о. Самара.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- централизованную/удалённую установку/деинсталляцию антивирусного продукта, настройку, администрирование, просмотр отчётов 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 путём внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

4.4. Подсистема межсетевого экранирования.

Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрацию на сетевом уровне для каждого сетевого пакета независимо (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);

- фильтрацию пакетов служебных протоколов. служащих для диагностики и управления работой сетевых устройств;

- фильтрацию с учётом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

- фильтрацию с учётом любых значимых полей сетевых пакетов;

- фильтрацию на транспортном уровне запросов на установление виртуальных соединений с учётом транспортных адресов отправителя и получателя;

- фильтрацию на прикладном уровне запросов к прикладным сервисам с учётом прикладных адресов отправителя и получателя;

- фильтрацию с учётом даты и времени;

- аутентификацию входящих и исходящих запросов методами. устойчивыми к пассивному и (или) активному прослушиванию сети;

- регистрацию и учёт фильтруемых пакетов (в параметры регистрации включается адрес, время и результат фильтрации);

- регистрацию и учёт запросов на установление виртуальных соединений;

- локальную сигнализацию попыток нарушения правил фильтрации;

- идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и пеороля условно-постоянного действия;

- предотвращение доступа не идентифицированного пользователя, подлинность идентификации которого при аутентификации не подтвердилось;

- идентификацию и аутентификацию администратора межсетевого экрана при его удалённых запросах методами, устойчивыми к пассивному и активному перехвату информации;

- регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и её программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);

- регистрацию запуска программ и процессов (заданий, задач);

- регистрацию действия администратора межсетевого экрана п изменению правил фильтрации;

- возможность дистанционного управления своими компонентами, в том числе возможность конфигурации фильтров, проверки взаимной согласованности всех фильтров. анализа регистрационной информации;

- контроль целостности своей программной и информационной части;

- контроль целостности своей программной и информационной части межсетевого экрана по контрольным суммам;

- восстановление свойств межсетевого экрана после сбоев и отказа оборудования;

- регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации запросов, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

4.5. Подсистема анализа защищённости.

Подсистема анализа защищённости, должна обеспечивать выявления 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 анализа защищённости.

4.6. Подсистема обнаружение вторжений.

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

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

4.7. Подсистема криптографической защиты.

Подсистема криптографической защиты предназначена для исключения НСД к защищаемой информации в ИСПДн МБОУ Школы № 52 г. о. Самара, при её передачи по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путём внедрения криптографических программно-аппаратных комплексов.

5. Пользователи ИСПДн.

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

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

- Администратора ИСПДн;
- Администратора безопасности;
- Оператора АРМ;
- Администратора сети;
- Технического специалиста по обслуживанию периферийного обслуживания;
- Программист-разработчик иИСПДн.

Данные о группах пользователей, уровня их доступа и информированности должен быть отражён в Положении о разграничении прав доступа к обрабатываемым персональным данным.

В ИСПДн МБОУ Школы № 52 г. о. Самара можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

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

5.1. Администратор ИСПДн.

Администратор ИСПДн, сотрудник МБОУ Школы № 52 г. о. Самара, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять представление 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.

5.2. Администратор безопасности.

Администратор безопасности отвечает 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;

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

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;

- устанавливать доверительные отношения своей защищённой сети с сетями других операторов ИСПДн.

5.3. Оператор АРМ.

Оператор АРМ, сотрудник МБОУ Школы № 52 г. о. Самара, осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчётов по информации, полученной из ИСПДн. 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), обеспечивающим доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

5.4. Администратор сети.

Администратор сети отвечает за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

- знает, по меньшей мере, одно легальное имя доступа.

5.5. Технический специалист по обслуживанию периферийного оборудования.

Технический специалист по обслуживанию, сотрудник МБОУ Школы № 52 г. о. Самара, осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий для управления подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает часть информации о технических средствах и конфигурации ИСПДн;

- знает, по меньшей мере, одно легальное имя доступа.

5.6. Программист-разработчик ИСПДн.

Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники МБОУ Школы № 52 г. о. Самара, так и сотрудники организаций.

Лицо этой категории:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, не декларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии её разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

6. Требования к персоналу по обеспечению защиты ПДн.

Все сотрудники МБОУ Школы № 52 г. о. Самара, являющиеся пользователями ИСПДн, должны чётко 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. регламентирующие требования по защите ПДн, а так же 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 МБОУ Школы № 52 г. о. Самара, 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 МБОУ колы № 52 г. о. Самара должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использование паролей (не используются технические средства аутентификации).

Сотрудники МБОУ Школы № 52 г. о. Самара должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещении имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности ПДн и процедуры защиты оборудования, оставленного без присмотра. а так же 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 (краткое наименование оператора), третьим лицам.

При работе с ПДн в ИСПДн сотрудники Учреждения обязаны обеспечить отсутствия 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 МБОУ Школы № 52 г. о. Самара должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утверждённой формальной процедурой наложений дисциплинарных взысканий на сотрудников, которые нарушили принятые Политику и процедуры безопасности ПДн.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых и подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а так же о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения 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;
- Инструкция пользователя при возникновении внештатных ситуаций.

8. Ответственность сотрудников ИСПДн МБОУ колы № 52 г. о. Самара.

В соответствии со ст.24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований настоящего 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, совершённые от имени их учётных записей или системных учётных записей, если не доказан факт несанкционированного использования учётных записей.

При нарушениях сотрудниками МБОУ Школы № 52 г. о. Самара – пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

9. Список использованных источников.

Основными нормативнбо-правовыми и методическими документами, на которых базируется настоящее Положение, являются:

- Федеральный Закон от 27.07. 2006 г № 152 ФЗ «О персональных данных» устанавливающий основные принципы и условия обработки ПДн, права, обязанность и ответственность участников отношений, связанных с обработкой ПДн;
- «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённое Постановлением Правительства РФ от 17.11.2007 г. № 781;
- «Порядок проведения классификации информационных систем персональных данных», утверждённый совместным Приказом ФСТЭК России № 55, ФСБ России № 86 и Мининформсвязи РФ № 20 от 13.02.2008 г.;
- «Положение об особенностях обработки персональных данных. осуществляемой без использования средств автоматизации», утверждённое Постановлением Правительства РФ от 15.09.2008 г. № 687;
- «Требования к материальным носителям биометрических персональных данных и технология хранения таких данных вне информационных систем персональных данных», утверждённые Постановлением Правительства РФ от 06.07.2008 г. № 512;

Нормативно-методические документы Федеральной службы по техническому и экспертному контролю Российской Федерации (далее ФСТЭК России) по обеспечению безопасности ПДн при их обработке в ИСПДн:

- Базовая модель угроз безопасности персональных данных при их обработки в информационных системах персональных данных, утв. зам директора ФСТЭК России 15.02.08 г. (ДСП)
- Методика проведения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г. (ДСП)
- «Положение о методах и способах защиты информации в информационных системах персональных данных», утверждённое директором ФСТЭК от 05.02.2010 г. № 58

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

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.

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.

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 – электрический сигнал, 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.

Не декларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующими 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 – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование и 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, организующее и / или осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

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

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес,

семейное, социальное, имущественное положение, образование, профессия, доходы и другая информация.

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 записи ключей и атрибутов доступа (паролей) на бумажные носители 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, 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 передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

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

Специальные категории персональных данных – персональные данные, касающиеся расовой и 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.

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.

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 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.

Учреждение – государственное образовательное учреждение.

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
АИС - автоматизированная информационная система
АРМ - автоматизированное рабочее место
ИНН - индивидуальный номер налогоплательщика
ИСПДн - информационная система персональных данных
ЛВС - локальная вычислительная сеть
ЛИС - локальная информационная система
МЭ - межсетевой экран
НСД - несанкционированный доступ
ОС - операционная система
ПДн - персональные данные
ПМВ - программно-математическое воздействие
ПО - программное обеспечение
ПФ - пенсионный фонд
ПЭМИН - побочные электромагнитные излучения и наводки
РИС - распределенная информационная система
СЗИ - средства защиты информации
СЗПДн - система (подсистема) защиты персональных данных
ТКУИ - технические каналы утечки информации
УБПДн - угрозы безопасности персональных данных
ФСТЭК России - Федеральная служба по техническому и экспортному контролю – федеральный орган исполнительной власти России, осуществляющим реализацию государственной политики, организацию межведомственной координации и взаимодействия, специальные и контрольные функции в области государственной безопасности.

Содержание