|  |
| --- |
| Общество с ограниченной ответственностью "Файт" |
| (Полное наименование оператора) |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **"УТВЕРЖДЕНО"** |  |  |  |  |
|  | Генеральный директор |  |  |  | Насибян Р.А. |
|  | (должность) |  | (личная подпись) |  | (расшифровка подписи) |
|  | № 01 от 01.09.2017г. |  |  |  |  |

## ПОЛИТИКА

## информационной безопасности оператора ИСПДн

### Введение

Настоящая Политика информационной безопасности (далее — Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ИСПД оператора Общество с ограниченной ответственностью "Файт".

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ "О персональных данных" и Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных" и на основании:

- Приказа ФСТЭК России от 18.02.2013 № 21 зарегистрирован в Минюсте России 14.05.2013 № 28375

"Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"

.

В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн оператора.

### Общие положения

* 1. Целью настоящей Политики является обеспечение безопасности объектов защиты оператора информационной системы от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн) информационной системы.
  2. 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.
  3. Информация и связанные с ней ресурсы должны быть доступны для авторизованных 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.

### Область действия

* 1. Требования настоящей Политики распространяются на всех сотрудников оператора (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

### Система защиты персональных данных

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

- Отчета о результатах проведения внутренней проверки;

- Перечня персональных данных, подлежащих защите;

- Положения о разграничении прав доступа к обрабатываемым персональным данным.

* 1. На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн оператора.
  2. 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;

- СУБД;

- Граница ЛВС;

- Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

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

- антивирусные средства для рабочих станций пользователей и серверов.

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

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечивать целостность данных;

- производить обнаружений вторжений.

* 1. 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 Учреждения или лицом, ответственным за обеспечение защиты ПДн.

### Требования к подсистемам СЗПДн

* 1. СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;

- обеспечения целостности и доступности;

- антивирусной защиты;

- анализа защищенности;

- обнаружения вторжений.

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

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;

- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;

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

- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.

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

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

* 1. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений и СУБД). Так же может быть внедрено специальное техническое средство или их комплекс осуществляющие дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.
  2. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн предприятия, а так же средств защиты, при случайной или намеренной модификации.
  3. Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а так же резервированием ключевых элементов ИСПДн.
  4. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн оператора.
  5. 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.

* 1. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.
  2. Подсистема анализа защищенности, должна обеспечивать выявления уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.
  3. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.
  4. Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена.
  5. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

### Пользователи ИСПДн

* 1. В Концепции информационной безопасности определены основные категории пользователей. На основании этих категории должна быть произведена типизация пользователей ИСПДн, определен их уровень доступа и возможности.
  2. В ИСПДн оператора можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;

- Технического специалиста по обслуживанию периферийного оборудования;

- Программист-разработчик ИСПДн.

* 1. Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положение о разграничении прав доступа к обрабатываемым персональным данным.
  2. Администратор ИСПДн, сотрудник оператора, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные.
  3. 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;

- осуществляет обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД.

* 1. Технический специалист по обслуживанию, сотрудник оператора, 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.
  2. Технический специалист по обслуживанию 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;

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

* 1. Программисты-разработчики (поставщики) прикладного программного обеспечения, обеспечивающие его сопровождение на защищаемом объекте. К данной группе могут относиться как сотрудники оператора, так и сотрудники сторонних организаций.
  2. Лицо этой категории:

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

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

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

### Требования к персоналу по обеспечению защиты ПДн

* 1. Все сотрудники оператора, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.
  2. При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.
  3. Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.
  4. Сотрудники оператора, 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.
  5. Сотрудники оператора должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).
  6. Сотрудники оператора 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.
  7. Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а так же записывать на них защищаемую информацию.
  8. Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами оператора, третьим лицам.
  9. При работе с ПДн в ИСПДн сотрудники оператора обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов.
  10. 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.
  11. Сотрудники оператора должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн.
  12. Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности ПДн.

### Ответственность сотрудников ИСПДн оператора

* 1. 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 (ст.ст. 272 - 274 Уголовного кодекса РФ).
  2. Администратор ИСПДн несет ответственность за все действия, совершенные от имени его учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.
  3. При нарушениях сотрудниками оператора - пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.
  4. Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников оператора.