|  |
| --- |
| **УТВЕРЖДАЮ**  Генеральный директор  ООО «ВЛАДЕЛЕЦ ИСПДН» |
| \_\_\_\_\_\_\_\_\_\_\_\_  М.П. |
|  |

**инструкция администратора информационной безопасности** **ИСПДн «ВЛАДЕЛЕЦ ИСПДН»**

**ООО «ВЛАДЕЛЕЦ ИСПДН»**

**1. Общие положения**

1.1. Администратор информационной безопасности назначается приказом Генерального директора ООО «ВЛАДЕЛЕЦ ИСПДН» (далее - Общества) и отвечает за обеспечение устойчивой работоспособности и информационной безопасности информационной системы персональных данных «ВЛАДЕЛЕЦ ИСПДН» (далее - ИСПДн).

1.2. Администратор информационной безопасности несет ответственность за организацию работ по обеспечению безопасности информации, обрабатываемой, передаваемой и хранимой при помощи средств вычислительной техники (далее - СВТ) в информационной системе персональных данных, а также правильность использования и нормального функционирования средств защиты информации, подготовку сотрудников по вопросам безопасной обработки информации на СВТ.

1.3. Система защиты персональных данных (далее - СЗПДн) в ИСПДн от несанкционированного доступа (НСД) построена на основе функционирования программно-аппаратного комплекса и организационно-технических мер защиты информации.

1.4. Парольная защита объекта информатизации является составной частью подсистемы управления доступом общей системы защиты от НСД. При организации парольной защиты необходимо руководствоваться требованиями соответствующих пунктов настоящей инструкции.

1.5. Администратор информационной безопасности в своей работе руководствуется положениями федеральных законов, руководящими и нормативными документами ФСТЭК России и регламентирующими документами на данном объекте информатизации Общества.

**2. Функции администратора информационной безопасности**

2.1. Администратор информационной безопасности осуществляет контроль за целевым использованием информационной системы персональных данных, а также всех ее внешних устройств.

2.2. Администратор информационной безопасности осуществляет настройку и сопровождение подсистемы управления доступом, при этом:

- реализует полномочия доступа пользователя к элементам защищаемых информационных ресурсов ИСПДн на основе утвержденной разрешительной системы доступа;

- проводит периодическую проверку работоспособности системы защиты от НСД, а также при изменении программной среды и полномочий пользователей ИСПДн;

- один раз в три месяца, а также в случае необходимости (компрометация пароля) производит смену паролей доступа в систему. Периодически, по указанию руководителя организации уточняет список прав доступа и полномочия сотрудников по доступу к средствам вычислительной техники, которые используются для обработки конфиденциальных сведений.

2.3. Проводит периодический контроль принятых мер по защите.

**3. Администратор информационной безопасности обязан:**

3.1. Обеспечивать функционирование и поддерживать работоспособность средств защиты информационной системы персональных данных, в пределах возложенных на него функций.

3.2. В случае отказа работоспособности технических средств и программного обеспечения СВТ ИСПДн Общества, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

3.3. Информировать ответственного за защиту информации о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам ИСПДн Общества.

3.4. Знать состав технических средств и программных ресурсов ИСПДн, предназначенных для обработки информации, и перечень задач (прикладных программ), решаемых с их использованием.

3.5. В случае выявления каких-либо несанкционированных действий пользователя, несущих в себе угрозу для безопасности информации, поставить в известность об этом ответственного за защиту информации, временно заблокировать возможность работы пользователя в ИСПДн и принять меры по исключению таких действий.

3.6. Не реже 1 раза в неделю выполнять работу по администрированию информационной безопасности ИСПДн, проверять данные в системном журнале на предмет несанкционированных действий и в случае необходимости распечатывать системные журналы СЗИ. В случае выявления попыток НСД к защищаемой информации представлять данный журнал ответственному по защите информации.

3.7. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических средств ИСПДн и отправке их в ремонт. При проведении технического обслуживания и ремонта запрещается передавать ремонтным организациям узлы и блоки с элементами накопления и хранения конфиденциальной информации (в том числе диски корпоративной системы хранения данных (СХД)). Вышедшие из строя элементы и блоки средств вычислительной техники заменяются на элементы и блоки, прошедшие специальные исследования и специальную проверку.

3.8. Присутствовать (участвовать) в работах по внесению изменений в аппаратно-программную конфигурацию ИСПДн.

3.9. Контролировать соответствие состава ИСПДн техническому паспорту на ИСПДн (в т.ч. реальной конфигурации информационных связей).

3.10. Хранить, осуществлять прием и выдачу персональных идентификаторов и аутентификаторов пользователей, осуществлять контроль за правильностью использования персонального идентификатора и аутентификатора пользователем ИСПДн.

3.11. Проводить работу по выявлению возможных каналов вмешательства в процесс функционирования ИСПДн и осуществления НСД к информации и техническим средствам ИСПДн. При выявлении таких каналов сообщать о них ответственному за защиту информации и принимать меры по исключению вмешательства в работу ИСПДн.

3.12. Не реже одного раза в год проводить тестирование всех функций СЗИ от НСД с помощью специальных программных средств.

**4. Администратор информационной безопасности имеет право:**

4.1. Контролировать работу пользователей в ИСПДн в части использования ими средств защиты информации.

4.2. Требовать прекращения обработки информации как в целом, так и для отдельных пользователей в случае выявления нарушений установленного порядка работ или нарушения функционирования ИСПДн.

**5. Организация парольной защиты при работе на объекте информатизации**

5.1 Личные пароли доступа пользователей (администратора информационной безопасности) к объекту информатизации, системе защиты от НСД, выбираются Администратором информационной безопасности (пользователем) при соблюдении следующих требований:

- длина пароля должна быть не менее 6-ти буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования ИСПДн, общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP, GUEST, ADMINISTRATOR и т.д.), и другие данные, которые могут быть подобраны злоумышленником путем анализа информации об ответственном исполнителе;

- не использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

- не использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- не использовать ранее использованные пароли.

5.2. Лица, использующие паролирование, обязаны:

- четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

- своевременно сообщать Администратору информационной безопасности обо всех нештатных ситуациях, нарушениях работы подсистем защиты от НСД, возникающих при работе с паролями.

5.3. При организации парольной защиты запрещается:

- записывать свои пароли в очевидных местах, внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.;

- хранить пароли в записанном виде на отдельных листах бумаги;

- хранить персональные идентификаторы в общедоступных местах;

- сообщать посторонним лицам свои пароли, а также сведения о применяемой системе защиты от НСД.