ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат:
61E9FE1E4B1E14DE0C45FE3D8935AF36
Владелец: Апрасидзе Лейла Георгиевна
Действителен: с 15.02.2023 до 10.05.2024

УТВЕРЖДАЮ
Директор МБОУ
г. Мурманска СОШ № 20
_____Л.Г. Апрасидзе
от 01.09.2023

ДОЛЖНОСТНАЯ ИНСТРУКЦИЯ АДМИНИСТРАТОРА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие положения.

1.1. Данная Инструкция определяет основные обязанности и права администратора безопасности информационных систем персональных данных (далее – ИСПДн) муниципального бюджетного общеобразовательного учреждения г. Мурманска «Средняя общеобразовательная школа № 20» (далее – Учреждение).

1.2. Администратор безопасности ИСПДн является штатным сотрудником Учреждения.

1.3. Администратор безопасности ИСПДн назначается приказом директора Учреждения.

1.4. Решение вопросов обеспечения информационной безопасности входит в прямые служебные обязанности администратора безопасности ИСПДн.

1.5. Администратор безопасности ИСПДн обладает правами доступа к любым программным и аппаратным ресурсам ИСПДн.

1.6. Администратор безопасности должен иметь специальное рабочее место – рабочую станцию (РС), размещенную в отдельном помещении и функционирующую постоянно при включении сети.

2. Должностные обязанности

2.1. Администратор безопасности ИСПДн обязан:

2.1.1. Знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций, руководства по защите информации и распоряжений, регламентирующих порядок действий по защите информации.

2.1.2. Знать перечень установленных в подразделениях Учреждения автоматизированных рабочих мест (далее – АРМ) и перечень задач, решаемых с их использованием.

2.1.3. Обеспечивать установку, настройку и своевременное обновление элементов ИСПДн:

- программного обеспечения АРМ и серверов (операционные системы, прикладное и специальное ПО);
- аппаратных средств;
- аппаратных и программных средств защиты.

2.1.4. Обеспечивать функционирование и поддерживать работоспособность элементов ИСПДн, в том числе средств защиты информации, и локальной вычислительной сети.

2.1.5. Информировать ответственного за обеспечение защиты персональных данных о фактах нарушения установленного порядка работ и попытках несанкционированного доступа к информационным ресурсам.

2.1.19. Участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате НСД.

2.1.20. Участвовать в работе комиссий по пересмотру планов защиты.

3. Порядок работы с ресурсами ИСПДн

3.1. Перечень работ, производимых администратором безопасности ИСПДн.

3.1.1. Проверка работоспособности и настройка системы доступа к ресурсам ИСПДн.

3.1.1.1. Администратор безопасности ИСПДн разрабатывает правила парольной защиты и контролирует их соблюдение.

3.1.1.2. Администратор безопасности ИСПДн сообщает пользователю его уникальное имя и предоставляет возможность задать пароль, кодирует аппаратный идентификатор пользователя (при наличии).

3.1.1.3. Администратор безопасности ИСПДн производит изменения учетных данных пользователя по требованию руководителя подразделения, при согласовании с ответственным за обеспечение безопасности персональных данных, а также периодически по утвержденному плану и в случае увольнения сотрудника.

3.1.1.4. Администратор безопасности ИСПДн имеет право в целях тестирования уязвимости системы доступа (выявление простейших паролей) производить попытки взлома паролей пользователей, в случае успешного взлома, администратор безопасности ИСПДн обязан потребовать у пользователя изменения пароля.

3.1.2. Проверка работоспособности и настройка аппаратных и программных средств защиты информации.

3.1.2.1. Администратор безопасности ИСПДн обязан перед началом работ включить и убедиться в работоспособности аппаратных СЗИ, в случае сбоя – прекратить работы.

3.1.2.2. В случае сбоя программных СЗИ, таких, как неправильная идентификация и аутентификация пользователей, администратор безопасности ИСПДн обязан прекратить работы, в случае производственной необходимости продолжения работ – отключить программное обеспечение (далее - ПО) СЗИ и лично контролировать проведение работ пользователем.

3.1.3. Антивирусная защита ресурсов ИСПДн.

3.1.3.1. Администратор безопасности ИСПДн в соответствии с инструкцией по организации антивирусной защиты разрабатывает и контролирует реализацию антивирусной политики, а именно:

- настраивает параметры антивирусной программы;
- контролирует работоспособность антивирусной программы;
- немедленно реагирует на сообщения пользователей о подозрительном поведении ПО, а также о появлении любых сообщений антивирусной программы;
- имеет право на проведение внеплановой проверки на присутствие вирусов;
- периодически обновляет антивирусные базы данных, а также исполняемые модули антивирусной программы.

3.1.4. Хранение дистрибутивов программного обеспечения СЗИ.

3.1.4.1. Администратор безопасности ИСПДн должен хранить дистрибутивы ПО СЗИ, установленных на АРМ ИСПДн, в месте, исключающем доступ посторонних лиц.

3.1.5. Проверка целостности системного и прикладного ПО.

3.1.5.1. Администратор безопасности ИСПДн должен периодически (не реже одного раза в квартал) производить проверку целостности системного и прикладного программного обеспечения с использованием специальных режимов работы СЗИ от НСД.

3.1.6. Резервное копирование и восстановление информации.

3.1.6.1. В соответствии с утвержденным регламентом, а также по требованию пользователей, администратор безопасности ИСПДн проводит резервное копирование и восстановление пользовательской информации. При этом необходимо выполнять следующие требования:

- иметь в наличии регламент резервного копирования и перечень резервируемой информации, утверждаемых приказом директора Учреждения;
- вне графика производить обязательное резервное копирование в случае обнаружения неисправностей в работе АРМ или отчуждаемых носителей;
- допускается обоснованное внеплановое резервное копирование информации по инициативе администратора безопасности ИСПДн, если это не нарушает технологию обработки информации;
- резервные копии хранятся на отдельных носителях в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение (ответственным за хранение является администратор безопасности ИСПДн);
- при устранении неисправностей АРМ администратор безопасности ИСПДн производит восстановление важной информации с резервных копий.

3.1.7. Вывод ресурсов ИС из эксплуатации.

3.1.7.1. При невозможности ремонта технических средств ИСПДн администратор безопасности ИСПДн обязан:

- физически уничтожать любые носители, независимо от содержащейся на них информации, отразить факт уничтожения носителя в «Журнале учета съемных носителей персональных данных».

4. Действия при обнаружении попыток несанкционированного доступа

4.1. К попыткам несанкционированного доступа относятся:

4.1.1. Сеансы работы с ИСПДн незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят реализуемые в процессе сеанса работы операции.

4.1.2. Действия третьего лица, пытающегося получить доступ (или получившего доступ) к ИСПДн, при использовании учетной записи администратора или другого пользователя ИСПДн, в целях получения коммерческой или другой личной выгоды, методом подбора пароля или другого метода (случайного разглашения пароля и т.п.) без ведома владельца учетной записи.

4.2. При выявлении факта НСД администратор безопасности ИСПДн обязан:

4.2.1. Прекратить доступ к ИСПДн со стороны выявленного участка НСД;

4.2.2. Доложить директору Учреждения служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;

4.2.3. Известить ответственного за обеспечение безопасности персональных данных и руководителя подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;

4.2.4. Проанализировать характер НСД, по результатам анализа составить письменный отчет и предоставить его директору Учреждения.

5. Права

5.1. Администратор безопасности ИСПДн имеет право:

5.1.1. Требовать от пользователей информационных ресурсов
выполнения инструкций пользователя ИСПДн;

5.1.2. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИСПДн;

5.1.3. Вносить свои предложения по совершенствованию мер защиты в ИСПДн.

6. Ответственность

6.1. Администратор безопасности ИСПДн несет ответственность за соблюдение требований настоящей инструкции, а также других нормативных документов в области защиты информации.

6.2. Администратор безопасности ИСПДн несет ответственность за программно-аппаратные, инженерно-технические и криптографические средства защиты информации, средства вычислительной техники, информационно - вычислительные комплексы, сети и информационные системы обработки информации, закрепленные за ним приказом директора Учреждения и за качество проводимых им работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

6.3. Администратор безопасности ИСПДн несет ответственность по действующему законодательству за разглашение информации, составляющей персональные данные, ставшие известными ему по роду работы.

6.4. Администратор безопасности ИСПДН несет ответственность за все действия, совершенные от имени его учетной записи или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

_____