Согласовано на заседании профсоюзного комитета МБОУ СОШ № 11 г.Брянска протокол № 54 от 25 октября 2021г.

Председатель ППО _____

Л.Е.Угарова

УТВЕРЖДАЮ:

Директор МБОУ СОШ № 11 г.Брянска

_____

А.Н.Семигулин

Приказ № 464 В от 25 октября 2021г.

Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа № 11 имени П.М. Камозина» г.Брянска

Инструкция
администратору безопасности персональных данных

1. Общие положения:

Настоящая Инструкция определяет задачи, функции, обязанности, права и ответственность администратора безопасности персональных данных (далее-администратора безопасности) по вопросам обеспечения безопасности персональных данных при их обработке в ИСПДн.

Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам обеспечения безопасности персональных данных и не исключает обязательного выполнения их требований.

2. Задачи администратора безопасности:

Основными задачами администратора безопасности являются:

- организация эксплуатации технических и программных средств защиты персональных данных в соответствии с установленными требованиями по защите информации;
- текущий контроль работы средств и систем защиты персональных данных;
- контроль за работой пользователей ИСПДн, выявление и регистрация попыток несанкционированного доступа к персональным данным.

3. Функции администратора безопасности:

3.1. Контроль за выполнением требований действующих нормативных документов по вопросам обеспечения безопасности персональных данных при их обработке в ИСПДн.

3.2. Настройка и сопровождение в процессе эксплуатации подсистемы управления доступом на ПЭВМ:

- реализация полномочий доступа (чтение, запись) для каждого пользователя к элементам защищаемых информационных ресурсов (файлам, каталогам, принтеру и т.д.);
- ввод описаний пользователей ИСПДн в информационную базу установленной на ПЭВМ СЗИ НСД;
- своевременное удаление описаний пользователей из базы данных СЗИ от НСД при изменении списка допущенных к работе в ИСПДн лиц;
- контроль доступа лиц в помещение, где установлены ПЭВМ, в соответствии со списком сотрудников, допущенных к работе в ИСПДн;
-контроль за проведением смены паролей для доступа к ПЭВМ пользователями ИСПДн *(в соответствии с требованиями Инструкции по организации парольной защиты).*

3.3. Настройка и сопровождение подсистемы регистрации и учета действий пользователей при работе в ИСПДн:

- введение в базу данных установленной на ПЭВМ СЗИ от НСД описания событий,

подлежащих регистрации в системном журнале;

- регулярное проведение анализа системного журнала для выявления попыток несанкционированного доступа к защищаемым ресурсам;

- своевременное информирование ответственного за обеспечение безопасности ПДн о несанкционированных действиях персонала и проведение расследования попыток НСД;

- организация печати файлов пользователей на принтере и осуществление контроля за соблюдением установленных правил и параметров регистрации и учета бумажных носителей информации.

3.4. Сопровождение подсистемы обеспечения целостности информации в ИСПДн:

- периодическое тестирование функций установленной на ПЭВМ СЗИ от НСД, особенно при изменении программной среды и полномочий исполнителей;

- восстановление программной среды, программных средств и настроек СЗИ от НСД при сбоях;

- ведение двух копий программных средств СЗИ от НСД и контроль их работоспособности;

- контроль за отсутствием на магнитных носителях остаточной информации по окончании работы пользователей;

3.4. Сопровождение подсистемы антивирусной защиты ИСПДн:

- поддержание установленного порядка и правил антивирусной защиты информации на ПЭВМ;

- периодическое обновление антивирусных средств (баз данных), установленных на ПЭВМ;

- контроль за соблюдением пользователями порядка и правил проведения антивирусного тестирования ПЭВМ.

3.5. Контроль соблюдения требований по размещению и использованию технических средств, указанных в Техническом паспорте ИСПДн.

4. Обязанности администратора безопасности:

Администратор безопасности обязан:

Обеспечивать функционирование и поддерживать работоспособность средств и систем защиты персональных данных в пределах возложенных на него обязанностей в соответствии с требованиями руководящих и нормативно-методических документов по защите информации.

Докладывать о выявленных нарушениях и НСД пользователей ИСПДн и обслуживающего персонала к персональным данным, принимать необходимые меры по устранению выявленных нарушений.

Совместно со специалистами органа по аттестации принимать меры по восстановлению работоспособности СЗИ НСД.

Проводить инструктаж пользователей ИСПДн и обслуживающего персонала ИСПДн по правилам работы с используемыми средствами и системами защиты персональных данных.

Знать состав пользователей ИСПДн и их производственную деятельность (выполняемые операции, права, привилегии).

Знать порядок и технологию включения и удаления пользователей в СЗИ НСД.

Назначать и отменять права и привилегии пользователям ИСПДн по доступу в систему, к объектам доступа и программным средствам в соответствии с Матрицей доступа, а также требованиями руководящих и нормативно-методических документов по защите персональных данных.

Знать порядок и контролировать процесс учета, хранения и обращения носителей персональных данных в ИСПДн в соответствии с требованиями организационно-распорядительных документов.

Знать порядок гарантированного уничтожения персональных данных средствами

СЗИ НСД.

5. Права администратора безопасности:

Администратор безопасности имеет право:

Контролировать работу пользователей ИСПДн на ПЭВМ.

Требовать от пользователей и обслуживающего персонала ИСПДн соблюдения установленных правил обработки персональных данных и выполнения требований руководящих и нормативно-методических документов по защите информации.

Требовать прекращения обработки персональных данных, как в целом, так и отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования ПЭВМ, средств и систем защиты информации.

Обращаться к руководителю требованием о прекращении доступа пользователя к работам в ИСПДн в случае грубых нарушений требований руководящих и нормативно-методических документов по защите персональных данных, порядка и правил обработки информации или нарушения функционирования средств и систем защиты информации.

Требовать объяснительных документов и назначения служебного расследования в отношении пользователя и обслуживающего персонала ИСПДн по фактам нарушения безопасности информации и НСД к персональным данным.

6. Ответственность администратора безопасности:

Администратор безопасности несет ответственность за организацию работ по обеспечению безопасности персональных данных, обрабатываемых, передаваемых и хранимых при помощи средств ИСПДн, а также правильность использования и нормального функционирования средств защиты информации, подготовку сотрудников по вопросам безопасной обработки персональных данных в ИСПДн.

7. Сокращения:

ИСПДн – информационная система персональных данных;
НСД – несанкционированный доступ;
ПДн – персональные данные;
ПЭВМ – персональная электронно-вычислительная машина;
СЗИ – средства защиты информации;

С инструкцией ознакомлен/а: _____