

**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ «СРЕДНЯЯ ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА № 2»
МУНИЦИПАЛЬНЫЙ ОБРАЗОВАТЕЛЬНЫЙ ОКРУГ СИМФЕРОПОЛЬ
РЕСПУБЛИКИ КРЫМ**

Принято на заседании
педагогического совета
Протокол № 12
От 30.08.2018 г.

УТВЕРЖДЕНО
Директор МБОУ «Средняя
общеобразовательная школа № 2»
В.А. Кухнина
Приказ № 429 от 31.08. 2018 г.
«Об утверждении организационно-
распорядительной документации по обработке
персональных данных в МБОУ «СОШ № 2» г.
Симферополя»

**ИНСТРУКЦИЯ
администратора безопасности информации
в МБОУ «СОШ №2» г. Симферополя**

1. Общие положения

Данная Инструкция является руководящим документом администратора безопасности информации в МБОУ «СОШ №2».

Требования настоящей инструкции должны выполняться во всех режимах функционирования.

Требования администратора безопасности, связанные с выполнением им своих функций, обязательны для исполнения всеми работниками.

Персональные данные относятся к категории информации ограниченного распространения.

Наиболее вероятными каналами утечки информации для информационных систем персональных данных (далее – ИСПДн) являются:

- несанкционированный доступ к информации, обрабатываемой в ИСПДн;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;
- просмотр информации с экранов дисплеев мониторов и других средств ее отображения с помощью оптических устройств;

- воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности обмена, в том числе электромагнитного, через специально внедренные электронные и программные средства («закладки»).

Работа с персональными данными (далее - ПДн) строится на следующих принципах:

- принцип персональной ответственности — в любой момент времени за каждый документ (не зависимо от типа носителя: бумажный, электронный) должен отвечать и распоряжаться конкретный работник, выдача документов осуществляется только под роспись;

- принцип контроля и учета — все операции с документами должны отражаться в соответствующих журналах и карточках (передача из рук в руки, снятие копии и т.п.).

2. Назначение администратора безопасности информации

На должность администратора безопасности назначается работник из числа наиболее квалифицированных пользователей автоматизированных рабочих мест (далее — АРМ), либо имеющим образование в области защиты информации, в котором эксплуатируется информационная система.

3. Обязанности администратора информационной безопасности

В своей повседневной деятельности администратор руководствуется данной инструкцией и другими документами, регламентирующими защиту персональных данных.

Администратор информационной безопасности:

- обеспечивает поддержку подсистем управления доступом, регистрации и учета информационных ресурсов;

- контролирует целостность программно-аппаратной среды, хранимой и обрабатываемой информации;

- контролирует доступность и конфиденциальность хранимой, обрабатываемой и передаваемой по каналам связи информации.

На администратора информационной безопасности возлагаются следующие обязанности:

- произвести опломбирование наклейками корпусов АРМ, где обрабатываются персональные данные;

- следить за сохранностью наклеек с защитной и идентификационной информацией на корпусах АРМ;

- знать уровень конфиденциальности обрабатываемой информации и класс ИСПДн, следить за тем, чтобы обработка информации производилась

только с использованием учтенных съемных и несъемных носителей информации;

- контролировать соблюдение требований по учету и хранению носителей конфиденциальной информации и персональных данных;
- обеспечивать доступ к защищаемой информации пользователям согласно их прав доступа;
- незамедлительно докладывать директору, обо всех выявленных попытках несанкционированного доступа к информации ограниченного доступа;
- контролировать правильность применения пользователями сети средств защиты информации;
- участвовать в испытаниях и проверках ИСПДн;
- не допускать к работе на рабочих станциях и серверах посторонних лиц;
- осуществлять контроль монтажа оборудования специалистами сторонних организаций;
- участвовать в приемке для нужд новых программных средств;
- обобщать результаты своей деятельности и готовить предложения по ее совершенствованию.

При выявлении нарушений администратор обязан немедленно прекратить работы в ИСПДн и подать служебную записку директору.

4. Ответственность

Администратор безопасности несет всю полноту ответственности за качество и своевременность выполнения задач и функций, возложенных на его в соответствии с настоящей Инструкцией и другими нормативными документами по защите информации.

С инструкцией ознакомлены:

Специалист по обслуживанию
компьютерных систем и оргтехники

Шкарбан З.В.

Зам. директора по АХЧ

Шабалина И.А.

Пронумеровано, прошито и скреплено печатью

Эксперт

Директор МБОУ «СОШ №2»
Г. Симферополя

В. А. Кухнина

В. А. Кухнина

