

**Муниципальное бюджетное общеобразовательное учреждение
«Средняя общеобразовательная школа №2
имени Сви́дерского Алекса́ндра Григо́рьевича»
города Бахчисарай Республики Крым**

СОГЛАСОВАНО:

Председатель проф. комитета
Е.Н. Чернышева
05.08.2024 г.

УТВЕРЖДАЮ:

Директор школы
Т.П. Линик
08.08.2024 г.

**Инструкция № АТ-14-2024
по информационной безопасности**

1. Общие положения.

1. Основная цель обеспечения информационной безопасности - предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации в компьютерных системах МБОУ «СОШ №2 им. Сви́дерского А.Г.».
2. Работники МБОУ «СОШ №2 им. Сви́дерского А.Г.» обязаны:
 - 2.1. Знать и соблюдать требования настоящей Инструкции и других документов по информационной безопасности при работе с ПК, имеющими доступ к информационным ресурсам локальной сети МБОУ «СОШ №2 им. Сви́дерского А.Г.» и сети «Интернет»;
 - 2.2. Знать и уметь правильно использовать то аппаратно - программное обеспечение, которое установлено на его ПК, а также строго выполнять правила работы со средствами защиты информации, установленными на них;
 - 2.3. Хранить в тайне свой пароль (пароли);
 - 2.4. Выполнять следующие требования по антивирусному контролю:
 - а) Антивирусный контроль всех дисков и файлов ПК должен проводиться ежедневно в начале работы при их загрузке в автоматическом режиме;
 - б) Обновление антивирусных баз должно проводиться в соответствии с периодичностью, указанной в руководствах по применению конкретных антивирусных средств.
 - в) В процессе работы обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съемных носителях (flesh-дисках, CD-, DVD- и т.п.). Разархивирование и контроль входящей информации должен проводиться непосредственно после ее приема. Контроль исходящей информации должен проводиться непосредственно перед архивированием и отправкой (записью на съемный носитель);
 - г) Устанавливаемое (изменяемое) на ПК программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения на ПК лицом, установившим (изменившим) программное обеспечение, в присутствии пользователя ПК должна быть выполнена антивирусная проверка;
 - д) При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) работник МБОУ «СОШ №2 им. Сви́дерского А.Г.» должен провести внеочередной антивирусный контроль своего ПК;

е) В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов работники обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов инженера по защите информации, владельца зараженных файлов;
- совместно с владельцем зараженных вирусом файлов провести анализ возможности дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, немедленно приостановить работу и сообщить о данном факте ответственному по защите информации;
- по факту обнаружения зараженных вирусом файлов составить служебную записку, в которой необходимо указать предположительный источник (отправителя, владельца и т.д.) зараженного файла, тип зараженного файла, характер содержащейся в файле информации, тип вируса и выполненные антивирусные мероприятия.

3. Присутствовать при работах по внесению изменений в аппаратно-программную конфигурацию закрепленного за ним ПК.

4. Хранить значение своих паролей на бумажном или другом носителе информации.

2. Работникам МБОУ «СОШ №2 им. Свищерского А.Г.» категорически запрещается:

- использовать компоненты программного и аппаратного обеспечения ПК в неслужебных целях;
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ПК или устанавливать дополнительно любые программные и аппаратные средства, не предусмотренные формулярами ПК;
- осуществлять обработку конфиденциальной информации (персональных данных) в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять обработку конфиденциальной информации (персональных данных) при подключенном ПК к сети Интернет;
- записывать и хранить конфиденциальную информацию (персональные данные) на неучтенных носителях информации (гибких магнитных дисках и т.п.);
- оставлять включенными без присмотра свои ПК, не активировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры), если таковые имеются;
- оставлять без личного присмотра на рабочем месте или где бы то ни было машинные носители и распечатки, содержащие конфиденциальную информацию;
- предпринимать попытки несанкционированного доступа к недоступным информационным ресурсам, осуществлять намеренное изменение, уничтожение, чтение, или передачу информации неавторизованным способом;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению кризисной ситуации. Об обнаружении такого рода ошибок немедленно ставить в известность ответственного по защите информации.

3. Права работников, имеющих доступ к информационным ресурсам локальной сети и сети «Интернет».

3.1. Работники МБОУ «СОШ №2 им. Свищерского А.Г.», пользователи ПК имеют право:

3.1.1. Давать ответственному по защите информации предложения по совершенствованию мер информационной безопасности в учреждении;

- 3.1.2. Обращаться к инженеру по защите информации для оказания необходимой технической и методологической помощи в своей работе.
- 3.2. Ответственный по защите информации имеет право:
- 3.2.1. Требовать от работников - пользователей ПК соблюдения установленных технологий обработки информации и выполнения инструкций и других документов по обеспечению безопасности и защите информации;
- 3.2.2. Обращаться к руководителю с требованием прекращения работы сотрудников - пользователей ПК при несоблюдении ими установленных технологий обработки информации или невыполнении требований по обеспечению информационной безопасности;
- 3.2.3. Инициировать проведение служебных расследований по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи информации и технических средств.

4. Ответственность.

Работники учреждения, пользователи ПК, имеющие доступ к информационным ресурсам локальной сети МБОУ «СОШ №2» г. Бахчисарай и сети «Интернет», несут персональную ответственность за обеспечение информационной безопасности при их использовании, и соблюдение требований настоящей Инструкции.

Ответственный за антитеррористическую
безопасность в МБОУ «СОШ №2 им. Свидерского А.Г.»

А.Н. Сахацкая