УТВЕРЖДАЮ
Директор МАОУ СОШ № 14

_____Е.В.Шуховцева
Приказ № 111 от 24.05.2021 года

Инструкция
сотрудников МАОУ СОШ № 14
по обеспечению информационной безопасности

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности и ответственность сотрудников МАОУ СОШ № 14[1], допущенных к обработке конфиденциальной информации[2].

1.2. Пользователь при выполнении работ в пределах своих функциональных обязанностей, обеспечивает безопасность конфиденциальной информации и несет персональную ответственность за соблюдение требований руководящих документов по защите информации.

2. Основные обязанности пользователя:

2.1. Выполнять общие требования по обеспечению режима конфиденциальности проводимых работ, установленные законодательством РФ, внутренними документами МАОУ СОШ № 14 и настоящей Инструкцией.

2.2. При работе с конфиденциальной информацией располагать во время работы экран видеомонитора так, чтобы исключалась возможность просмотра отображаемой на нем информации посторонними лицами.

2.3. Соблюдать правила работы со средствами защиты информации и установленный режим разграничения доступа к техническим средствам, программам, базам данных, файлам и другим носителям конфиденциальной информацией при ее обработке.

2.4. После окончания обработки конфиденциальной информации в рамках выполнения одного задания, а также по окончании рабочего дня, произвести стирание остаточной информации с жесткого диска ЭВМ.

2.5. В случае выявления инцидентов информационной безопасности (фактов или попыток несанкционированного доступа к информации, обрабатываемой в ЭВМ или без использования средств автоматизации) немедленно сообщить об этом директору школы, написать служебную записку на имя директора и принять участие в служебной проверке по данному инциденту.

2.6. Самостоятельно не устанавливать на ЭВМ какие-либо аппаратные или программные средства.

2.7. Знать штатные режимы работы программного обеспечения, основные пути проникновения и распространения компьютерных вирусов.

2.9. Помнить личные пароли и персональные идентификаторы, хранить их в тайне, не оставлять без присмотра носители, их содержащие, и хранить в запирающемся ящике стола или сейфе. С установленной периодичностью менять свой пароль (пароли).

2.10. При применении внешних носителей информации перед началом работы провести их проверку на предмет наличия компьютерных вирусов средствами ЭВМ.

2.11. Знать и строго выполнять правила работы с установленными на его ЭВМ средствами защиты информации (антивирус, средства разграничения доступа, средства криптографической защиты и т.п.) в соответствии с технической документацией на эти средства.

2.12. Передавать для хранения установленным порядком свое индивидуальное устройство идентификации (Touch Memory , Smart Card , Proximity и т.п.), другие реквизиты разграничения доступа и носители ключевой информации (при наличии) только директору школы, ответственному за проведение мероприятий по обеспечению антитеррористической защищенности или системному администратору.

2.13. Надежно хранить и никому не передавать личную печать (при наличии).

---

[1] Далее – МАОУ СОШ № 14, школа.
[2] Далее – пользователь.

2.14. Немедленно ставить в известность директора школы и ответственного за проведение мероприятий по обеспечению антитеррористической защищенности при обнаружении:

- нарушений целостности пломб (наклеек, нарушении или несоответствии номеров печатей) на аппаратных средствах или иных фактов совершения в его отсутствие попыток несанкционированного доступа к закрепленной за ним ЭВМ;
- некорректного функционирования установленных на ЭВМ технических средств защиты;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию ЭВМ, выхода из строя или неустойчивого функционирования узлов ЭВМ или периферийных устройств (дисководов, принтера и т.п.), а также перебоев в системе электроснабжения.

2.15. По завершении работ по изменению аппаратно-программной конфигурации, закрепленной за ним ЭВМ проверять ее работоспособность.

3. Обеспечение антивирусной безопасности

3.1.Основными путями проникновения вирусов в информационно-вычислительную сеть организации являются: съемные носители информации, электронная почта, файлы, получаемые из сети Интернет, ранее зараженные ЭВМ.

3.2. При возникновении подозрения на наличие компьютерного вируса (сообщение антивирусной программы, нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь должен провести внеочередной антивирусный контроль ЭВМ.

3.3. В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь **ОБЯЗАН:**

- прекратить (приостановить) работу;
- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов директора школы, ответственного за информационную безопасность, а также иных сотрудников, находящихся в сети учреждения;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь системного администратора администратора).

3.4. Пользователю **ЗАПРЕЩАЕТСЯ:**

- отключать средства антивирусной защиты информации;
- без разрешения копировать любые файлы, устанавливать и использовать любое программное обеспечение, не предназначенное для выполнения служебных задач.

4. Обеспечение безопасности конфиденциальной информации

4.1. Основанием для допуска работника МАОУ СОШ № 14 к обработке конфиденциальной информации в рамках своих функциональных обязанностей является Перечнем должностей, утвержденным директором школы и должностная инструкция работника. Основанием для прекращения допуска к конфиденциальной информации является исключение из Перечня должностей, утвержденным директором школы и (или) изменение должностной инструкции работника.

4.3. Каждый работник школы, участвующий в процессах обработки конфиденциальной информации и имеющий доступ к аппаратным средствам, программному обеспечению и базам данных системы организации, является пользователем и несет персональную ответственность за свои действия.

4.4. Пользователь ***ОБЯЗАН***:

- *знать требования* руководящих документов по защите конфиденциальной информации;
- производить обработку защищаемой информации в строгом соответствии с утвержденными технологическими инструкциями (техническими порядками);
- строго соблюдать установленные правила обеспечения безопасности конфиденциальной информации при работе с программными и техническими средствами.

4.5. Пользователю **ЗАПРЕЩАЕТСЯ**:

- использовать компоненты программного и аппаратного обеспечения не по назначению (в неслужебных целях);
- использовать средства разработки и отладки программного обеспечения стандартных программных средств общего назначения (MS Office и др.);
- самовольно вносить какие-либо изменения в конфигурацию аппаратно-программных средств ЭВМ или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку конфиденциальной информации в присутствии посторонних (не допущенных к данной информации) лиц;
- осуществлять несанкционированную распечатку конфиденциальной информации;
- оставлять включенной без присмотра свою ЭВМ, не активизировав средства защиты от несанкционированного доступа (временную блокировку экрана и клавиатуры);
- оставлять без личного присмотра на рабочем месте или где бы то ни было свое персональное устройство идентификации, носители и распечатки, содержащие конфиденциальную информацию;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям безопасности конфиденциальной информации. Об обнаружении такого рода ошибок - ставить в известность системного администратора (при наличии) и директора школы.

4.6. Особенности обработки конфиденциальной информации без использования средств автоматизации.

4.6.1. Обработка конфиденциальной информации считается неавтоматизированной, если она осуществляется без использования средств вычислительной техники.

4.6.2. Допуск к неавтоматизированной обработке конфиденциальной информации осуществляется в соответствии с Перечнем должностей работников школы, имеющих доступ к конфиденциальной информации, которые несут ответственность за реализацию требований по обеспечению безопасности конфиденциальной информации.

4.6.3. Конфиденциальная информация при её неавтоматизированной обработке и хранении должна обособляться от иной информации путем фиксации её на отдельных материальных носителях.

4.6.4. Хранение материальных носителей конфиденциальной информации осуществляется в специальных шкафах (ящиках, сейфах и т.д.), обеспечивающих сохранность материальных носителей и исключающих несанкционированный к ним доступ.

5. Обеспечение информационной безопасности при использовании ресурсов сети Интернет

5.1. Ресурсы сети Интернет могут использоваться для осуществления выполнения требований законодательства Российской Федерации, дистанционного обслуживания, получения и распространения информации, связанной с деятельностью МАОУ СОШ № 14 (в том числе, путем создания информационного web-сайта), информационно-аналитической работы в интересах школы, обмена почтовыми сообщениями, а также ведения собственной хозяйственной деятельности. Иное использование ресурсов сети Интернет, решение о котором не принято руководством школы в установленном порядке, рассматривается как нарушение информационной безопасности.

5.2. С целью ограничения использования сети Интернет в неустановленных целях выделяется ограниченное число пакетов, содержащих перечень сервисов и ресурсов сети Интернет, доступных для пользователей. Наделение работников школы правами пользователя конкретного пакета выполняется в соответствии с его должностными обязанностями.

5.3.Особенности использования сети Интернет:

- сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- гарантии по обеспечению информационной безопасности при использовании сети Интернет никаким органом не предоставляются.

5.4. При осуществлении дистанционного обслуживания и электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет МАОУ СОШ № 14 применяет соответствующие средства защиты информации (межсетевые экраны, антивирусные средства, средства криптографической защиты информации и пр.), обеспечивающие прием и передачу информации только в установленном формате и только для конкретной технологии.

5.5. Электронная почта МАОУ СОШ № 14 подлежит периодической архивации. Доступ к архиву разрешен только лицу, ответственному за обеспечение информационной безопасности. Изменения в архиве не допускаются.

5.6. При пользовании ресурсами сети Интернет **ЗАПРЕЩАЕТСЯ:**

- использовать на рабочем месте иные каналы доступа ЭВМ к сети Интернет, кроме установленного;
- проводить самостоятельное изменение конфигурации технического и программного обеспечения ЭВМ, подключенной к сети Интернет;
- осуществлять отправку электронных почтовых сообщений, содержащих конфиденциальную информацию, по открытым каналам;
- использовать иные, кроме служебных, почтовые ящики для электронной переписки;
- открывать файлы, пришедшие вместе с почтовым сообщением, если не известен источник этого сообщения;
- осуществлять перенос полученной по сети Интернет документированной информации в электронном виде на другие компьютеры без проверки ее антивирусными программами;
- скачивать из сети Интернет, в том числе средствами электронной почты, информацию, содержащую исполняемые модули, программы, драйверы и т.п., без предварительного согласования с руководством школы или ответственным за информационную безопасность;
- использовать сеть Интернет вне служебных задач, посещать интернет-сайты, не связанные с выполнением должностных обязанностей.

6. Организация парольной защиты.

6.1. Пароль для своей учетной записи пользователь устанавливает самостоятельно.

6.2. Запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке ЭВМ) для входа в иные автоматизированные системы.

6.2. Длина пароля должна быть не менее 7 символов. В числе символов пароля рекомендуется использовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.).

6.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (логины, имена, фамилии и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

6.4. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 5 позициях.

6.5. Пользователь обязан хранить в тайне свой личный пароль.

6.6. Смена пароля осуществляется не реже 1 раза в 6 месяцев.

7. Ответственность пользователей

7.1. Работники МАОУ СОШ № 14 несут ответственность согласно действующему законодательству, за разглашение сведений, составляющих служебную, коммерческую и иную охраняемую законом тайну (в том числе персональные данные) и сведений ограниченного распространения, ставших им известными по роду работы.

7.2. Нарушения установленных правил и требований по обеспечению информационной безопасности являются основанием для применения к работнику (пользователю) мер наказания, предусмотренных трудовым законодательством.