ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00902E3B3BFD20F82A578BBD92E97957BD
Владелец: Пономарева Ирина Павловна
Действителен: с 24.08.2022 до 17.11.2023

УТВЕРЖДАЮ
Директор МБОУ «Школа № 64»
_____И.П. Пономарева
(подпись)
«___»_____ ___2023 г.

Инструкция по информационной безопасности для сотрудников объекта имеющих доступ к конфиденциальной информации

г. Ростов-на-Дону

1. Общие положения

1.1. Настоящая Инструкция определяет основные обязанности и ответственность пользователя, допущенного к обработке конфиденциальной информации, в том числе по средствам технических средств.

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 организации и настоящей Инструкцией.

2.2. При работе с конфиденциальной информацией располагать во время работы экран видео монитора 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 персонального компьютера.

2.5. В случае выявления инцидентов информационной безопасности (фактов или попыток несанкционированного доступа к информации, обрабатываемой в персональном компьютере или без использования средств автоматизации) немедленно сообщить об этом руководителя, для принятия решения по проведению проверке по данному инциденту.

2.6. Самостоятельно не устанавливать на персональный компьютер 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 персонального компьютера.

2.11. Знать и строго выполнять правила работы с установленными на его персональном компьютере 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 (TouchMemory, SmartCard, Proximity и т.п.), другие реквизиты разграничения доступа и носители ключевой информации только руководителю или ответственному за информационную безопасность.

2.13. Надежно хранить и никому не передавать личную печать.

2.14. Немедленно ставить в известность руководителя 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 защищенном персональном компьютере;
- некорректного функционирования установленных на персональный компьютер технических средств защиты;
- отклонений в нормальной работе системных и прикладных программных средств, затрудняющих эксплуатацию персонального компьютера, выхода из строя или неустойчивого функционирования узлов персонального компьютера 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 персонального компьютера проверять его 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 персональные компьютеры.

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 персонального компьютера.

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 своего руководителя, ответственного за информационную безопасность, а также смежные подразделения, использующие эти файлы в работе;
- оценить необходимость дальнейшего использования файлов, зараженных вирусом;
- провести лечение или уничтожение зараженных файлов (при необходимости для выполнения требований данного пункта следует привлечь администратора системы).

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 персональных данных

4.1. Основанием для допуска работника организации к обработке персональных данных в рамках своих функциональных обязанностей является Перечнем должностей, утвержденным директором организации и должностная инструкция работника. Основанием для прекращения допуска к персональным данным является исключение из Перечня должностей, утвержденным директором организации и (или) изменение должностной инструкции работника.

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

4.3. Пользователь обязан:

- знать требования руководящих документов по защите персональных данных;
- производить обработку защищаемой информации в строгом соответствии с утвержденными технологическими инструкциями;
- строго соблюдать установленные правила обеспечения безопасности персональных данных 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 персонального компьютера или устанавливать дополнительно любые программные и аппаратные средства;
- осуществлять обработку персональных данных в присутствии посторонних (не допущенных к данной информации) лиц;
- записывать и хранить персональные данные на неучтенных съемных носителях информации (гибких магнитных дисках, флэш — накопителях и т.п.), осуществлять несанкционированную распечатку персональных данных;
- оставлять включенной без присмотра свой персональный компьютер, 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 персональные данные;
- умышленно использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к нарушениям безопасности персональных данных. Об обнаружении такого рода ошибок — ставить в известность ответственного за безопасность информации и руководителя.

4.6. Особенности обработки персональных данных без использования средств автоматизации.

4.6.1. Обработка персональных данных считается не автоматизированной, если она осуществляется без использования средств вычислительной техники.

4.6.2. Допуск к не автоматизированной обработке персональных данных осуществляется в соответствии с Перечнем должностей сотрудников организации, имеющих доступ к персональным данным, которые несут ответственность за реализацию требований по обеспечению безопасности персональных данных.

4.6.3. Персональные данные при их не автоматизированной обработке и хранении должны обособляться от иной информации путем фиксации их на отдельных материальных носителях в специальных разделах или на полях форм (бланков).

4.6.4. При фиксации персональных данных на материальных носителях не допускается фиксация на одном материальном носителе персональных данных, цели обработки которых заведомо не совместимы.

4.6.5. Для каждой категории персональных данных используется отдельный материальный носитель.

4.6.6. Хранение материальных носителей персональных данных 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 организации (в том числе, путем создания информационного web-сайта), информационно-аналитической работы в интересах организации, обмена почтовыми сообщениями, а также ведения собственной хозяйственной деятельности. Иное использование ресурсов сети Интернет, решение о котором не принято руководством организации 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 организации 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 электронного документооборота, в связи с повышенными рисками информационной безопасности при взаимодействии с сетью Интернет организация 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. Почтовый обмен конфиденциальной информацией через сеть Интернет осуществляется с использованием защитных мер.

5.6. Электронная почта организации подлежит периодической архивации. Доступ к архиву разрешен только лицам в организации, ответственным за обеспечение информационной безопасности, руководителю организации. Изменения в архиве не допускаются.

5.7. При взаимодействии с сетью Интернет, технические средства обеспечиваются программными и аппаратными средствами противодействие атакам хакеров и распространению спама**.**

5.8. При пользовании ресурсами сети Интернет запрещается**:**

- использовать на рабочем месте иные каналы доступа персонального компьютера к сети Интернет, кроме установленного;
- проводить самостоятельное изменение конфигурации технического и программного обеспечения персонального компьютера, 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 руководителем;
- использовать сеть Интернет вне служебных задач, посещать интернет – сайты, не связанные с выполнением должностных обязанностей.

6. Порядок работы с носителями ключевой информации

6.1. В некоторых подсистемах организации для обеспечения контроля за целостностью передаваемых по технологическим каналам электронных документов (далее – ЭД), а также для подтверждения их подлинности и авторства могут использоваться средства электронной подписи (далее – ЭП).

6.2. Работнику организации (владельцу ключа ЭП), которому в соответствии с его должностными обязанностями предоставлено право постановки на ЭД его ЭП, выдается персональный ключевой носитель информации, на который записана уникальная ключевая информация (ключ ЭП), относящаяся к категории сведений ограниченного распространения.

6.3. Ключевые носители маркируются соответствующими этикетками, на которых отражается: регистрационный номер носителя и, при возможности размещения, дата изготовления и подпись уполномоченного сотрудника, изготовившего носитель, вид ключевой информации — эталон или рабочая копия, фамилия, имя, отчество и подпись владельца ключа ЭП.

6.4. Персональные ключевые носители (эталон и рабочую копию) владелец ключа ЭП должен хранить в специальном месте, гарантирующем их сохранность.

6.5. Ключи проверки ЭП установленным порядком регистрируются в справочнике «открытых» ключей, используемом при проверке подлинности документов по установленным на них ЭП.

6.6. Владелец ключа обязан:

- под подпись в «Журнале учета ключевых носителей и носителей ограниченной, служебной информации» получить ключевые носители, убедиться, что они правильно маркированы и на них установлена защита от записи;
- использовать для работы только рабочую копию своего ключевого носителя;
- сдавать свой персональный ключевой носитель на временное хранение руководителю подразделения или ответственному за информационную безопасность в период отсутствия на рабочем месте (например, на время отпуска или командировки);
- в случае порчи рабочей копии ключевого носителя (например, при ошибке чтения) владелец ЭП обязан передать его уполномоченному сотруднику, который должен в присутствии исполнителя сделать новую рабочую копию ключевого носителя с имеющегося эталона и выдать его взамен испорченного. Испорченная рабочая копия ключевого носителя должна быть уничтожена.

6.7. Владельцу ключа ЭП запрещается:

- оставлять ключевой носитель без личного присмотра;
- передавать свой ключевой носитель (эталонную или рабочую копию) другим лицам (кроме как для хранения руководителю или ответственному за информационную безопасность);
- делать неучтенные копии ключевого носителя, распечатывать или переписывать с него файлы на иной носитель информации (например, жесткий диск персонального компьютера), снимать защиту от записи, вносить изменения в файлы, находящиеся на ключевом носителе;
- использовать ключевой носитель на заведомо неисправном дисководе и/или персональном компьютере;
- подписывать своим персональным ключом ЭП любые электронные сообщения и документы, кроме тех видов документов, которые регламентированы технологическим процессом;
- сообщать третьим лицам информацию о владении ключом ЭП для данного технологического процесса.

6.8. Действия при компрометации ключей

6.8.1. Если у владельца ключа ЭП появилось подозрение, что его ключевой носитель попал или мог попасть в чужие руки (был скомпрометирован), он обязан немедленно прекратить (не возобновлять) работу с ключевым носителем, сообщить об этом руководителю, сдать скомпрометированный ключевой носитель с пометкой в журнале учета ключевых носителей и носителей ограниченной, служебной информации, о причине компрометации, написать пояснительную записку о факте компрометации персонального ключевого носителя на имя руководителя.

6.8.2. В случае утери ключевого носителя владелец ключа ЭП обязан немедленно сообщить об этом руководителю, написать объяснительную записку об утере ключевого носителя на имя руководителя и принять участие в проверке по факту утери ключевого носителя.

6.8.3. Ответственный за информационную безопасность обязан немедленно оповестить о факте утраты или компрометации ключевого носителя руководство организации для принятия действий по блокированию ключей для ЭП указанного исполнителя.

6.8.4. По решению руководства организации установленным порядком владелец ключа ЭП может получить новый комплект персональных ключевых носителей взамен скомпрометированных.

6.8.5. В случае перевода владельца ключа ЭП на другую работу, увольнения или прекращения трудовых отношений иным образом он обязан сдать (сразу по окончании последнего сеанса работы) свой ключевой носитель ответственному за информационную безопасность под подпись в журнале учёта.

7. Организация парольной защиты

7.1. Пароль для своей учетной записи пользователь устанавливает самостоятельно.

7.2. Запрещается использовать пароль домена локальной вычислительной сети (вводится при загрузке персонального компьютера) для входа в иные автоматизированные системы.

7.2. 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.).

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

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

7.5. Пользователь обязан хранить в тайне свой личный пароль.

7.6. Требования к паролю и периодичность его смены устанавливаются в групповых доменных политиках.

8. Ответственность пользователей

8.1. Работники организации 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.

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