

ИНСТРУКЦИЯ ПО УПРАВЛЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Общие сведения.

1.1. Назначение Настоящая Инструкция определяет обязанности, права и ответственность пользователей при обработке персональных данных с использованием средств автоматизации и информационных систем персональных данных, используемых в МАОУ «Средняя общеобразовательная школа № 2» (далее – Организация).

1.2. Цель разработки Инструкции.

Настоящая Инструкция принята в целях:

- обеспечения безопасности при работе пользователей с персональными данными с использованием средств автоматизации и информационных систем персональных данных;
- соблюдения требований законодательства и нормативных документов в сфере персональных данных.

1.3. Область применения.

Настоящий документ применяется:

- к процессам обработки персональных данных, в которых используются средства автоматизации и информационные системы персональных данных;
- ко всем обособленным подразделениям Организации;
- ко всем удаленным сотрудникам, независимо от их местоположения.

1.4. Аудитория.

Инструкция предназначена для следующих категорий сотрудников Организации:

- сотрудники, являющиеся пользователями средств автоматизации и информационных систем персональных данных;
- системные администраторы;
- администраторы информационной безопасности.

Под сотрудниками в настоящей Инструкции понимаются лица, состоящие в трудовых или договорных отношениях с Организацией.

1.5. Нормативные ссылки.

Инструкция разработана в целях реализации следующих нормативных правовых актов:

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состав и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

1.6. Срок действия и порядок внесения изменений.

Инструкция действует с момента утверждения и действует бессрочно до утверждения в новой редакции или издания документа, её заменяющего. Документ подлежит регулярному пересмотру с периодичностью не реже 1 раза в 3 года, а также в случае изменения требований законодательства, изменения оценки рисков информационной безопасности. Изменения в положение вносятся путем издания новой версии и ознакомления с ним сотрудников.

Срок хранения после прекращения действия: постоянно.

1.7. Используемые сокращения.

БД – база данных;

ИБ – информационная безопасность;

ИСПДн – информационная система персональных данных;

ПДн – персональные данные;

ПК – персональный компьютер;

ПО – программное обеспечение;

ОТР – One-Time Password.

2. Общие положения.

2.1. В настоящей инструкции рассматриваются обязанности, права и ответственность для следующих функциональных ролей:

- Администратор ИБ – сотрудник, отвечающий за установление и контроль требований безопасности при обработке ПДн автоматизированными средствами и в ИСПДн.
- Системный администратор – сотрудник, выполняющий установку, настройку и поддержку ПК пользователей, а также отдельных средств защиты информации в соответствии с настоящей инструкцией.
- Пользователь – сотрудник, работающий с сервисами и информационными системами персональных данных, и использующий для этого ПК, в рамках выполнения своих функциональных обязанностей.

2.2. Обязанности Администратора ИБ и Системного администратора назначаются приказом Руководителя Организации, определяются отдельными инструкциями, а также настоящей инструкцией.

2.3. Перечень ИСПДн, разрешенных к использованию, их характеристики и уровни защищенности персональных данных устанавливаются и утверждаются приказом.

2.4. Перечень сотрудников, которым разрешена запись персональных данных на съемные носители информации (USB Flash, Floppy, USB HDD, DVD и другие) определяется приказом по Организации.

2.5. Разрешается сотрудникам использовать ноутбуки за пределами организации, в дистанционном режиме работы при условии соблюдения мер безопасности в соответствии с разделом 8 настоящей Инструкции.

3. Основные требования для компьютеров.

3.1. Мониторы компьютеров не должны быть просматриваемы посетителями и через окна. На окнах должны быть предусмотрены шторы или жалюзи, не допускающие просмотра мониторов, повернутых в сторону окна.

3.2. Компьютеры при отсутствии активности пользователя в течение 10 минут должны блокироваться автоматически.

3.3. Компьютеры и сеть Организации должны быть обеспечены:

- ОС Windows (версия, не снятая с поддержки производителем);
- антивирус Kaspersky Endpoint Security (текущая версия), регулярное обновление не реже 2 раз в день и подключение к облачным сервисам безопасности Kaspersky Security Network;
- надёжные сложные пароли и учетные записи пользователей;
- регулярное обновление не реже 1 раза в месяц операционных систем и системного ПО или при выходе критических обновлений.

4. Обязанности пользователя.

4.1. Пользователь в рамках своих функциональных обязанностей в процессе обработки персональных данных с использованием средств автоматизации обязан:

- а. использовать их для выполнения служебных задач в строгом соответствии со своей должностной инструкцией и требованиями настоящей Инструкции;
- б. использовать для доступа к средствам автоматизации и ИСПДн собственную уникальную учетную запись и соответствующий ей пароль;
- в. хранить в тайне пароли доступа;
- г. не допускать при работе со средствами автоматизации просмотр посторонними лицами персональных данных, отображаемых на дисплее ПК;

- д. блокировать экран дисплея АРМ при оставлении рабочего места (нажатием Win+L в Windows;
- е. немедленно информировать лицо, ответственное за защиту информации, в случае обнаружения попыток несанкционированного доступа или вирусного заражения;
- ж. не открывать вложения подозрительных входящих сообщений электронной почты, не нажимать ссылки в таких сообщениях, удалять такие сообщения в случае невозможности удостовериться в источнике сообщения и его назначении;
- з. не открывать неизвестные сайты и не переходить по подозрительным ссылкам;
- и. использовать съемные носители информации только в целях обеспечения обязанностей, определенных приказом по организации;
- к. при работе с чувствительной информацией, коммерческой тайной применять для удаления черновиков и неиспользуемых файлов только специальные программы, гарантирующие удаление: например, Wipe, sdelete, которые могут быть встроены в менеджеры файлов.

4.2. Пользователю запрещается:

- а. предоставлять доступ к информации, содержащей персональные данные, лицам, не допущенным к их обработке в соответствии с приказом;
- б. самостоятельно изменять конфигурацию аппаратно-программных средств ИС;
- в. осуществлять действия по преодолению установленных ограничений на доступ к средствам автоматизации и ИСПДн;
- г. отключать или изменять конфигурацию средств защиты информации;
- д. устанавливать на автоматизированное рабочее место программное обеспечение, не связанное с исполнением служебных обязанностей;
- е. сообщать кому-либо устно или письменно личные атрибуты доступа к средствам автоматизации и ИСПДн;
- ж. производить какие-либо изменения в подключении и размещении технических средств;
- з. оставлять бесконтрольно автоматизированное рабочее место с загруженными персональными данными, с установленными маркированными носителями, а также распечатываемыми бумажными документами с персональными данными.

4.3. Пользователь имеет право:

- а. обрабатывать (создавать, редактировать, уничтожать, копировать, выводить на печать) информацию в пределах установленного объема и полномочий;
- б. получать от лиц, ответственных за организацию обработки персональных данных и за защиту информации консультативную помощь по вопросам эксплуатации средств автоматизации и ИСПДн.

5. Порядок использования паролей.

5.1. Общие требования к паролям и средствам аутентификации.

5.1.1. Порядок применяется к паролям для средств автоматизации и ИСПДн, а также к средствам VPN, сетевому оборудованию, системам обеспечения эксплуатации, инфраструктурным сервисам, сервисам безопасности, резервного копирования и другим.

5.1.2. Личные пароли доступа сотрудников Организации должны формироваться и распределяться с учетом следующих требований:

- а. идентификаторы пользователей и их пароли должны быть уникальными для каждого пользователя;
- б. пароли должны состоять как минимум из 8 символов (не должны быть именами или известными фразами);
- в. длина паролей для администраторов серверов, баз данных, сетевого оборудования, а также средств защиты информации должна составлять не менее 10 буквенно-цифровых символов;
- г. в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры. Рекомендуется использовать в парольной фразе специальные символы (@, #, \$, &, *, % и т.п.);
- д. пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования ПК и т.д.), а также общепринятые сокращения (ПК, ЭВМ, USER и т.п.);
- е. пароли должны держаться в тайне, то есть не должны сообщаться другим людям, не должны вставляться в тексты программ, и не должны записываться на бумагу;

- ж. чтобы предотвратить использование того же самого или угадываемого пароля, пароли должны меняться не реже, чем каждые 90 дней;
- з. пароли учетных записей администраторов серверов, баз данных, сетевого оборудования, а также средств защиты информации должны меняться не реже чем раз в месяц;
- и. при смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях;
- к. учетные данные пользователей должны быть заблокированы после 5 (пяти) неудачных попыток входа в систему на 30 минут. Все случаи неверно введенных паролей и факт блокировки должны быть записаны в системный журнал, в целях определения и расследования инцидента информационной безопасности;
- л. сеансы работы пользователей с ПК и сетевых соединений с сервером должны блокироваться после 15 минут неактивности (или другого согласованного периода). Для возобновления сеанса должен снова требоваться ввод пароля.
- 5.1.3. Работники Организации, использующие в работе средства автоматизации и имеющие доступ к ИСПДн, должны быть ознакомлены с перечисленными выше требованиями и ответственности за разглашение парольной информации, а также за использование паролей, не соответствующих данным требованиям.
- 5.1.4. Для генерации сложных паролей могут применяться специальные программные средства.
- 5.1.5. Система централизованной генерации и распределения паролей должна исключать возможность ознакомления посторонних лиц с паролями сотрудников подразделений.
- 5.1.6. В рамках домена Организации должны использоваться централизованные политики, реализуемые средствами контроллера домена Microsoft Active Directory с применением групповых политик.
- 5.1.7. В случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т.п., а также при наличии технологической необходимости использования имен и паролей некоторых сотрудников (исполнителей) в их отсутствие, такие сотрудники обязаны сразу же после смены своих паролей их новые значения (вместе с именами соответствующих учетных записей) в запечатанном конверте передавать на хранение администратору ИС.
- 5.2. Порядок смены паролей.
- 5.2.1. Плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в полугодие.
- 5.2.2. Внеплановая смена личного пароля, блокировка или удаление учетной записи работника Организации в случае прекращения его полномочий (увольнение, переход в другое подразделение и т.д.) должна производиться Системным администратором немедленно после окончания последнего сеанса работы данного работника с информационными системами.
- 5.2.3. Полная внеплановая смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри организации и другие обстоятельства), Администратора ИБ, Системного администратора и других сотрудников, которым по роду работы были предоставлены повышенные права.
- 5.2.4. В случае компрометации личного пароля пользователя должны быть немедленно предприняты меры по внеплановой смене паролей в зависимости от полномочий владельца скомпрометированного пароля.
- 5.2.5. Хранение сотрудником (исполнителем) значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у администратора информационной безопасности или руководителя подразделения в опечатанном личной печатью конверте (возможно вместе с персональными ключевыми носителями).

6. Антивирусная защита.

- 6.1. В целях обеспечения защиты от вредоносного ПО, а также защиты от различных видов атак на рабочие места предусматривается установка на рабочие места антивирусного программного обеспечения.
- 6.2. Ответственность за поддержание установленного в настоящей Инструкции порядка проведения антивирусного контроля возлагается на Системного администратора.
- 6.3. К применению на ПК допускаются только лицензионные антивирусные средства.

- 6.4. На ПК запрещается установка программного обеспечения, не связанного с выполнением функций, предусмотренных технологическим процессом обработки информации.
- 6.5. Пользователи при работе со съемными носителями информации обязаны перед началом работы осуществить их проверку на предмет отсутствия компьютерных вирусов. Должна быть настроена автоматическая проверка носителя перед открытием.
- 6.6. Системный администратор обязан осуществлять или организовывать периодическое обновление антивирусных пакетов и контроль их работоспособности.
- 6.7. Системный администратор обязан проводить периодическое тестирование всего установленного программного обеспечения и дискового пространства ИСПДн на предмет отсутствия компьютерных вирусов.
- 6.8. При обнаружении компьютерного вируса пользователь обязан прекратить какие-либо действия на своем АРМ и немедленно доложить об этом Системному администратору.
- 6.9. В случае необходимости Системный администратор обязан проводить «лечение» зараженных файлов путем выбора соответствующего пункта меню антивирусной программы. По окончании «лечения» должен быть проведен повторный антивирусный контроль.
- 6.10. В случае обнаружения на АРМ или на съемном носителе информации вируса, не поддающегося «лечению», Системный администратор обязан запретить работу на АРМ и в возможно короткие сроки обновить пакет антивирусных программ.
- 6.11. Признаки заражения персонального компьютера вредоносным ПО:
- Изменение стандартной стартовой страницы поиска интернет-браузера без вашего одобрения.
 - Несанкционированное открытие новых окон, появление на экране монитора сообщений о том, что на компьютере обнаружены вредоносные или рекламные программы.
 - Сообщения антивируса о невозможности обновиться.
 - Отключение антивируса и средств защиты, отсутствие запроса пароля.
- 6.12. Необходимо соблюдать внимательность так как некоторые вредоносные программы нейтрализуют возможность обновления антивирусных средств, что делает систему защиты неэффективной.

7. Порядок доступа в сеть Интернет и работы с электронной почтой.

7.1. Правила работы с ресурсами сети Интернет.

Запрещается осуществлять выход в сеть «Интернет» при:

- отсутствующем либо не работающем на ПК установленном антивирусном средстве защиты информации;
- возникновении ошибок антивируса (отсутствие лицензии, наличие угроз, не обновленные базы);
- невыполнении обновления операционной системы и браузеров на ПК.

7.1.1. Доступ к ресурсам сети «Интернет» предоставляется работникам Организации только для исполнения должностных обязанностей.

7.1.2. Запрещается осуществлять доступ к ресурсам сети «Интернет» в других целях (развлекательные и игровые ресурсы, социальные сети), поскольку такие ресурсы могут быть источником вирусов и проникновения атакующих.

7.1.3. Необходимо закрывать страницы сайтов с большим количеством навязчивых рекламных предложений в виде баннеров или всплывающих окон сразу после их открытия.

7.1.4. Запрещается загружать и запускать файлы и программное обеспечение из сети Интернет».

7.1.5. Разрешено скачивать файлы с официальных интернет-сайтов известных Организаций, проверенных репозиторий, сайтов органов власти РФ, территориальных органов федеральных органов исполнительной власти, государственных порталов.

7.1.6. Запрещается сохранять пароли на доступ к информационным ресурсам в сети «Интернет» в кэше интернет-браузера или в открытом виде. Допускается применять менеджеры паролей типа Kaspersky Password Manager или KeePass.

7.1.7. Необходимо использовать при работе в сети «Интернет» браузеры, для которых отслеживаются и своевременно устанавливаются обновления (например, Yandex.Browser).

7.2. Правила работы с электронной почтой и облачными сервисами.

7.2.1. Электронная почта и аккаунты в облачных сервисах, предоставляемые

Организацией, должна использоваться пользователями только для исполнения служебных

обязанностей.

7.2.2. Запрещается:

- использовать рабочий электронный адрес в личных целях или для пересылки личных сообщений, для подписки на рассылки и другие сервисы сети «Интернет», а также при регистрации на любых сайтах сети «Интернет», если это прямо не связано с должностными обязанностями;

- использовать аккаунт в облачном сервисе для личных целей.

7.2.3. В служебных целях необходимо использовать только почтовый сервис, предоставленный Организацией.

7.2.4. Не допускается передача по сети «Интернет» информации об учетных записях (имена пользователей, пароли) и другой конфиденциальной информации, включающей персональные данные, коммерческую тайну Организации и её партнеров, и др.

7.2.5. При необходимости передача такой информации через «Интернет» производится только с согласия её обладателя.

7.2.6. Запрещается переходить по ссылкам и открывать файлы в сообщениях, содержащих:

- текст рекламного характера с просьбой перейти по ссылке или открыть вложение;

- файл и пароль от файла;

- информацию, файлы или ссылки, не имеющие отношения к служебной деятельности, ранее обсуждаемой теме и не затребованные у отправителя, в том числе в случаях, когда отправителем является официальная организация;

- информацию, имеющую отношение к работе или соседним подразделениям, но пришедшую от неизвестного лица.

7.2.7. При необходимости следует уточнить у отправителя (по телефону) факт отправки сообщения, вызывающего подозрения о его достоверности.

7.2.8. При получении подозрительных сообщений от известных пользователю организаций и пользователей – не удалять сообщение и сообщить об этом факте Администратору ИБ.

7.2.9. В случае наличия подозрений о присутствии вредоносных программ необходимо информировать об этом Администратора ИБ.

7.2.10. Удалять сообщения от неустановленных отправителей с подозрительными вложениями, не открывая вложения, и очищать корзину, где хранятся удаленные сообщения.

8. Порядок обеспечения безопасности при дистанционной работе.

8.1. Дистанционная работа отличается от работы в Организации отсутствием контролируемых Организацией мер физической защиты компьютеров, а также отсутствием защищенной офисной сети, в которой может работать ПК и получать доступ к локальным ресурсам. При этом применяются средства защищенного доступа, в том числе с использованием VPN и средств шифрования.

8.2. Актуальность угроз безопасности определяется оценкой угроз, проводимой в Организации. К угрозам могут относиться: кража ПК, носителей информации, паролей, ключей шифрования, выход из строя оборудования, несанкционированный доступ угрозы, связанные с несоблюдением ограничений использования, внедрение вирусов и т.п.

8.3. Сотрудники, которым разрешается дистанционная форма работы, должны быть допущены приказом, закрепляющим должности и виды работ, для которых разрешается дистанционная работа.

8.4. Дистанционная работа разрешается с использованием ПК, выданных Организацией и настроенных с учетом требований настоящей инструкции.

8.5. При предоставлении доступа пользователю Администратор ИБ:

- производит инструктаж сотрудника по вопросам безопасности удаленной работы;

- формирует необходимые дополнительные средства аутентификации (пароли, OTP) и доступа по VPN;

- включает усиленный профиль операционной системы и средств антивирусной защиты ПК;

включает при необходимости дополнительные средства мониторинга ПК и пользователя на предмет событий и инцидентов информационной безопасности.

8.6. Пользователь при работе в дистанционной форме обязан:

- соблюдать требования безопасности;

- не сообщать никому пароль, не выписывать его и не передавать средства аутентификации;
- проявлять бдительность в общественных местах и обеспечивать сохранность ПК и другого выданного оборудования;
- при утрате ПК,
- носителей информации незамедлительно сообщать Администратору ИБ для блокирования доступа в открытые ранее ресурсы и планирования дальнейших действий.

9. Порядок обслуживания и контроля.

9.1. Обслуживание компьютеров, системного ПО, прикладного ПО, ИС должно производиться с обеспечением конфиденциальности и безопасности персональных данных и информации, которая хранится и обрабатывается с их помощью.

9.2. Пользователям запрещается препятствовать работе средств мониторинга и контроля, применяемых на ПК.

9.3. Обслуживание осуществляется:

- внутренних ИСПДн Организации - Системным администратором;
- ПК – Системным администратором или назначенным специалистом;
- внешних и облачных сервисов - операторами этих сервисов по договору (соглашению) с Организацией.

9.4. Управление доступом к внутренним ИСПДн, ресурсам и ПК осуществляется Системным администратором.

9.5. При необходимости выполнения ремонта в стороннем сервисном центре технических средств ПК необходимо снять с них носители информации или надежным образом удалить с них данные.

9.6. Мониторинг и контроль корректности эксплуатации пользователями ИС и ПК выполняется Системным администратором.

9.7. Мониторинг и контроль соблюдения мер безопасности в ИС и на ПК организовывается и осуществляется Администратором ИБ.

10. Ответственность пользователя.

10.1. Пользователь несет ответственность в соответствии с действующим законодательством Российской Федерации, а также внутренними организационно-распорядительными документами Организации за:

- а. нарушение работоспособности или вывод из строя функций безопасности ИСПДн, ПК и других средств автоматизации;
- б. преднамеренные действия, повлекшие модификацию или уничтожение персональных данных в ИС;
- в. несанкционированный доступ к персональным данным в ИС;
- г. разглашение персональных данных;
- д. причинение ущерба субъектам персональных данных, Организации и иным лицам.

10.2. Сотрудники, имеющие расширенные права в ИС, в том числе Администраторы ИБ и Системные администраторы, несут ответственность за собственные действия (бездействие), которые привели к некорректному функционированию прикладного программного обеспечения ИС, утечке данных, и причинению ущерба в соответствии с законодательством РФ.