Муниципальное бюджетное общеобразовательное учреждение «Добрянская средняя общеобразовательная школа № 1 (Кадетская школа)»

ПРИКАЗ

г. Добрянка

от 21.08.2023г. № 162

«Об утверждении Политики информационной безопасности»

В соответствии с Федеральным законом от 27 июля 2006г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 26 июля 2017г. № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации», Указом Президента Российской Федерации от 05 декабря 2016г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Приказом Управления образования № 192 от 02 августа 2023 года «Об утверждении Политики информационной безопасности»

ПРИКАЗЫВАЮ

1. Назначить администратором безопасности, обеспечивающим функцию по обеспечению информационной безопасности – Бурцеву Анну Сергеевну, заместителя директора по АХЧ.
2. Утвердить политику по информационной безопасности в Муниципальном бюджетном общеобразовательном учреждении «Добрянская средняя общеобразовательная школа № 1 (Кадетская школа)» (Приложение 1).
3. Утвердить инструкцию по работе пользователя в автоматизированной системе (Приложение 2).
4. Администратору безопасности: проводить инструктажи не реже одного раза в год и внепланово для вновь поступивших сотрудников; вести журнал регистрации проведения инструктажей по информационной безопасности.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор школы О.А. Пискунова

Приложение 1 к приказу
МБОУ «ДСОШ № 1 (КШ)»
№ 162 от 21.08.2023г.

ПОЛИТИКА
по информационной безопасности в Муниципальном бюджетном общеобразовательном учреждении «Добрянская средняя общеобразовательная школа № 1 (Кадетская школа)»

1. Работа с документами и носителями информации

1.1. Работа с документами и носителями информации в МБОУ «ДСОШ № 1 (КШ)» осуществляется в соответствии с нормативными актами администрации ДГО: постановление администрации Добрянского городского округа от 22 марта 2022 г. № 627 «Об утверждении Политики обработки и защиты персональных данных в администрации Добрянского городского округа и отраслевых (функциональных) органах администрации Добрянского городского округа»; постановление администрации Добрянского городского округа от 13 мая 2022 г. № 1202 «Об утверждении Правил обработки и защиты персональных данных в администрации Добрянского городского округа»; распоряжение администрации Добрянского городского округа от 16 августа 2022 г. № 285-р «Об утверждении Инструкции по делопроизводству и ведению архива в администрации Добрянского городского округа, отраслевых (функциональных) и территориальных органах администрации округа».

1.2. Запрещается выносить рабочие документы на бумажных или иных носителях информации (флеш-карты, внешние накопители и др.) из административных здания учреждения без служебной необходимости.

1.3. Уничтожение документов на бумажных носителях должно производиться сотрудниками с использованием прибора для измельчения бумаги, с общим доступом для сотрудников.

1.4. Запрещается утилизировать в урны для мусора, корзины для макулатуры не измельченные на специальном оборудовании документы.

1.5. В случае утери сотрудником рабочих документов и иных носителей информации (флеш-карты, внешние накопители и др.) необходимо незамедлительно сообщить об этом непосредственному руководителю, в особых случаях, при утере документов конфиденциального характера - ответственному сотруднику.

1.6. В МБОУ «ДСОШ № 1 (КШ)» внедрена и эксплуатируется система электронного документооборота (далее - СЭД). При работе с СЭД сотрудникам запрещается передавать учетные данные (логин, пароль) третьим лицам и другим сотрудникам, загружать в СЭД документы, содержащие информацию ограниченного распространения (с ограничительной пометкой

«для служебного пользования») и документы, содержащие персональные данные (паспорт, СНИЛС и др.).

2. Работа с автоматизированными рабочими местами учреждений

2.1. Сотрудникам необходимо располагать экран монитора в помещении во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами.

2.2. При отсутствии визуального контроля сотрудника за автоматизированным рабочим местом (далее – АРМ) сотруднику необходимо блокировать доступ. Для блокировки необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию «Блокировка».

2.3. Сотрудникам по окончании рабочего дня необходимо выключать АРМ.

2.4. Сотрудникам, за исключением технических специалистов, действующих в рамках договоров с учреждением на оказание услуг по техническому обслуживанию компьютеров и оргтехники и IT-сопровождению, запрещается: самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение; изменять установленный алгоритм функционирования технических и программных средств; несанкционированно открывать общий доступ к каталогам на АРМ, а также производить удаленное подключение к АРМ по незащищенным каналам связи; подключать к АРМ личные съемные машинные носители информации и мобильные устройства, а также копировать информацию, ставшую им известной в ходе выполнения должностных обязанностей на такие носители без служебной необходимости, за исключением технических специалистов, действующих в рамках договоров на оказание услуг по техническому обслуживанию компьютеров и оргтехники и IT-сопровождению; отключать (удалять) установленные на АРМ средства защиты информации; привлекать лиц, не являющихся сотрудниками обслуживающих организаций, осуществляющих техническое обслуживание на договорной основе с учреждением, для осуществления установки программного обеспечения, ремонта или настройки технических средств АРМ; производить какие-либо изменения в электрических схемах, монтаже и размещении технических средств АРМ, обслуживающих организаций, осуществляющих техническое обслуживание на договорной основе с учреждениями; использовать личные автоматизированные рабочие места (ноутбуки, персональные компьютеры) для выполнения своих должностных обязанностей; осуществлять фото- и видеосъемку рабочих документов, а также публикацию таких документов в социальных сетях и других открытых ресурсах (за исключением случаев, когда это необходимо для выполнения должностных обязанностей, по согласованию с непосредственным руководителем); производить деструктивные действия в отношении АРМ учреждений.

2.5. Сотрудникам необходимо: соблюдать правила парольной защиты при работе с АРМ в соответствии с разделом V настоящей Политики;

соблюдать правила работы в сети Интернет в соответствии с разделом VI настоящей Политики; соблюдать правила антивирусной защиты в соответствии с разделом VII настоящей Политики; не допускать случаев социальной инженерии и фишинга в соответствии с разделом VIII настоящей Политики.

3. Правила парольной защиты

3.1. Требования к паролю:

пароль не должен содержать имя учетной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из 8 символов, в числе символов пароля обязательно должны присутствовать цифры и буквы как строчные, так и прописные (заглавные) буквы;

запрещается использовать в качестве пароля простые пароли, такие как «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о сотруднике;

пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения;

смена пароля должна производиться не реже одного раза в 90 дней;

при смене пароля новое значение должно отличаться от предыдущего не менее чем на четыре символа.

3.2. Правила ввода пароля:

ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

во время ввода пароля необходимо исключить возможность его раскрытия иными лицам, в том числе с помощью технических средств (видеокамеры и др.).

4.3. Правила хранения пароля:

рекомендуется не записывать пароль на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

запрещается сообщать другим сотрудникам и третьим лицам личный пароль от АРМ;

сотрудникам необходимо своевременно сообщать об утере, компрометации, несанкционированном изменении паролей непосредственному руководителю, а также ответственному сотруднику.

4. Правила работы в сети Интернет

4.1. При работе в сети Интернет сотрудник обязан: производить работу в сети Интернет исключительно в целях исполнения своих должностных обязанностей; не открывать вложения в письмах от неизвестных источников, не переходить по подозрительным баннерам и ссылкам на веб-сайтах, проверять вводимый адрес веб-сайтов на предмет опечаток; обращаться к

ответственному сотруднику в случае выявления фактов нарушения информационной безопасности.

4.2. При работе в сети интернет сотруднику запрещается: посещать сайты сомнительной репутации (сайты, содержащие нелегально распространяемое программное обеспечение, торрент-сайты и т.д.) и скачивать с таких сайтов какие-либо файлы и программное обеспечение; нецелевое использование подключения к сети «Интернет» (просмотр фильмов, скачивание игр и т.д.).

4.3. Использование электронной почты. Каждому сотруднику при трудоустройстве создается служебный адрес электронной почты, который при увольнении сотрудника в обязательном порядке подлежит удалению. Использовать в служебных целях личные адреса электронной почты запрещается, за исключением необходимости её использования для аутентификации в Единой системе идентификации и аутентификации (ЕСИА), с целью обеспечения санкционированного доступа к информации в государственных системах. Не допускается передача учетных данных (логин, пароль) электронной почты другим сотрудникам и третьим лицам. Не допускается использование электронной почты для отправки информации, содержащей персональные данные. Не допускается использование электронной почты для отправки конфиденциальной информации, информации ограниченного доступа и информации, содержащей государственную тайну.

Для приема обращений граждан недопустимо использование сторонних почтовых сервисов, не отвечающих требованиям безопасности в соответствии с действующим законодательством в области защиты персональных данных. Для направления ответов на обращения граждан рекомендуется использовать только служебный адрес электронной почты, размещенный на почтовом сервере Единого почтового домена Пермского края, в адресном пространстве permkrai.ru.

4.4. Использование социальных сетей в рабочих целях. В случае если должностными обязанностями работника предусмотрено использование социальных сетей «Вконтакте», «Telegram», «Одноклассники» (далее – Приложение), необходимо:

ознакомиться с политикой использования Приложения;

не загружать конфиденциальную информацию, в том числе персональные данные;

исключить передачу учетных данных (логин, пароль) третьим лицам и другим сотрудникам;

в случае наличия технической возможности Приложения использовать двухфакторную аутентификацию.

5. Соблюдение антивирусной защиты информации

5.1. Антивирусная проверка АРМ и отчуждаемых машинных носителей (флэш-накопители, внешние накопители на жестких дисках и иные устройства) учрежденя производится в автоматическом режиме без участия

конечных пользователей АРМ, под контролем сотрудников обслуживающих организаций, осуществляющих техническое обслуживание на договорной основе.

5.2. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник должен: уведомить непосредственного руководителя и администратора безопасности; временно приостановить работу с АРМ.

5.2. Сотруднику запрещается: удалять средства антивирусной защиты, установленные на АРМ; вносить изменения в настройки средства антивирусной защиты, установленного на АРМ.

6. Противодействие социальной инженерии и фишингу

6.1. Социальная инженерия – совокупность приемов и методов, применяемых злоумышленниками, направленных на получение от сотрудника служебной (конфиденциальной) информации. В целях противодействия социальной инженерии сотруднику необходимо: не сообщать по электронной почте и по телефону служебной информации пока не будет установлена личность запрашивающего и его право на доступ к такой информации; не осуществлять работу за АРМ и с документами в присутствии посторонних лиц; блокировать АРМ (при отсутствии за рабочим местом, при окончании рабочего дня и т.д.); в случае попытки посторонних лиц получить от сотрудника служебную (конфиденциальную) информацию, незамедлительно сообщить об этом непосредственному руководителю;

6.2. Фишинг - вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям и т.д.).

6.2.1. В целях противодействия фишингу сотрудникам необходимо: осуществлять проверку адреса любого сайта, который запрашивает идентификационную информацию; осуществлять проверку электронной почты отправителя писем; не проходить по подозрительным ссылкам и не скачивать подозрительные файлы; об утере или компрометации логинов и паролей сообщать непосредственному руководителю и администратору безопасности.

7. Проведение совещаний в формате Видеоконференции

В учреждении для проведения совещаний в формате видеоконференции рекомендуется использовать такие системы, как «Trueconf», Яндекс. Телемост (далее – системы ВКС). Использование сотрудниками в ходе исполнения должностных обязанностей иностранных сервисов для проведения видеоконференций, таких как Zoom, Skype, запрещается.

8. Дистанционная (удаленная) работа

8.1. В особых случаях, на основании нормативно-правового акта учреждения, для всех или отдельных сотрудников может быть установлен дистанционный (удаленный) режим работы.

8.2. При установлении дистанционного (удаленного) режима работы на сотрудников в период выполнения ими трудовой функции дистанционно распространяется действие трудового законодательства и иных актов, содержащих нормы трудового права, с учетом особенностей, установленных главой 49.1 Трудового кодекса Российской Федерации.

9. Обработка персональных данных

9.1. Обработка персональных данных сотрудниками должна производиться с соблюдением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

10. Подготовка технических заданий и проведение закупочных процедур

Запрещается разглашать сведения об осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд в соответствии с Федеральным законом от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» до момента их официального опубликования, а именно, извещения, технические задания и иную информацию, относящуюся к процедурам определения поставщика (конкурсную, аукционную документацию и т.д.).

11. Ответственность сотрудника за нарушение правил информационной безопасности

11.1. Ответственность за нарушение правил информационной безопасности несет каждый сотрудник в пределах своих служебных обязанностей и полномочий.

11.2. На основании статьи 192 Трудового кодекса Российской Федерации сотрудники, нарушающие правила настоящего документа, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговоры увольнение с работы.

11.3. На основании статьи 238 Трудового кодекса РФ все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный учреждению в результате нарушения ими правил настоящего документа.

11.4. На основании статьи 81 Трудового кодекса Российской Федерации с сотрудником может быть расторгнут трудовой договор в случае разглашения сотрудником охраняемой законом тайны (коммерческой, служебной и иной), ставшей известной сотруднику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого сотрудника.

11.5. На основании статьи 26 Федерального закона от 21 июля 1993 г.№ 5485-1 «О государственной тайне» сотрудники, виновные в нарушении законодательства РФ о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

12. Порядок доступа в здание. Защита от несанкционированного доступа в помещения зданий.

Порядок доступа в здание и защита от несанкционированного доступа в помещения зданий учреждения осуществляется, в соответствии с требованиями антитеррористической безопасности.

Приложение 2 к приказу
МБОУ «ДСОШ № 1 (КШ)»
№ 162 от 21.08.2023г.

Инструкция
по работе пользователя в автоматизированной системе

Общие положения

Настоящая инструкция определяет правила работы пользователя в защищаемых от несанкционированного доступа (далее – НСД) автоматизированных системах учреждений (далее – АС).

Допуск пользователей для работы с данными, находящимися в АС, осуществляется в соответствии со списком лиц, допущенных к работе, утвержденным руководителем учреждения.

Вход пользователя в АС осуществляется на основе ввода персонального идентификатора (по запросу системы) имени учетной записи и пароля конкретного пользователя.

Пользователь несет персональную ответственность за свои действия.

Квалификационные требования

Пользователь должен знать:

– законодательные и нормативные правовые акты, регламентирующие деятельность юридических лиц в сфере обработки информации конфиденциального характера;

– внутренние локальные акты, регламентирующие обработку информации конфиденциального/секретного характера в АС.

Основные функциональные обязанности пользователя, работающего в АС

Пользователь обязан:

– Выполнять требования действующих нормативных и руководящих документов, а также внутренних локальных актов, регламентирующих обработку информации секретного характера в АС учреждения;

– выполнять на автоматизированном рабочем месте (АРМ) только те процедуры, которые определены для него его обязанностями;

– соблюдать установленные требования по режиму обработки информации секретного характера, учету, хранению и пересылке носителей информации, обеспечению безопасности информации секретного характера, а также руководящих и организационно-распорядительных документов;

– экран монитора в помещении располагать во время работы так,. чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами;

– обо всех выявленных нарушениях, связанных с информационной безопасностью, а также для получения консультаций по вопросам информационной безопасности, необходимо обратиться к руководителю или администратору безопасности;

– для получения консультаций по вопросам работы и настройки элементов АС необходимо обращаться к руководителю или администратору безопасности;

– при отсутствии визуального контроля за рабочей станцией доступ к компьютеру должен быть немедленно заблокирован. Для этого необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, либо иным способом, предусмотренным в операционной системе;

– по окончании работы в АС выйти из системы и выключить компьютер;

– соблюдать правила работы со съемными носителями защищаемой информации.

Пользователю запрещается:

– разглашать защищаемую информацию третьим лицам;

– копировать защищаемую информацию на внешние носители без разрешения руководителя работ;

– самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств;

– несанкционированно открывать общий доступ к каталогам на своей рабочей станции;

– подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства;

– отключать (блокировать) средства защиты информации;

– обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к АС;

– сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам АС;

– привлекать посторонних лиц для производства ремонта или настройки АРМ без согласования с руководителем или администратором безопасности.

Организация парольной защиты

Личные пароли доступа к элементам АС выдаются пользователям администратором безопасности.

Полная плановая смена паролей в АС проводится не реже одного раза в 3 месяца.

Правила формирования пароля:

Пароль не может содержать имя учетной записи пользователя или какую-либо его часть.

Пароль должен состоять не менее чем из 8 символов, желательно использовать пароли, состоящие из 10 и более символов.

Запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также свои имена и даты рождения, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

Пароль не должен включать в себя легко вычисляемые сочетания символов, а также общепринятые сокращения.

Запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например,1234567 и т.п.).

В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры, желательно использовать специальные символы.

Запрещается выбирать пароли, которые уже использовались ранее. При смене пароля новое значение должно отличаться от предыдущего не менее чем на четыре символа.

Правила ввода пароля:

– ввод пароля должен осуществляться с учётом регистра, в котором пароль был задан;

– во время ввода паролей необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (видеокамеры и др.).

Правила хранения пароля:

– запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

– запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем;

– лица, использующие паролирование, обязаны:

а) четко знать и строго выполнять требования настоящей инструкции и других руководящих документов по паролированию;

б) своевременно сообщать руководителю или администратору безопасности об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.

Обязанности пользователя по обеспечению антивирусной защиты

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.) пользователь самостоятельно или вместе с администратором безопасности должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователь обязан:

– приостановить работу;

– немедленно поставить в известность о факте обнаружения зараженных вирусом файлов администратора безопасности;

– по факту обнаружения зараженных вирусом файлов составить служебную записку руководителю, 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.

При необходимости пополнения базы АС данными, полученными со стороны с помощью съемных носителей, пользователь обязан контролировать отсутствие вирусного заражения информации на съемном носителе.

Пользователь обязан проводить проверку антивирусом на наличие вирусного заражения не реже, чем один раз в неделю.

Права пользователя, работающего в АС

Пользователь имеет право:

– в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам АС, присвоенными ему администратором безопасности.

Правила работы со съемными носителями защищаемой информации

К носителям защищаемой информации относятся:

– съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);

– машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

Выдачу съемных носителей защищаемой информации осуществляет администратор безопасности. Сотрудники учреждения получают учтенный съемный носитель от администратора безопасности для выполнения работ на конкретный срок. При получении делаются соответствующие записи в журнале учета. По окончании работ пользователь сдает съемный носитель для хранения администратору безопасности, о чем делается запись в журнале учета.

При использовании съемных носителей с защищаемой информацией запрещается:

– хранить съемные носители с защищаемой информацией вместе с носителями открытой информации на рабочих столах, оставлять их без присмотра или передавать на хранение другим людям;

– выносить съемные носители с защищаемой информацией из служебных помещений для работы с ними на дому, в гостиницах и т.д., без соответствующего на то разрешения лица, выдавшего съемный носитель.

При отправке или передаче защищаемой информации на съемные носители записываются только предназначенные адресатам данные. Вынос съемных носителей защищаемой информации для непосредственной передачи адресату осуществляется только с письменного разрешения руководителя.

В случае утраты съемных носителей, содержащих защищаемую информацию, либо разглашения содержащихся в них сведений немедленно ставится в известность руководителя. Организуется служебное расследование с оформлением акта и разработкой мер, устраняющих повторный факт утраты съемных носителей. На утраченные носители составляется акт. Соответствующие отметки вносятся в журнал учета машинных носителей конфиденциальной\секретной информации.

Ответственность

Пользователь несет ответственность за:

– неисполнение (ненадлежащее исполнение) своих должностных обязанностей, предусмотренных настоящей должностной инструкцией, в пределах, определенных трудовым законодательством Российской Федерации;

– совершенные в процессе осуществления своей деятельности правонарушения – в пределах, определенных административным, уголовным и гражданским законодательством Российской Федерации;

– невыполнение или ненадлежащее выполнение внутренних приказов, распоряжений и поручений;

– некачественное и несвоевременное выполнение обязанностей, возложенных на него настоящей инструкцией;

– правильность заполнения и ведения всей документации, регламентированной требованиями;

– разглашение информации конфиденциального/секретного характера учреждения.