КОМИТЕТ ПО ДЕЛАМ ОБРАЗОВАНИЯ ГОРОДА ЧЕЛЯБИНСКА

МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«СПЕЦИАЛЬНАЯ (КОРРЕКЦИОННАЯ) ОБЩЕОБРАЗОВАТЕЛЬНАЯ ШКОЛА ДЛЯ ДЕТЕЙ
С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ (НАРУШЕНИЕМ ИНТЕЛЛЕКТА) № 57 г.ЧЕЛЯБИНСКА» (МБОУ
«С(К)ОШ № 57 Г.ЧЕЛЯБИНСКА»)

УТВЕРЖДАЮ
Директор
МБОУ «С(К)ОШ № 57 г.Челябинска»
_____ В.И.Сычёва
«31» 08 2023г.

ИНСТРУКЦИЯ
ПО ОБЕСПЕЧЕНИЮ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.Общие сведения

К защищаемой информации, обрабатываемой в МБОУ «С(К)ОШ № 57 г Челябинска» (далее – ОО), относится информация ограниченного доступа: персональные данные работников и обучающихся, технологическая информация информационных систем, парольная информация, паспорт безопасности.

К информационным системам, которые использует ОО, относятся:

-- централизованные информационные системы города Челябинска (в частности, Комитет по делам образования города Челябинска, МКУ ЦОДОО, отдел ИМСОО);

-- локальные информационные системы ОО.

Допуск пользователей к работе в централизованных информационных системах осуществляется по заявке от руководства ОО. Допуск пользователей к работе в локальных информационных системах осуществляется в соответствии с должностными обязанностями пользователя.

Ответственный за информационную безопасность в ОО назначается из числа администрации приказом директора.

Настоящая Инструкция устанавливает единый порядок обеспечения безопасности информации пользователями при ее обработке с использованием информационных систем и определяет:

-- общие меры обеспечения безопасности информации и правила работы с информацией ограниченного доступа;

-- правила по организации парольной защиты;

-- правила по организации антивирусной защиты;

-- правила по использованию съемных носителей;

-- правила при работе с ресурсами сети Интернет и электронной почтой.

Данная Инструкция обязательна для исполнения всеми пользователями информационных систем в ОО.

Пользователь должен ознакомиться с настоящей Инструкцией под роспись.

2. Требования к уровню подготовки пользователя

Перед началом эксплуатации автоматизированного рабочего места пользователь должен ознакомиться:

-- с положениями настоящего документа;

-- с регламентирующими документами по обеспечению информационной безопасности, принятыми в ОО;

--с руководствами по эксплуатации информационных систем, к которым пользователю предоставлен доступ.

Контроль знания положений нормативных документов по обеспечению информационной безопасности и настоящей Инструкции, а также контроль выполнения требований возлагаются на Ответственного за информационную безопасность.

3. Обязанности пользователя

3.1.Общие положения

Пользователем информационной системы (далее – Пользователь) является лицо, участвующее в процессах автоматизированной обработки информации в информационной системе и имеющее доступ к программному обеспечению и данным, обрабатываемым в этой системе.

Каждый Пользователь несет персональную ответственность за свои действия и обязан:

-- знать и строго соблюдать установленные настоящей Инструкцией правила

обеспечения безопасности информации при работе с программными средствами и средствами защиты информации информационных систем согласно соответствующим инструкциям на данные средства;

-- располагать в помещении экран видеомонитора во время работы так, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;

-- обеспечивать запирание помещения на ключ при выходе всех работников из помещения, в котором осуществляется работа с информационными системами;

-- поддерживать постоянную работу (не отключать (блокировать) средства защиты информации;

-- сообщать ответственному за эксплуатацию информационных систем (программисту) о замеченных нарушениях информационной безопасности (в т. ч. о сбоях в работе средств защиты информации);

-- передавать в случае прекращения трудовых отношений Ответственному за информационную безопасность в ОО все имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

Учитель:

--определяет время и место работы обучающихся в сети Интернет с учетом использования в образовательном процессе соответствующих технических возможностей, а также длительность сеанса работы одного обучающегося;

--наблюдает за использованием обучающимися компьютеров и сети Интернет;

--запрещает дальнейшую работу обучающегося в сети Интернет на уроке (занятии) в случае нарушения им порядка использования сети Интернет и предъявляемых к обучающимся требований при работе в сети Интернет;

--доводит до классного руководителя информацию о нарушении обучающимся правил работы в сети Интернет;

--принимает необходимые меры по пресечению обращений к ресурсам, не имеющим отношения к образовательному процессу.

Ответственный за информационную безопасность:

-- обеспечивает комплексную защиту информации;

--контролирует работ, позволяющих выявить потенциальные угрозы информационной системы и каналы утечки ценных сведений;

-- разрабатывает документацию по защите информации для внутреннего пользования;

-- определяет потребности в технических средствах защиты и контроля;

--проверяет выполнение требований нормативных документов по защите информации.

3.2. Правила работы с информацией ограниченного доступа

Информация ограниченного доступа, не содержащая сведений, составляющих государственную тайну, должна обрабатываться в электронном виде только на рабочих местах, аттестованных по требованиям безопасности информации, предъявляемым ФСТЭК России к таким автоматизированным рабочим местам.

При работе с информацией ограниченного доступа пользователю запрещается:

-- создавать и хранить документы, содержащие информацию ограниченного доступа, в папках, предназначенных для обмена открытыми документами;

-- работать с информацией ограниченного доступа в общественных местах и на рабочих страницах, не оборудованных средствами защиты информации;

-- осуществлять обработку информации на автоматизированном рабочем месте в присутствии лиц, не допущенных к данной информации;

-- оставлять без личного контроля съемные и другие носители информации (в т. ч. и установленные на автоматизированном рабочем месте), распечатки, содержащие информацию ограниченного доступа;

-- записывать на устройства, предназначенные для хранения информации ограниченного доступа, посторонние данные;

-- использовать информацию ограниченного доступа в личных целях, в т. ч. в целях получения выгоды;

-- выносить за пределы контролируемой зоны ОО материальные носители с информацией ограниченного доступа;

-- оставлять без личного контроля включенное автоматизированное рабочее место без активированной блокировки (п. 3.3).

Процедура блокирования доступа к автоматизированному рабочему месту

При необходимости временно прервать работу на автоматизированном рабочем месте для защиты от несанкционированного использования необходимо воспользоваться функцией временной блокировки компьютера, при которой блокируется клавиатура и экран монитора.

Порядок действий при блокировке автоматизированного рабочего места вручную: нажать комбинацию клавиш «Win» (между клавишами «Ctrl» и «Alt») +«L».
Для разблокировки автоматизированного рабочего места пользователю необходимо ввести свой пароль доступа.

3.3.Правила использования паролей

Пользователь должен следовать следующим правилам при использовании паролей, применяемых для доступа к автоматизированному рабочему месту и входу в информационные системы:

-- использовать только свои персональные учетные записи (идентификаторы);

-- обеспечить смену пароля на используемых адресах электронной почты не реже, чем раз в 3 месяца;

-- не использовать одинаковые пароли к разным информационным ресурсам;

-- хранить в тайне свой пароль (пароли), не размещать на рабочем месте документы, содержащие пароль (пароли), не сохранять пароль в браузере и не передавать пароль (пароли) другим лицам;

-- во время ввода пароля необходимо исключить возможность его просмотра посторонними лицами;

-- не оставлять без присмотра автоматизированное рабочее место после ввода пароля.

Пользователь обязан использовать пароли, отвечающие следующим требованиям по парольной защите:

-- длина пароля должна быть не менее 8 символов;

-- пароль должен содержать прописные и строчные буквы, цифры(не менее 2) и специальные символы (@, #, $, &, *, % и т. п.);

-- если информационная система позволяет изменять предустановленный (выданный администратором) пароль, то Пользователь должен сменить пароль на новый при первом входе.

Выбранный пароль не должен поддаваться подбору, поэтому при выборе пароля запрещается:

-- использовать в пароле имя Пользователя (идентификатор) или его часть;

-- использовать идущие подряд символы на клавиатуре и в алфавите (qwerty, 45678, abcdef);

-- использовать распространенные осмысленные слова, общеупотребительные выражения или сокращения, имена собственные (USER, password, system, ADMIN, gfhjkm («пароль» в английской раскладке);

-- использовать три и более повторяющихся символов подряд (ggg254, UUU444).

Пользователь обязан в случае подозрения на компрометацию пароля сообщить об

этом ответственному за эксплуатацию соответствующей информационной системы и произвести смену пароля (самостоятельно, если такая функция доступна пользователю, либо совместно с ответственным).

3.4.Защита от воздействий вредоносных программ

Вредоносный код – любой программный код (компьютерный вирус, троян, сетевой червь), приводящий к нарушению функционирования средств вычислительной техники и/или предназначенный для искажения, модификации, уничтожения, блокирования или несанкционированного копирования информации. Вредоносный код способен создавать свои копии, сохраняющие все его свойства и требующие для своего размножения другие программы, каналы связи или машинные носители.

Возможен следующий характер проявлений действий вредоносного кода:

-- искажение изображения на экране монитора;

-- искажение символов, вводимых с клавиатуры;

-- блокирование клавиатуры, звуковые эффекты;

-- стирание или порча отдельных частей диска или файлов;

-- повреждение загрузочных секторов жесткого диска персонального компьютера и серверов;

-- остановка загрузки или зависание компьютера, значительное замедление его работы;

-- уничтожение или искажение информации о системной конфигурации персонального компьютера и серверов.

В целях обеспечения защиты от воздействий вредоносного кода Пользователю автоматизированного рабочего места запрещается:

-- самостоятельно устанавливать программное обеспечение, в том числе командные файлы;

-- использовать при работе «зараженный» вредоносным кодом либо с подозрением на «заражение» носитель информации и/или файл;

-- использовать личные носители информации на автоматизированном рабочем месте;

-- использовать служебные носители информации на домашних компьютерах и в неслужебных целях;

-- самостоятельно отключать, удалять и изменять настройки установленных средств защиты информации.

Пользователь автоматизированного рабочего места обязан проводить контроль на отсутствие вредоносных программ любых сменных и подключаемых носителей (дискет, CD-дисков, DVD-дисков, Flash-памяти) и открываемых архивов (ZIP, RAR и др.).

3.5.Правила обращения со съемными носителями

Пользователь использует съемные носители информации только в случаях, когда это необходимо для выполнения трудовых (служебных) обязанностей. При использовании съемных носителей Пользователь обязан:

-- использовать съемные носители исключительно для выполнения трудовых обязанностей и не использовать в личных целях;

-- обеспечивать физическую безопасность съемных носителей;

-- обеспечивать проверку отсутствия вредоносного программного обеспечения на съемных носителях;

-- извещать Ответственного за организацию обработки персональных данных в ОО о фактах утери съемных носителей, содержавших персональные данные работников и (или) обучающихся;

-- не передавать съемные носители третьим лицам при отсутствии в этом производственной необходимости;

-- не оставлять съемные носители без присмотра.

3.6.Использование электронной почты и ресурсов сети Интернет

При использовании электронной почты Пользователям запрещается:

-- пересылать информацию ограниченного доступа с использованием общедоступных почтовых сервисов (Яндекс, Рамблер, Mail.ru, Google и другие);

-- открывать вложения подозрительных электронных сообщений: сообщений от незнакомых отправителей; сообщений, содержащих исполняемые файлы (EXE, COM, BAT); сообщений рекламного, развлекательного, оскорбительного характера;

-- переходить по ссылкам на сайты из подозрительных электронных сообщений, в том числе сообщений, содержащих приглашения «открыть», «запустить», «посетить», «нажать», «перейти»;

-- отправлять электронные письма от имени других работников ОО, если иное не определено их служебными обязанностями;

-- предпринимать попытки несанкционированного доступа к почтовым ящикам других работников ОО.

При использовании ресурсов сети Интернет Пользователям запрещается:

-- использовать для обмена информацией ограниченного доступа сайты, предоставляющие услуги хранения и обмена информацией;

-- размещать, публиковать информацию ограниченного доступа на общедоступных ресурсах;

-- загружать из сети Интернет программное обеспечение и устанавливать его на автоматизированные рабочие места;

-- предпринимать попытки к получению несанкционированного доступа к ресурсам сети Интернет, в том числе использовать специализированные средства для обхода блокировок ресурсов, установленных поставщиком услуг связи.

3.7.Порядок действий в случае возникновения нештатных ситуаций

При возникновении нештатных ситуаций, связанных с использованием информационных систем, а также в случаях:

-- подозрения на компрометацию (утерю, разглашение, несанкционированное копирование или использование) личных паролей;

-- подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.);

-- обнаружения фактов совершения в отсутствие пользователя попыток несанкционированного доступа к техническим средствам и носителям информации (следов вскрытия, измененного состава подключенных устройств, кабелей, в том числе отводов кабелей);

-- невозможности запуска средств защиты информации или при ошибках в процессе их выполнения;

-- несанкционированных изменений в конфигурации программного обеспечения;

-- отклонений в нормальной работе программного обеспечения, затрудняющих эксплуатацию автоматизированного рабочего места;

-- обнаружения ошибок в программном обеспечении, пользователь обязан обратиться с описанием проблемы к программисту МБОУ «С(К)ОШ № 57 г Челябинска», ответственному за эксплуатацию соответствующей информационной системы в ОО, и, при необходимости, в службу технической поддержки информационной системы.

4. Ответственность пользователя

Пользователь несет персональную ответственность за надлежащее исполнение

своих обязанностей, а также сохранность технических средств автоматизированного рабочего места, съемных носителей информации, электронных идентификаторов и целостность установленного программного обеспечения.

Пользователь, виновный в нарушениях, несет ответственность, предусмотренную действующим законодательством Российской Федерации.

Лист ознакомления

№ п/п	Ф.И.О.	Должность	Подпись	Дата
