ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ

Государственное бюджетное профессиональное образовательное учреждение города Москвы «Первый Московский Образовательный Комплекс»

УТВЕРЖДАЮ
Директор ГБПОУ «1-й МОК»
_____ Ю.Д. Мироненко
«25» 11 2021 г.

Система менеджмента качества

ИНСТРУКЦИЯ ПОЛЬЗОВАТЕЛЯ

по обеспечению безопасности персональных данных при их обработке в информационной системе

Экземпляр № _____

Содержание

1.Общие сведения

1.1. Настоящая Инструкция (далее – Инструкция) устанавливает единый порядок обеспечения пользователями безопасности персональных данных и иной защищаемой информации при их 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.

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

Пользователь должен ознакомиться с Инструкцией под роспись.

1.3.К защищаемой информации, обрабатываемой в ГБПОУ «1-й МОК» (далее – ОО), относится информация ограниченного доступа – персональные данные работников и обучающихся, технологическая информация информационных систем, парольная информация.

1.4. К информационным системам, использующимся в ОО, относятся:

– информационные системы Правительства Москвы (в том числе Департамента образования и науки города Москвы и Департамента информационных технологий города Москвы, далее – централизованные ИС);

– локальные информационные системы ОО (далее – локальные ИС).

1.5.Допуск пользователей к работе в централизованных ИС осуществляется по заявке от руководства ОО и (или) ответственного за эксплуатацию системы. Допуск пользователей к работе в локальных ИС осуществляется в соответствии с должностными обязанностями пользователя.

1.6. Инструкция составлена с учетом требований МС ISO (9001:2008) системы менеджмента качества ГБПОУ «1-й МОК», Политикой и Целями в области качества.

2.Требования к уровню подготовки пользователя

2.1. Перед началом эксплуатации автоматизированного рабочего места пользователь должен ознакомиться:

– с положениями Инструкции;

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

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

2.2. Контроль знания требований нормативных документов по обеспечению информационной безопасности и настоящей Инструкции, а также контроль выполнения указанных требований возлагаются на ответственного за организацию обработки персональных данных в ГБПОУ «1-й МОК» (далее – Ответственный).

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 информации, обрабатываемой в этой системе.

Пользователь обязан:

– знать и строго соблюдать установленные Инструкцией правила обеспечения безопасности информации при работе с программными средствами и средствами защиты информации информационных систем согласно соответствующим инструкциям на данные средства;

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

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

– не отключать (блокировать) средства защиты информации;

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

– при прекращении трудовых или гражданско-правовых отношений с ООм передать ответственному за организацию обработки персональных данных в ОО имеющиеся в пользовании материальные носители информации, содержащие информацию ограниченного доступа.

3.2.Правила работы с информацией ограниченного доступа

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 станциях, 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.

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.

3.4.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);

– хранить в тайне свой пароль (пароли), не размещать на рабочем месте документы, содержащие пароль (пароли), 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;

– в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры 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 на клавиатуре и/или в алфавите символы (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).

При создании нового пароля необходимо обеспечить отличие вновь созданного пароля минимум на 1 символ от предыдущего. Запрещается использование последнего использованного пароля при создании нового пароля.

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).

3.5.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 персональной электронно-вычислительной машины и серверов;

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

– уничтожение или искажение информации о системной конфигурации персональной электронно-вычислительной машины 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.).

3.6.Правила обращения со съемными носителями

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

– использовать их исключительно для выполнения трудовых обязанностей и не использовать в личных целях;

– обеспечивать их физическую безопасность;

– обеспечивать проверку отсутствия на них вредоносного программного обеспечения;

– 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.

3.7.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, Департаментом информационных технологий города Москвы и/или инженером по автоматизации (техником) ОО.

3.8.Порядок действий в случае возникновения нештатных ситуаций

В случае возникновения нештатных ситуаций (инцидентов) пользователь обязан обратиться с описанием проблемы к инженеру по автоматизации (технику), ответственному за эксплуатацию соответствующей информационной системы в ОО и при необходимости - в службу технической поддержки информационной системы 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.

4.Ответственность пользователя

4.1.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.

4.2.Пользователи, виновные в нарушениях требований Инструкции, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством Российской Федерации.