

Обеспечение безопасности ПДн при их обработке в информационной системе

ГАОУ СО «Гимназия № 1»

**На основании письма
Министерства образования СО
от 19.04.2023 № 01-26/2573**

Инструкция пользователя по обеспечению
безопасности персональных данных при их
обработке в информационной системе

Обязанности пользователя

- экран видеомонитора в помещении располагать во время работы так, чтобы исключить возможность несанкционированного ознакомления с отображаемой на нем информацией посторонними лицами;
- при выходе всех работников из помещения, в котором осуществляется работа с информационными системами, обеспечить запираение помещения на ключ;
- не отключать (блокировать) средства защиты информации;
- сообщать ответственному за эксплуатацию информационных систем (системному администратору) о замеченных нарушениях информационной безопасности (в т. ч. о сбоях в работе средств защиты информации).

Правила работы с информацией ограниченного доступа

- 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

Процедура блокирования доступа к автоматизированному рабочему месту

нажать комбинацию клавиш

«Win»

+

«L»

Правила использования паролей

- 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 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).

Защита от воздействий вредоносных программ

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

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

Использование электронной почты

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;

Использование ресурсов сети Интернет

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, системным администратором ОО.

Порядок действий в случае возникновения нештатных ситуаций

пользователь обязан обратиться с описанием проблемы к системному администратору ОО, ответственному за эксплуатацию соответствующей информационной системы в ОО