Информационная безопасность образовательных учреждений: правила и рекомендации

Информационные технологии широко вошли в практику современных образовательных организаций. С одной стороны, они оказывают существенную помощь педагогам в организации рабочего процесса, повышают качество учебно-воспитательной работы. С другой стороны, являются источником большого количества угроз. Поэтому в цифровую эпоху проблема информационной безопасности становится одной из наиболее актуальных, в том числе для образовательных учреждений.

Политика информационной безопасности образовательного учреждения должна включать не только разумное и безопасное использование современных технологий в образовательном процессе, но и обеспечивать сохранность конфиденциальных данных всех его участников.

Источником угроз информационной безопасности могут стать как внешнее воздействие (например, злоумышленники, вирусы), так и необдуманные действия, ошибки самих пользователей. Соблюдение базовых правил позволяет минимизировать риски нарушения информационной безопасности в рамках образовательной организации. К таким правилам можно отнести следующие:

1. Используйте программные средства защиты информации

На всех устройствах должны быть установлены [антивирусные программы](#). Они помогают обнаруживать и предотвращать утечки данных, а также защищать систему от внешних угроз, таких как вирусы. Важно периодически производить полную проверку устройства антивирусом (не реже чем раз в месяц).

2. Перед началом работы с внешним носителем (флешкой, жестким диском и т.д.) проверьте его на наличие вредоносной программы

Довольно часто заражение компьютера происходит через съемные внешние носители. Особенно это актуально для образовательных организаций. Поэтому сначала необходимо проверить внешний носитель антивирусной программой и лишь потом приступать к работе.

3. Регулярно делайте резервные копии важных данных

Создание копий позволяет предотвратить полную утрату данных вследствие различных угроз, в том числе непредсказуемых (например, аварий, сбоев, поломок). Одна из наиболее удобных и общепринятых стратегий резервного копирования предлагает придерживаться следующей схемы: создавайте не менее 3 копий каждого файла, храните копии файлов как минимум на 2 разных типах носителей, 1 копию данных следует хранить в удаленном месте (например, в облачном хранилище)

4. Создавайте сложные и уникальные пароли

Надежный пароль должен быть не только длинным (8-12 символов), но и сложным (состоять из цифр, букв разного регистра, специальных символов). Меняйте пароли как минимум раз в квартал (а лучше раз в месяц). Паролями необходимо защитить не только доступ к рабочим веб-ресурсам, но и сам рабочий компьютер (ноутбук).

5. Соблюдайте политику "чистого" рабочего стола и экрана

Не храните и не оставляйте на рабочем столе конфиденциальные данные, храните их в надежном месте (желательно запирающимся на ключ). Для утилизации конфиденциальных документов (например, ксерокопий договоров и документов) используйте шредер.

Не храните пароли в электронном виде на рабочем столе, не стоит держать записанные пароли в общедоступных местах, не сообщайте пароли коллегам и другим третьим лицам.

Не оставляйте компьютер без присмотра с авторизацией в информационных системах. Всегда закрывайте активные сеансы по завершении работы. Покидая рабочее место, всегда блокируйте экран рабочего устройства (ноутбука, компьютера, планшета).

6. Будьте внимательны при работе в Интернете

Не станьте жертвой фишинга – интернет-мошенничества, чаще всего представляющего выдачу поддельных сайтов, рассылку электронных писем или сообщений, содержащих вредоносные ссылки и файлы. Цель фишинга – кража конфиденциальных данных, в первую очередь паролей. Следуйте следующим правилам:

- Внимательно проверяйте адреса сайтов в адресной строке, пользуйтесь исключительно сайтами с защищённым протоколом https;
- При осуществлении служебной переписки используйте только рабочую электронную почту, внимательно проверяйте правильность написания адреса отправителя и получателя (даже тех, с кем вы переписываетесь ежедневно);
- На любой подозрительный запрос по электронной почте необходимо использовать альтернативный канал связи (например, телефон), чтобы подтвердить запрос у адресата;
- Не переходить по ссылкам в подозрительных письмах электронной почты
- Не открывайте и не скачивайте прикрепленные к подозрительному письму файлы.

7. Берегите персональные данные

Помните, что обработка, передача и распространение персональных данных допускается только с согласия субъекта или его законных представителей. Поэтому перед публикацией в общий доступ персональных данных (например, фотографий, результатов аттестаций, иных материалов, содержащих ФИО, класс и иную персональную информацию), необходимо получить согласие родителей ребенка на обработку и на размещение их в сети Интернет.

Не используйте мессенджеры для передачи документов и другой личной информации. В частности, не стоит выкладывать в общую беседу список с именами детей в сочетании с оценками, паролями и логинами от электронных дневников и другой информацией.