

Базовые требования соблюдения информационной безопасности на рабочих местах

Подготовлено с использованием материалов сайта компании «Лаборатория Касперского»

Доступ к ресурсам и сервисам, обеспечивающим функции образовательной организации

1. **Используйте только сложные пароли:** они должны быть не менее 12 знаков длиной, не состоять из словарных слов, содержать спецсимволы и цифры. Если пароль простой, злоумышленник удаленно с помощью специальных программ сможет подобрать его простым перебором.
2. **Пароли должны быть уникальными:** не используйте один и тот же пароль для всех рабочих ресурсов. Тем более — не используйте его же и в личных целях. Достаточно будет утечки из одного из сервисов, чтобы скомпрометировать в этом случае доступ ко всем ресурсам.
3. **Пароли должны быть секретными:** не записывайте пароль на бумаге и не храните около рабочего места; не вписывайте их в файлы и не делитесь ими с коллегами. Иначе случайный посетитель или уволившийся сотрудник сможет воспользоваться таким паролем.
4. **Если сервис позволяет включить двухфакторную аутентификацию, включите ее.** Это не позволит злоумышленнику получить доступ к сервису даже в случае утечки пароля.

О важности персональных данных

1. **Не передавайте файлы с персональными данными по электронной почте или по открытым каналам** (например, через Google Docs по прямой ссылке или через публичные файлохранилища).
2. **Не делитесь персональными данными, к которым Вы по своим обязанностям имеете доступ,** с коллегами, чьи рабочие функции не требуют такого доступа, с посторонними лицами, с обучающимися.

О самых распространенных киберугрозах

1. **Тщательно проверяйте ссылки в письмах, прежде чем по ним переходить.** Убедительно выглядящее имя отправителя — не гарантия подлинности. Злоумышленники могут попробовать подsunуть фишинговую ссылку, особенно если им удастся захватить почту кого-то из ваших коллег.
2. **Убедитесь, что на всех рабочих компьютерах подключена автоматическая проверка антивирусом при подключении USB устройств** (флеш-накопители, карты памяти, переносные жесткие диски, телефоны сотрудников через USB). При настройке антивируса установите отключение автозапуска любой информации с подключаемых через USB устройств. Не подключайте к рабочему компьютеру любые сторонние флеш носители.
3. **Не открывайте и не запускайте любые файлы из непроверенного источника** (например, присланные по почте). При открытии файла всегда нужно смотреть, не является ли он исполняемым (злоумышленники часто маскируют вредоносные файлы под офисные документы). Любой присланный по почте файл необходимо сначала сохранить в папку, выделенную на локальном компьютере для файлов, которые не проверены антивирусом, затем, не открывая его, запустить проверку на вирусы в этом файле.

Ссылки на полезные ресурсы

Инструкция по информационной безопасности для новых сотрудников
<https://www.kaspersky.ru/blog/security-awareness-basic-instruction/30980/>

Как создавать сложные пароли <https://www.kaspersky.ru/blog/use-strong-passwords/22732/>

Почему нельзя использовать один и тот же пароль для нескольких сервисов
<https://www.kaspersky.ru/blog/never-reuse-passwords-story/21823/>

Что такое BEC-атака и как ей противостоять (методы получения доступа к электронной почте сотрудников организации, основанные на технологических и социальных методах мошенничества) <https://www.kaspersky.ru/blog/what-is-bec-attack/27623/>