Список рекомендаций по обеспечению безопасности личных данных при работе с компьютером.

# Пароли.

# «Лентяйские» пароли

Пароль не должен быть «лентяйским». Очень часто, из-за опасения забыть пароль или из-за нежелания придумывать сложные комбинации букв, цифр и специальных символов, пользователи используют в качестве пароля ряд знаков записанных в алфавитном порядке или в той последовательности, в которой они даны на клавиатуре (например йцукен, qwerty, 12345, абвгд, abcd, 54321, ytrewq и т.п.). Такие пароли очень легко подбираются злоумышленниками и не дают в сущности никакой защиты.

# Шифрование паролей

Пароль нужно шифровать, так как программы, подбирающие пароли используют слова из словарей. Выработайте несколько правил, с помощью которых вы могли бы превратить словарное слово в комбинацию букв, цифр и специальных символов. Например можно заменять в словарном слове некоторые буквы: password = P@sSw0Rd.

# Сложность шифра и длина пароля

Придуманные вами правила должны обеспечивать достаточную защиту. Такой шифр, как простое чередование прописных и строчных букв не даст требуемой надежности, так как его легко подобрать. Сложный шифр подразумевает использование специальных символов и цифр. Длина пароля также имеет большое значение. Чем длиннее пароль, тем труднее его подобрать (к сожалению и запомнить тоже…). Оптимальная длина пароля на наш взгляд составляет 8-12 символов, хотя наиболее важные данные можно защищать и более длинными паролями.

# Одинаковые пароли и рекомендации по хранению

Нельзя использовать одинаковые пароли на разных серверах/устройствах, так как в таком случае злоумышленник, подобрав один пароль, получит доступ ко всем вашим данным. Поскольку паролей может быть довольно много, удержать их в памяти будет непросто. Запишите придуманные вами пароли на бумаге и храните их отдельно от компьютера в таком месте, куда никто посторонний не имеет доступа. Никогда не наклеивайте бумажки с паролями на монитор, клавиатуру, на чехол смартфона или планшета, или на стену рядом с компьютером, так как в этом случае они могут быть доступны очень многим и смысл такой защиты будет потерян. Также не рекомендуется класть бумажки с паролями под клавиатуру или где-то рядом с компьютером, так как в таких местах их легко найти.

# Ввод паролей в общественных сетях

Большинство публичных сетей, таких как WiFi-сети в общественном транспорте или в кафе, являются открытыми. Данные, передаваемые по таким сетям, не шифруются и поэтому могут стать легкой добычей киберпреступников, способных с помощью специальных программ перехватывать ваши информационные потоки. Не шифруются в том числе и вводимые вами пароли. Да, именно так, в публичных сетях ваши пароли передаются в открытом виде, поэтому, пользуясь, например, интернет-банкингом в метро вы рискуете потерять свои деньги!

# Дополнительные сведения.

# Обновления

Злоумышленники постоянно тестируют программное обеспечение в поисках уязвимостей, которые позволили бы им осуществлять свои атаки. Также над поиском уязвимостей трудятся и сами разработчики программ. При обнаружении потенциальных проблем, компании-производители программного обеспечения выпускают обновления, в которых часто закрываются возможные «лазейки» для хакеров. Поэтому, если вы заботитесь о безопасности, необходимо регулярно проверять установленные на ваших устройствах программы на наличие обновлений и устанавливать их.

# Незнакомые приложения

Наиболее часто используемый способ распространения вирусов состоит в том, чтобы спровоцировать пользователя запустить вредоносное программное обеспечение на своем устройстве. Чтобы эта беда не случилась с вами, категорически не рекомендуется:

- Устанавливать непроверенные приложения с незнакомых сайтов;  
- Переходить по непроверенным ссылкам;  
- Открывать непроверенные документы или документы от неизвестных отправителей;  
- Открывать неизвестные или непроверенные вложения в письмах электронной почты.  
  
Невыполнение этих правил может привести к установке вредоносного программного обеспечения на ваши устройства.

# Средства защиты от кибератак.

# Антивирусы.

Настоятельно рекомендуется установить антивирусное программное обеспечение на все используемые (а в идеале и на неиспользуемые, но которые могут быть использованы в будущем) устройства. Антивирус должен выполнять проверку в реальном времени (в таком режиме проверяются все работающие, устанавливаемые и запускаемые программы, загружаемые файлы и т.п.). Антивирусное программное обеспечение необходимо регулярно обновлять, так как злоумышленники постоянно ищут новые способы атак и пишут новые версии вредоносных программ. Обязательно периодически (не реже одного раза в неделю) проводить полную проверку всех устройств на наличие вредоносного программного обеспечения. Такую проверку можно настроить в автоматическом режиме по расписанию в большинстве современных антивирусных программ. Желательно быть в курсе новостей в области антивирусного программного обеспечения, чтобы использовать современные и надежные программы. Кроме того, установленное антивирусное программное обеспечение должно реализовывать функции онлайн-защиты при работе в Интернет (например McAfee Web Advisor или Kaspersky Internet Security). Такая защита должна быть включена постоянно и предупреждениями, которые выдаются средствами онлайн-защиты при работе в сети, нельзя пренебрегать.

# Firewall.

Современные программы для защиты от кибератак представляют собой комплексы, имеющие в своем составе брандмауэр (например McAfee Live Safe или Kaspersky Total Security). Если у вас установлен такой комплекс, специальных действий по настройке межсетевого экрана, как правило, не требуется. Если брандмауэра у вас нет, его настоятельно рекомендуется установить. Компьютеры без брандмауэров представляют собой идеальную мишень для хакерских атак. Как показывает практика, в среднем за неделю на компьютере, подключенном к сети интернет, блокируется несколько сотен нежелательных подключений. Многие производители антивирусного программного обеспечения предлагают брандмауэры как в виде отдельных продуктов, так и в составе комплексной защиты устройств.

Оглавление

[1 Пароли. 1](#_Toc496442066)

[1.1 «Лентяйские» пароли 1](#_Toc496442067)

[1.2 Шифрование паролей 1](#_Toc496442068)

[1.3 Сложность шифра и длина пароля 1](#_Toc496442069)

[1.4 Одинаковые пароли и рекомендации по хранению 1](#_Toc496442070)

[1.5 Ввод паролей в общественных сетях 1](#_Toc496442071)

[2 Дополнительные сведения. 2](#_Toc496442072)

[2.1 Обновления 2](#_Toc496442073)

[2.2 Незнакомые приложения 2](#_Toc496442074)

[2.3 Средства защиты от кибератак. 2](#_Toc496442075)

[2.3.1 Антивирусы. 2](#_Toc496442076)

[2.3.2 Firewall. 3](#_Toc496442077)