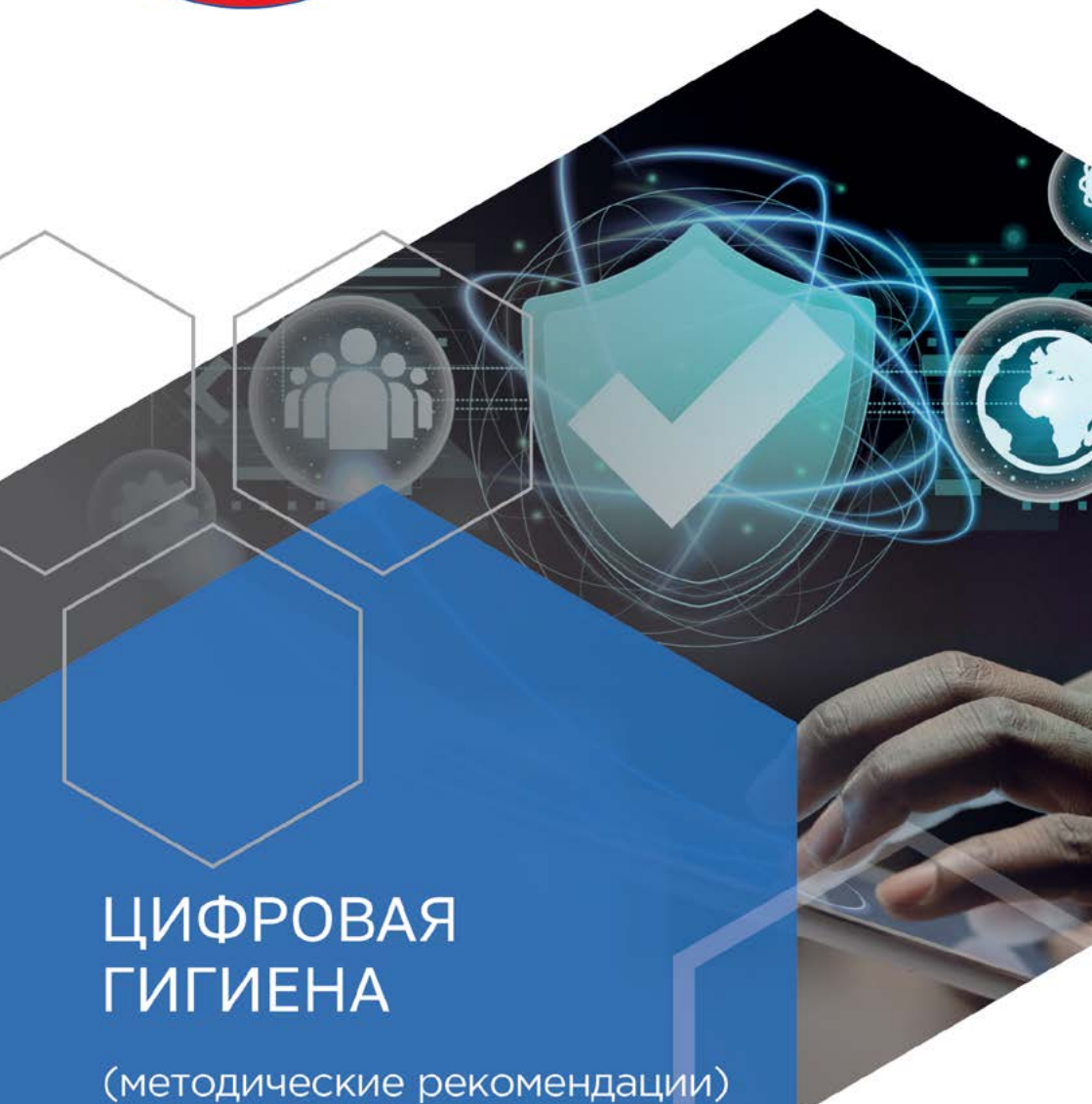
ОБЩЕРОССИЙСКИЙ ПРОФЕССИОНАЛЬНЫЙ СОЮЗ РАБОТНИКОВ НЕФТЯНОЙ, ГАЗОВОЙ ОТРАСЛЕЙ ПРОМЫШЛЕННОСТИ И СТРОИТЕЛЬСТВА



ЦИФРОВАЯ ГИГИЕНА

(методические рекомендации)

Москва
2024

НЕФТЕГАЗСТРОЙПРОФСОЮЗ
РОССИИ

Цифровая гигиена – это свод правил, следуя которому, пользователь обеспечивает себе минимальную информационную безопасность.

В данном методическом пособии приведен базовый набор таких правил.

Базовая безопасность

1. Используйте разные пароли для входа в разные системы. Не используйте везде один и тот же пароль.

Правила:

• Пароль должен состоять минимум из 8 символов.

• Обязательно использование комбинации букв, цифр и специальных символов (! ” № и т.д.)

Совет: Используйте следующую схему и Вам не придется запоминать пароли для каждой системы:

• Придумайте основу пароля, которую никогда не забудете. Это будет начало всех паролей. Например: PavLiC

• Выберите спецсимвол и цифру, которые Вы будете добавлять после основы пароля. Например: &3

• При создании пароля в конце добавляйте 3 символа из названия системы, для которой создается пароль.

Например:

– для vkontakte.ru - PavLiC&3vko

– для odnoklassniki.ru - avLiC&3odn

– для mail.ru - PavLiC&3mai

В последующем, если система принудит к изменению пароля по сроку (у разных систем могут быть разные регламенты, но, как правило, это происходит раз в 6 месяцев), Вы сможете изменить только спецсимволы, при этом сохранив общую логику построения пароля.

2. Не храните в «виртуальном облаке» сканы и документы с персональными данными.

Подсказка: Если Вам необходимы цифровые копии документов, лучше храните их на флеш-карте, которая будет на брелоке с ключами или вовсе рядом со стационарным компьютером, с которого Вы обычно отправляете сканы документов.

3. Не делитесь слишком личной информацией в социальных сетях.

Пояснение: Всему миру не нужно знать кличку Вашего домашнего животного, так как это может быть секретным вопросом от Вашей же почты. Секретные вопросы лучше придумывать такие, на которые точно никто кроме Вас не знает ответа.

4. При необходимости авторизации использования чужого устройства для веб-серфинга (ноутбук, моноблок и т.д.) используйте режим инкогнито.

Настройки электронной почты

Электронная почта сегодня стала неотъемлемой частью нашей жизни, особенно на работе. Однако обработка большого количества писем может быть утомительной и занимать много времени. Вот несколько лайфхаков и настроек, которые помогут Вам гораздо быстрее и эффективнее работать с почтой.

1. Создайте группы для писем

Группы – отличный способ организации почты и сокращения времени на поиск нужного письма. Вы можете создать группу для писем, связанных с определенным проектом или событием. Это позволит Вам быстро найти нужное письмо, а также поможет легко отслеживать все письма.

2. Используйте «+» в адресе

Подавляющее большинство почтовых серверов не учитывают символы после «+»: письма, отправленные на primer+spam@domain.ru и primer+rassylka@domain.ru, все равно придут на адрес primer@domain.ru. Это может быть полезно, если Вы хотите создать несколько адресов для различных целей, но не хотите создавать отдельный почтовый ящик для каждого из них.

Вы можете использовать этот метод, чтобы легко фильтровать письма, связанные с определенными проектами, клиентами или задачами. Например, Вы можете создать фильтр, который автоматически перенаправляет все письма, отправленные на адрес primer+podryad@domain.ru, в папку «Подрядчики».

Вариаций может быть неограниченное количество.

3. Используйте фильтры

Фильтры – отличный способ автоматизации обработки почты. Например, Вы можете создать фильтр, который автоматически перенаправляет все письма от руководства в папку «Важное», чтобы Вы не пропустили важную информацию.

4. Оптимизируйте настройки уведомлений

Уведомления электронной почты могут отвлекать Вас от работы и занимать много времени. Однако Вы можете оптимизировать настройки уведомлений, чтобы получать только важные уведомления. Например, Вы можете настроить уведомления только для писем от определенных контактов или только для писем, помеченных как «Важные».

5. Используйте быстрые ответы

Быстрые ответы – это заранее написанные ответы на часто задаваемые вопросы. Вы можете создать несколько быстрых ответов и использовать их для быстрой и эффективной обработки почты. Например, если Вы часто

получаете письма с вопросами о Вашей компании, то можете создать «быстрый ответ» с информацией о компании и использовать его для быстрой отправки ответа.

6. Используйте отложенную отправку

Отложенная отправка – это отличный способ управления временем и эффективной работы с почтой. Вы можете написать письмо заранее и настроить его на отправку в определенное время. Например, если Вы хотите отправить письмо в конце рабочего дня, то можете настроить его на отправку в 17:00.

Обновление программного обеспечения

Любой программный продукт требует периодического обновления. Чем популярнее программа, тем больше число злоумышленников, систематически работающих над поиском уязвимостей в ней.

Следует понимать, что невозможно написать идеально защищенную программу, особенно в текущих реалиях: подавляющее большинство ПО не обладает изолированным кодом и постоянно взаимодействует со сторонними сервисами для обмена данными. Каждая подобная «точка входа» является потенциальной уязвимостью.

В качестве профилактики выполняйте следующие рекомендации:

• без необходимости не производите на телефоне Rooting (Android), Jailbreak (Apple iOS), HardSPL (Windows Phone)[1] ;

• обновляйте мобильные приложения по мере получения уведомлений от разработчика;

• при обновлении программ на компьютере / ноутбуке пользуйтесь автоматическим обновлением или загружайте обновления только с сайта производителя;

• периодически обновляйте прошивку на вашем роутере;

• не забывайте об обновлении «умных устройств» (умные колонки, бытовая техника и устройства с выходом в интернет);

• при необходимости обновления специализированных / прикладных программ (например, 1С Предприятие) обязательно предварительно проконсультируйтесь с IT-специалистом.

«Пиратское» программное обеспечение

В связи с уходом ряда ведущих поставщиков ПО с российского рынка возникает соблазн использования «ломаного софта». Зачастую именно

---

[1]*Rooting / Jailbreak / HardSPL – процесс получения прав суперпользователя на устройствах. Основными целями являются снятие ограничений производителя либо оператора связи, манипулирование системными приложениями и возможность запуска приложений, требующих прав администратора.*

такие продукты являются источником заражения операционной системы.

Необходимо понимать, что нередко в комплексе с «кряком» пользователь, не осознавая того, своими руками устанавливает вредоносное ПО и предоставляет ему полные права, исключая из сканирования антивирусом.

Не обязательно негативное воздействие будет проявляться сразу после попадания в систему. Злоумышленник в состоянии настроить работу программы таким образом, что пользователь долгое время не сможет распознать заражение.

За время скрытого нахождения в системе программа злоумышленника соберет достаточно информации, чтобы при единовременной передаче данных снабдить создателя всем необходимым для нанесения максимального ущерба.

В целом даже без получения платежных реквизитов банковских карт злоумышленник в силах монетизировать полученную информацию.

Например: Идентифицировав жертву и получив доступ к аккаунтам социальных сетей, возможно инициировать сбор денежных средств для якобы находящихся в тяжелом состоянии родственников. Сопроводив данные посты сканами реальных паспортов и используя другую конфиденциальную информацию, злоумышленник проведет «идеальную» атаку.

Фактически вариантов подобных атак – бесконечное множество.

Без крайней необходимости НИКОГДА не используйте взломанные версии лицензионного программного обеспечения.

Фишинг

Фишинг — вид кибермошенничества, целью которого является получение доступа к конфиденциальным данным пользователей: логинам и паролям, платежным реквизитам банковских карт.

Поскольку фишинг базируется на социальной инженерии, защита от него ложится в основном на обычного пользователя. Действия злоумышленника направлены на побуждение пользователя к самостоятельной передаче необходимых данных на поддельной странице.

Как защититься:

1. Разделите почтовые ящики:

– Отдельный email для подписок, акций и регистрации в интернет-магазинах;

– Личный ящик для важных и личных писем;

– Не используйте рабочий email для регистрации без крайней необходимости.

Таким образом Вы заведомо отделите потенциально опасные письма.

2. Ставьте под сомнение каждое письмо с почтовыми вложениями и ссылками:

перед переходом по ссылке и открытии вложения удостоверьтесь, что письмо пришло от ожидаемого отправителя.

Также посимвольно проверьте домен ссылки из письма: мошенники часто используют похожие адреса типа «odnoklsssniki.ru».

3. Не спешите реагировать на письма с «провокационными» заголовками.

Зачастую, чтобы гарантированно привлечь внимание пользователя, фишеры используют заголовки типа «Подтверждение списания с банковского счета» или «Начисление штрафа за неуплату налогов».

Практически все подлинные сообщения организаций содержат в себе упоминание некой информации, недоступной для фишеров. Подозрительны любые письма, не содержащие какой-либо конкретной личной информации.

Проанализируйте, есть ли предпосылки для получения подобных писем. Свяжитесь с организацией, от имени которой пришло письмо, по номеру телефона из альтернативного источника (например: Яндекс.Карты).

4. Вместо перехода по ссылке из письма – введите веб-адрес в адресную строку браузера самостоятельно.

5. Не переходите по подозрительным ссылкам, которые также распространяются через социальные сети и мессенджеры.

Банкоматы: скиммеры и шиммеры

Наличные деньги постепенно уходят из повседневной жизни, но все же нам по-прежнему приходится взаимодействовать с банкоматами. Несмотря на то что Ваша банковская карта защищена сразу несколькими технологиями, шанс потерять с нее все средства остается. Чтобы этого не произошло, проявляйте должную бдительность.

Одним из способов воровства денег с карт является скимминг[2] . Основой данного способа является монтирование на щель картоприемника банкомата специальной накладки, которая считывает магнитную ленту банковской карты и пересылает данные хозяину устройства. Как правило, такие накладки используются в паре со скрытой камерой, направленной на клавиатуру для ввода пин-кода.

В российских условиях скимминг практически не прижился в силу низкой распространенности терминалов оплаты, использующих магнитную ленту, и в целом использования более продвинутых моделей банко-

---

[2]*Скимминг (от англ. skim – быстро читать) – метод кражи данных банковской карты с использованием специальных технических устройств, несанкционированно вмонтированных в банкомат.*

матов. Несмотря на это, рекомендуем всякий раз проверять банкомат по следующим параметрам:

– проверьте картоприемник на наличие накладки: попробуйте его оторвать;

– проверьте все выступающие панели – фальшивые плохо держатся;

– если клавиатура кажется Вам избыточно выпуклой или отличающейся по цвету / тону, попробуйте ее поддеть.

Не стесняйтесь проверять панели банкомата!

В последние годы набирает обороты более продвинутая технология с использованием шиммера[3]. Шиммер устанавливается внутрь картоприемника, и снаружи его обнаружить невозможно. До сих пор использование шиммеров было не слишком распространено в силу дороговизны изготовления устройства и высоких рисков быть замеченным при его установке в банкомат.

Несмотря на это, стоит следовать следующим правилам:

– по возможности не пользуйтесь картоприемником – все современные банкоматы позволяют использовать карту бесконтактно;

– избегайте банкоматы, установленные на улице, старайтесь пользоваться теми, что находятся под постоянным наблюдением.

Использование публичных Wifi сетей

Все больше общественных мест, кафе и транспорта открывает в публичный доступ свои Wi-Fi сети. Часто для выхода для бесплатного Wi-Fi даже не нужен пароль. Несомненно, это удобно для пользователей, но каждая такая точка доступа является потенциальным источником цифровой инфекции.

Киберпреступники давно научились эксплуатировать подобные публичные Wi-Fi для достижения своих целей: собирать логины и пароли, а также другие личные данные в общественных местах можно в промышленных масштабах.

Проявляйте должную бдительность:

1. Не доверяйте точкам доступа в интернет, которые не закрыты паролем

Чаще всего именно такие сети используют для воровства конфиденциальных данных пользователей.

2. Выключайте Wi-Fi, если Вы им не планируете пользоваться

---

[3]Шиммер (от англ. shim – клин, тонкая прокладка) – это тонкая прокладка, которая располагается между чипом на карте и считывающим устройством чипов в банкомат или терминале и записывает данные с чипа, когда их считывает терминал.

Во-первых, это сэкономит заряд батареи. Во-вторых, не позволит следить за Вами: включенный модуль Wi-Fi периодически отправляет в эфир свои идентификационные данные (MAC-адрес). Таким образом вполне можно составить маршрут вашего передвижения. Как правило, подобный прием используют крупные компании для внутренних исследований с целью повышения маркетинговых мероприятий. Но данная информация может использоваться и злоумышленниками.

3. Отключите функцию автоматического подключения к Wi-Fi на телефоне и планшете

Преступник легко создаст клон реальной публичной точки доступа для того, чтобы собирать данные пользователей, подключившихся автоматически.

4. Не заходите в интернет-банк

В прошлом номере Вы касались темы фишинга. В случае использования публичного Wi-Fi Вам не удастся определить фишинговый сайт по неправильному написанию адреса сайта: злоумышленник может перенаправить обращение к реальному сайту и подставить данные со своего сервера. В таком случае по визуальным признакам будет невозможно понять, что Вас ввели в заблуждение.

5. По возможности используйте VPN

Это хороший способ не только защитить передаваемые через интернет данные, но и в целом анонимизировать Ваше нахождение в сети.

Универсальные горячие клавиши

Запомните и используйте горячие клавиши. Это позволит значительно ускорить работу с информацией.

Ctrl + S — сохранить
Shift + Ctrl + S — сохранить как
Ctrl + Z — вернуться на шаг назад
Ctrl + Y — вернуться на шаг вперед
Ctrl + C — копировать
Ctrl + V — вставить
Shift + Ctrl + V — вставить без форматирования
Ctrl + X — вырезать
Ctrl + A — выделить все
Ctrl + F — найти
Ctrl + P — отправить на печать
Ctrl + O — открыть файл
Ctrl + → — перейти в конец слова
Ctrl + ← — перейти в начало слова
Shift + → — выделить 1 символ вправо
Shift + ← — выделить 1 символ влево
Shift + Ctrl + → — выделить все слово вправо

Shift + Ctrl + ← — выделить все слово влево
Alt + Tab — переключение между открытыми приложениями

Сохранение результатов работы

Заведите привычку при каждом удобном случае сохранять документ, в котором работаете. Вы можете делать это с помощью меню в интерфейсе программы или используя горячие клавиши. В подавляющем большинстве программ работают комбинации Ctrl + S и Shift + Ctrl + S. Сохраняйтесь если:

- вынуждены отвлечься от документа
- потеряли мысль
- собираетесь перейти в другое окно

Выработав стойкую привычку систематически сохраняться, Вы существенно снизите вероятность потерять промежуточные результаты работы.

Блокировка экрана

Каждый раз, вставая с рабочего места, блокируйте экран ПК. Сделать это можно, используя горячие клавиши:

- для Windows: Win + L
- для MacOS: Command + Control + Q .

Это значительно повысит информационную безопасность и защитит данные от посторонних глаз.

Режим «инкогнито»

При использовании чужого устройства обязательно используйте режим «инкогнито» в браузере. Это действие позволяет:

– не сохранять историю просмотров;
– не сохранять поисковые запросы;
– не сохранять файлы cookie;
– не записывать новые пароли;
– не сохранять временные файлы и кешированное содержимое сайтов;
– не записываются данные в формах на сайтах.

Для включения анонимного режима используйте меню браузера или комбинацию клавиш Shift + Ctrl + N.

Безусловно, данный режим не делает Вас анонимным в интернете, однако позволяет не задумываться о следах пребывания в сети: как только Вы закроете браузер, они будут удалены. Учитывайте, что история переходов все равно будет доступна Вашему системному администратору и интернет-провайдеру.

Пустой рабочий стол

Старайтесь не захламлять рабочий стол в Windows. Каждый ярлык или файл, находящийся на рабочем столе, автоматически подгружается в оперативную память для быстрого запуска. Таким образом, большое количество объектов на рабочем столе негативно влияет на скорость операционной системы.

Настройка автозагрузки

Автозагрузка – удобная функция, которая позволяет запускать программы автоматически при загрузке операционной системы. Это может быть полезно для тех приложений, которые Вы используете ежедневно и хотите, чтобы они были доступны сразу после запуска компьютера.

ВАЖНО: Автозагрузка программ может замедлить загрузку системы, особенно если Вы добавили много приложений. Поэтому рекомендуется добавлять только те приложения, которые действительно используются ежедневно и нужны сразу после включения компьютера.

Как настроить автозагрузку в Windows:

1. Нажмите на клавишу Win + R , чтобы открыть окно «Выполнить».
2. Введите команду «shell:startup» без кавычек и нажмите Enter. Откроется папка «Автозагрузка».
3. Перетащите ярлык программы, которую Вы хотите запускать при загрузке системы, в эту папку.
4. Перезагрузите компьютер, чтобы убедиться, что программа запускается автоматически.

Как настроить автозагрузку на MacOS:

1. Откройте «Настройки системы» и выберите «Пользователи и группы».
2. Выберите свой профиль пользователя и перейдите на вкладку «Вход».
3. Нажмите на кнопку «+» и выберите приложение, которое Вы хотите запускать при входе в систему.
4. Нажмите на «Добавить», чтобы сохранить изменения.
5. Перезагрузите компьютер, чтобы убедиться, что программа запускается автоматически.

Резервные копии

Несмотря на достаточно высокую отказоустойчивость современных устройств, рано или поздно они выходят из строя. При отсутствии систематического создания резервных копий поломка устройства зачастую будет сопровождаться утратой критически важной информации.

И если в случае с потерей отсканированных документов архив еще будет возможно восстановить, то в случае с фото- и видеоматериалами потеря, скорее всего, будет невосполнимой.

При организации бэкапирования[4] необходимо учитывать основные источники проблем:

- физическая порча или утрата носителя;
- удаление или ошибочная правка оригинальной информации пользователем;
- сбой программного обеспечения;
- повреждение данных вредоносным ПО.

Критически важная информация должна иметь минимум три независимые резервные копии. Под независимостью подразумевается отсутствие связи между устройствами, на которых хранится копия. В первую очередь автономность каждой копии необходима для защиты ото всех вышеперечисленных причин потери данных.

Базовый подход к созданию и хранению резервных копий не подразумевает обязательного применения дорогостоящего ПО и аппаратуры. Для реализации приемлемого минимума достаточно стандартных утилит Windows и бесплатных программ.

Рекомендации

1. Имейте текущую копию всех важных данных на Вашем основном устройстве и периодически ее обновляйте.

В случае ошибочного удаления или правки информации эта копия позволит оперативно вернуться к «правильной версии документа».

2. Заведите отдельный внешний диск для хранения долгосрочных бекапов.

Такую копию можно обновлять реже, но необходимо делать это систематически, иначе в случае утраты основного устройства (или носителя с текущей копией) Вы вернетесь к архиву с неактуальными данными.

3. Заведите аккаунт в облачном хранилище и сохраняйте там информацию, не содержащую персональные данные.

Для подавляющего большинства пользователей будет достаточно объема хранилища, который предоставляется сервисами бесплатно.

4. Для более продвинутых пользователей рекомендуется использование сетевого хранилища, желательно с отключенным доступом в интернет.

[4] от англ. backup — резервный — процесс создания резервной копии данных

Такое хранилище представляет собой небольшое устройство с 2-4 жесткими дисками, к которому есть доступ через локальную сеть.

Важно понимать, что все мероприятия по резервному копированию должны иметь системный характер, иначе теряется их основной смысл.

Очистка кэша

При просмотре веб-сайтов или использовании приложений на устройстве сохраняется большое количество информации. Как правило, разработчики используют кэш для ускорения перезагрузки страниц/приложений. Кэш загружает данные с устройства практически мгновенно, вместо того чтобы повторно загружать их через Интернет.

Недостатком такой оптимизации является то, что информация с течением времени становится неактуальной. Например, на сайте может быть изменено одно изображение на другое, но Ваше устройство все еще показывает старое изображение, потому что оно было ранее закэшировано.

Кроме того, большое количество кэшированных данных может привести к замедлению работы вашего устройства.

Поэтому рекомендуется периодически очищать кэш на Вашем устройстве.

Android

1. Откройте настройки смартфона.
2. Перейдите в раздел «Приложения».
3. Выберите из списка нужную программу.
4. Откройте пункт «Использование памяти».
5. Выберите действие «Очистить кэш».

Windows

1. Нажмите Win + R и в появившемся окне «Выполнить» введите %temp% и нажмите «ОК».
2. Выделите все файлы и нажмите «Удалить».
3. Затем в окне «Выполнить» пропишите temp и нажмите «ОК».
4. Выделите все элементы и удалите их.

MacOS

1. На Mac выберите меню Apple > «Системные настройки», нажмите «Основные» в боковом меню, затем нажмите «Общий доступ» справа. (Возможно, потребуется прокрутить вниз).
2. Рядом с параметром «Кэширование контента» нажмите кнопку информации.
3. Нажмите «Параметры».
4. Нажмите «Сбросить», затем нажмите «Сбросить» еще раз, чтобы подтвердить запрос.

Cookie

Куки[5] — это данные (или их фрагменты), которые создаются в процессе работы с тем или иным сайтом и хранятся на компьютере пользователя. Как правило, куки используются владельцами сайтов для аутентификации пользователей и сохранения его настроек и предпочтений.

Рекламные сети, кроме прочего, используют их для сбора статистики о пользователе. Посещая интернет-ресурсы, на которых установлен код рекламной сети, пользователь оставляет «цифровой след». Анализ полученных данных позволяет прогнозировать дальнейшее поведение пользователя и актуально на него реагировать: например, возможно определение потребности в том или ином товаре, с тем чтобы вовремя предложить его пользователю.

Куки достаточно просто перехватить в случае, если пользователь использует нешифрованное соединение или публичные WiFi-сети. Используя перехваченные данные, злоумышленник может получить доступ к Вашим личным кабинетам и другой ценной информации.

Для обеспечения минимальной безопасности следуйте следующим рекомендациям:

1. Настройте ваш браузер таким образом, чтобы на вашем устройстве сохранялись только нужные вам куки:

– Зайдите в меню разрешений браузера и убедитесь, что заблокированы все cookies, которые Вы не хотите сохранять.

– Если нужно, для некоторых сайтов можно сделать исключение.

– Заблокировать только сторонние (рекламные) или запретить вообще все cookies можно в настройках браузера.

2. При подключении к сайту проверяйте защищенность соединения.

Посмотрите, какой значок появился слева от адреса сайта:

– Соединение защищено.

– Соединение не защищено.

– Соединение не защищено или опасно.

3. При использовании чужого устройства используйте режим «инкогнито» (приватного просмотра) в браузере.

Операторы поисковых систем

Поисковые системы (например, Google и Яндекс) способны воспринимать не только слова, но и специальные символы, которые позволяют сузить или расширить критерии поиска, так называемые «операторы поисковых систем». С их помощью Вы сможете уточнить свой запрос и быстро найти именно ту информацию, которая Вам нужна.

Подобных команд достаточно много, однако для решения большинства

[5] от англ. cookie, букв. — печенье

типовых задач достаточно ограниченного списка операторов.

Оператор « + »

«Плюс» позволяет указать слово, которое обязательно должно присутствовать на странице (помимо основного).

Пример: «робот + пылесос».

Поисковая система покажет только те страницы сайтов, которые содержат оба слова.

Оператор « - »

«Минус» указывает, что слово, следующее за ним, не должно находиться на странице.

Пример: «робот пылесос – инструкция».

Оператор «” “»

Заключив фразу в кавычки, Вы указываете, что на искомой странице данная фраза должна находиться в неизменном виде.

Пример: «каталог роботов пылесосов».

Оператор « * »

«Звездочка» заменяет любое количество слов и необходима в тех случаях, когда Вы не помните часть искомой фразы.

Пример: «оставь * я в печали».

Оператор « | »

Вертикальная черта предназначена для указания синонимов.

Пример: «смартфон | телефон sony»

Все операторы можно комбинировать и использовать совместно.

Защита от посторонних глаз

Защита данных – актуальнейшая тема в современной цифровой эпохе. С каждым днем мы все больше зависим от технологий и передаем все больше чувствительной информации во внешние источники. С увеличением количества устройств, которые мы используем в нашей повседневной жизни, увеличивается и риск случайного взгляда на наш экран, что может привести к самым серьезным негативным последствиям.

Существует множество способов, которые могут помочь Вам защитить свои данные от случайного взгляда. Вот несколько из них:

1. Используйте специальную защитную пленку для экрана

Подобные пленки еще называют «антишпионские»: в их структуре используется специальный слой, который значительно уменьшает угол обзора — уже при 30–60 градусах экран выглядит полностью черным.

2. Настройте время блокировки экрана

Если Вы оставите свое устройство без присмотра, оно автоматически заблокируется через определенное время. Рекомендуем выставить минимальное значение, при котором Вам комфортно пользоваться устройством.

3. Используйте функцию «невидимый режим»

В основном эта рекомендация относится к банковским приложениям. Многие банки предлагают функцию «невидимый режим», которая может помочь Вам скрыть информацию о картах и балансе счетов.

4. Должная осмотрительность

Старайтесь всегда контролировать свое устройство: не оставляйте его без присмотра и избегайте посторонних взглядов на Ваш экран.

5. Настройте уведомления на смартфоне

Возможна ситуация, когда нет возможности избежать чужого взгляда на смартфон в момент получения сообщения. В случае если уведомления отображаются сразу на экране блокировки, возможны негативные последствия. Рекомендуем не отображать содержимое уведомлений на заблокированном устройстве.

Уход за компьютером

Клавиатура, мышь и компьютер уже давно стали неотъемлемой частью нашей жизни. Мы используем их каждый день, и они подвергаются множеству различных загрязнений. В результате они могут быстро выйти из строя или же стать постоянным источником бактерий и грязи.

Чтобы продлить их жизнь, необходимо регулярно проводить процедуры по очистке клавиатуры, мыши и системного блока компьютера.

Клавиатура

Для ее очистки Вы можете использовать баллон со сжатым воздухом, салфетки и микрофибру. Если клавиатура сильно загрязнена, то можно воспользоваться щеткой. Не забудьте выключить компьютер, чтобы избежать случайного нажатия клавиш. При использовании ватных палочек или салфеток не забудьте обработать их антистатиком, чтобы избежать статического электричества.

Мышь

Для очистки мыши Вы можете использовать те же инструменты, что и для клавиатуры. Если мышь имеет оптический датчик, не забудьте очистить его, чтобы он мог правильно работать. Для этого можно использовать ватные палочки или микрофибру, смоченную в воде или спирте.

Системный блок

Системный блок также нуждается в регулярной очистке. Он может запылиться, что может привести к перегреву и сбоям. Для очистки компьютера необходимо использовать баллон со сжатым воздухом. Предварительно не забудьте выключить компьютер. Желательно проводить очистку в хорошо

проветриваемом помещении. Отлично подойдет балкон или лоджия.

В заключение хотим подчеркнуть, что регулярная чистка клавиатуры, мыши и компьютера является необходимой процедурой, которая поможет продлить их жизнь и сохранить чистоту. Она не займет много времени, но поможет избежать множества проблем в будущем. Не забывайте проводить очистку регулярно и постоянно следите за чистотой Ваших устройств.

Сохранение здоровья

Мы проводим много времени за компьютерами, телефонами и планшетами и часто не задумываемся о том, как это влияет на наше здоровье. Однако существует много осложнений, связанных с длительным использованием цифровых устройств, включая проблемы со зрением, головными болями, нарушениями сна и т.д.

Вот несколько советов, которые помогут Вам сохранить здоровье в эпоху технологий:

1. Давайте отдых глазам

Длительное время работы за компьютером может привести к усталости глаз и другим проблемам со зрением. Чтобы их избежать, рекомендуется делать перерыв каждые 20 мин и смотреть на объекты в отдалении в течение нескольких минут.

2. Используйте правильную освещенность

Чтобы избежать напряжения в глазах, рекомендуется использовать искусственное освещение, которое не отражается на экране, и регулировать яркость экрана в соответствии с освещенностью помещения.

3. Соблюдайте правильную позу

Неправильная поза при работе за компьютером может привести к болезням позвоночника и другим проблемам со здоровьем. Чтобы не допустить их появления, рекомендуется сидеть прямо, с опорой на спину стула и держать экран на уровне глаз.

4. Ограничьте непрерывное время работы за компьютером

Рекомендуется ограничить время работы за компьютером и делать перерывы каждые 45-60 мин.

5. Используйте специальное программное обеспечение

Существует много программ, которые помогают автоматически регулировать яркость экрана в соответствии со временем суток или напоминают Вам о необходимости делать перерывы каждые 60 мин.

Если Вы проводите много времени за компьютером или другими цифровыми устройствами, рекомендуется следовать этим советам и заботиться о своем здоровье.

Чек-лист для самопроверки

Наш чек-лист поможет Вам оценить Вашу текущую цифровую безопасность и подскажет практические шаги для усиления защиты. Это отличная возможность обновить свои знания о цифровой безопасности и принять меры, чтобы быть защищенным в сети. Не забывайте, что безопасность в сети – наша общая ответственность. Защита своих данных – это знание и практика.

Стационарный компьютер / ноутбук

- ☐ Установлены актуальные обновления для операционной системы
- ☐ Установлены все критические обновления для используемого программного обеспечения
- ☐ Установлен антивирус и настроено регулярное обновление баз
- ☐ Включен фаерволл
- ☐ Используется ограничение прав доступа на компьютере
- ☐ Не используете расширения для браузеров (например, блокировщики рекламы)
- ☐ Отключены из автозагрузки ненужные и редко используемые программы
- ☐ Используется только лицензионное ПО
- ☐ Проводится периодическая чистка куков и проверяются настройки уведомлений

Смартфон/планшет

- ☐ Установлены только проверенные приложения (из официального магазина или другого официального источника)
- ☐ Периодически проводится очистка кэша
- ☐ Установлены актуальные обновления приложений и прошивки устройства
- ☐ На устройстве не проводился Rooting / Jailbreak / HardSPL
- ☐ Используете защитную «антишпионскую» пленку для экрана
- ☐ Используете «невидимый режим» в банковских приложениях
- ☐ Устройство не оставляется без присмотра
- ☐ На устройстве отключен вывод уведомлений с «чувствительной информацией» на экране блокировки
- ☐ Выключаете wi-fi, если не планируете им пользоваться
- ☐ Отключена функция автоматического подключения к доступным wi-fi сетям

Полезные привычки

- ☐ Используются сложные пароли
- ☐ Не используется один и тот же пароль для нескольких учетных записей
- ☐ Не переходите по подозрительным ссылкам в письмах

- ▢ Регулярно создаются резервные копии важных данных
- ▢ По возможности используется двухфакторная аутентификация
- ▢ Для доступа к «чувствительной информации» на чужом устройстве используется режим «инкогнито»
- ▢ Повсеместно используете горячие клавиши
- ▢ Не делитесь личной информацией в социальных сетях
- ▢ Блокируете экран устройства при покидании рабочего места
- ▢ Регулярно сохраняете промежуточные результаты работы в программах
- ▢ Не входите в личный кабинет банка при использовании публичных wi-fi сетей
- ▢ При каждом использовании банкомата проверяете его на наличие скиммера
- ▢ Используете разные почтовые ящики для разных задач (личная переписка, регистрация на сторонних сервисах, рабочие задачи)

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

ДЛЯ ЗАМЕТОК

НЕФТЕГАЗСТРОЙПРОФСОЮЗ РОССИИ

119119, г. Москва
Ленинский проспект, 42
rogwu@rogwu.ru

ROGWU.RU