



ОБЩЕРОССИЙСКИЙ ПРОФЕССИОНАЛЬНЫЙ СОЮЗ
РАБОТНИКОВ НЕФТЯНОЙ, ГАЗОВОЙ ОТРАСЛЕЙ
ПРОМЫШЛЕННОСТИ И СТРОИТЕЛЬСТВА



ЦИФРОВАЯ ГИГИЕНА

(методические рекомендации)

Москва
2025



НЕФТЕГАЗСТРОЙПРОФСОЮЗ
РОССИИ



ЦИФРОВАЯ ГИГИЕНА.....	4
БАЗОВАЯ БЕЗОПАСНОСТЬ.....	4
Почему нельзя использовать один пароль везде.....	4
Как создать надежный пароль самостоятельно.....	4
Менеджеры паролей.....	5
Двухфакторная аутентификация.....	5
ЗАЩИТА УСТРОЙСТВ.....	6
Обновление ПО.....	6
Лицензионное ПО.....	6
БЕЗОПАСНОСТЬ В СЕТИ.....	7
Фишинг.....	7
Публичные Wi-Fi сети.....	8
КОНФИДЕНЦИАЛЬНОСТЬ.....	9
Защита персональных данных.....	9
Работа с электронной почтой.....	9
Cookie.....	9
ЭФФЕКТИВНЫЕ РАБОЧИЕ ПРИВЫЧКИ.....	10
Горячие клавиши.....	10
Универсальные горячие клавиши (Windows/MacOS).....	10
Сохранение результатов работы.....	11
Режим «инкогнито» (приватного просмотра).....	12
Резервные копии.....	12
Оптимизация работы устройства.....	12
Пустой рабочий стол.....	12
Настройка автозагрузки.....	13
Очистка кэша.....	13
УСТРОЙСТВО РАБОЧЕГО ПРОСТРАНСТВА.....	14
ИТОГОВЫЙ ЧЕК-ЛИСТ.....	16
ЗАКЛЮЧЕНИЕ.....	17

Цифровая гигиена

Сегодня наша профессиональная и личная жизнь неразрывно связана с цифровыми технологиями. Мы общаемся, работаем с документами, получаем услуги и совершаем платежи онлайн. Эта удобная среда, к сожалению, также привлекает злоумышленников.

Эта брошюра — не сложный технический справочник, а сборник простых и эффективных правил цифровой гигиены. Следуя им, вы не станете хакером, но сможете защитить свои личные данные, финансы и репутацию от большинства угроз.

Правила разделены на логические блоки — от основ создания паролей до тонкостей работы с почтой и социальными сетями. Начните с малого — выберите 2–3 совета, внедрите их в свою жизнь на этой неделе, и вы уже значительно повысите свой уровень безопасности.

Базовая безопасность

Почему нельзя использовать один пароль везде

Безопасность ваших цифровых аккаунтов начинается с надежного контроля доступа. Основа этого контроля — уникальные *стойкие пароли* и *многофакторная аутентификация*.

Как создать надежный пароль самостоятельно

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 одну из следующих схем, и вам не придется запоминать пароли для каждой системы.

Вариант 1

- 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* — PavLiC&3odn;
- для *mail.ru* — PavLiC&3mai.

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

Вариант 2

- Возьмите легко запоминающуюся для вас фразу из 4–5 слов (с цифрами и пунктуацией).
- Возьмите первые буквы каждого слова, сохраняя заглавные буквы и пунктуацию.
- Добавьте цифры и спецсимволы или возьмите по 1–2 буквы из каждого слова.

Пример: Фраза «Я член Профсоюза с 2014 года!» превращается в пароль «YaChlenProfSouzaS2014Goda!» или «YaChPrS2014G!». Такой пароль длинный, сложный и уникальный, и при этом его можно запомнить.

Менеджеры паролей

Это специальные программы, которые создают, хранят и автоматически подставляют сложные уникальные пароли для каждого сайта и сервиса.

Вам нужно запомнить всего один главный пароль — от самого менеджера.

Преимущество: вам не нужно придумывать и запоминать десятки паролей. Программа сделает это за вас, используя максимально стойкие комбинации.

Двухфакторная аутентификация

Суть двухфакторной аутентификации — использование двух независимых устройств для подтверждения вашей личности при входе в аккаунт.

Как это работает:

1. Вы вводите логин и пароль (первый фактор).
2. Сайт сразу запрашивает второй фактор, *например:*
 - код из SMS или push-уведомления на ваш телефон;
 - код из приложения-аутентификатора;
 - подтверждение отпечатком пальца или лицом на вашем устройстве («то, что вы есть»).

Главная цель: даже если злоумышленник украдет ваш пароль, без второго фактора он не сможет войти в ваш аккаунт.

Всегда включайте двухфакторную аутентификацию для всех важных сервисов: почта, социальные сети, онлайн-банкинг, «Госуслуги» и т.п.

Защита устройств

Обновление ПО

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);
- 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.

Лицензионное ПО

В связи с уходом ряда поставщиков ПО с российского рынка может возникнуть соблазн использования нелегального, «взломанного» софта. Зачастую именно такие продукты являются источником заражения операционной системы.

Необходимо понимать, что нередко вместе с «кряком» (программой-взломщиком) пользователь, не осознавая того, своими руками устанавливает вредоносное ПО (вирусы, майнеры, шпионские программы) и предоставляет ему полные права, исключая файлы взлома из сканирования антивирусом.

Негативное воздействие может проявиться не сразу. Злоумышленник в состоянии настроить работу вредоносной программы таким образом, что пользователь долгое время не сможет распознать заражение. За это

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.

время программа соберет достаточно информации (логины, пароли, личные файлы), чтобы нанести максимальный ущерб. Одной из самых опасных угроз являются шифровальщики (ransomware), которые блокируют доступ ко всем вашим файлам, требуя выкуп за их возврат.

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.

Вывод: без крайней необходимости НИКОГДА не используйте взломанные версии лицензионного программного обеспечения. Риск потери данных и компрометации личной информации неизмеримо выше любой кажущейся экономии.

Безопасность в сети

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 самого пользователя. Действия злоумышленника направлены на то, чтобы побудить вас к самостоятельной передаче данных на поддельной странице или в результате выполнения определенных действий.

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 e-mail для личной регистрации без крайней необходимости.

Это поможет заранее отделить потенциально опасные письма.

2. Проверяйте каждое письмо с вложениями и ссылками.

Перед переходом по ссылке или открытием вложения убедитесь, что письмо пришло от ожидаемого и надежного отправителя. Внимательно проверьте адрес отправителя и домен ссылки: мошенники часто используют похожие адреса, например, «odnoklassnikl.ru» вместо «odnoklassniki.ru».

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

Чтобы гарантированно привлечь внимание, фишеры используют заголовки вроде «Подтверждение списания средств» или «Начисление штрафа». Практически все подлинные сообщения от организаций содержат в себе уникальную информацию, недоступную мошенникам (например, часть номера договора, Ф. И. О.). Любое письмо, не содержащее конкретной личной информации, — подозрительно.

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 вручную.

Это самый надежный способ попасть на настоящий сайт, а не на его подделку.

5. Остерегайтесь фишинга в мессенджерах и социальных сетях.

Мошенники активно используют WhatsApp, Telegram, Viber и социальные сети, притворяясь вашими коллегами, друзьями или службой поддержки. Они могут просить перевести деньги, сообщить код из SMS или перейти по срочной ссылке. Всегда перепроверяйте такую информацию через известный вам надежный канал связи (например, звонок).

Публичные Wi-Fi сети

Доступ к бесплатному Wi-Fi в общественных местах — это удобно, но каждая такая точка доступа является потенциальным источником «цифровой инфекции». Киберпреступники могут создавать поддельные сети или перехватывать данные в реальных сетях, чтобы собирать логины, пароли и другую личную информацию в промышленных масштабах.

Проявляйте должную бдительность.

1. Не доверяйте открытым точкам доступа, которые не защищены паролем. Чаще всего именно их используют для воровства данных.

2. Выключайте Wi-Fi, если не планируете им пользоваться. Это экономит заряд батареи и не позволяет отслеживать ваше местоположение по MAC-адресу устройства.

3. Отключите функцию автоматического подключения к Wi-Fi на телефоне и планшете. Преступник может легко создать клон реальной публичной точки доступа, и ваше устройство подключится к ней автоматически.

4. Не входите в интернет-банк и не вводите пароли от важных сервисов при использовании публичного Wi-Fi. Злоумышленник может перенаправить вас на фишинговый сайт, который будет выглядеть как настоящий.

5. Используйте VPN (Virtual Private Network). Это лучший способ защитить передаваемые через публичную сеть данные. VPN создает зашифрованный «туннель» между вашим устройством и интернетом, через который злоумышленник не сможет подглядеть вашу информацию.

Конфиденциальность

Защита персональных данных

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



Подсказка: если вам необходимы цифровые копии документов, лучше храните их на зашифрованной флеш-карте, которая будет на брелоке с ключами.



2. Не делитесь слишком личной информацией в социальных сетях.

Пояснение: всему миру не нужно знать кличку вашего домашнего животного или девичью фамилию матери, так как они могут быть ответами на секретные вопросы для восстановления пароля. Секретные вопросы лучше придумывать такие, на которые точно никто, кроме вас, не знает ответа.

Дополнение: будьте осторожны с публикацией информации о графике отпусков, дорогих покупках или номерах документов. Настройте приватность вашего профиля так, чтобы ваши посты видели только друзья.

Работа с электронной почтой

Электронная почта сегодня стала неотъемлемой частью нашей жизни, особенно на работе. Вот несколько приемов, которые помогут вам гораздо быстрее и эффективнее работать с почтой и повысить ее безопасность.

1. Используйте «+» в адресе для фильтрации.

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.

Как использовать: вы можете использовать этот метод, чтобы легко фильтровать письма. Например, при регистрации на сайте «Авито» укажите почту ivanov+avito@domain.ru. Затем создайте правило, которое будет автоматически перемещать все письма на этот адрес в отдельную папку «Авито». Это помогает сразу идентифицировать, откуда пришло письмо, и быстро заметить утечку данных, если этот адрес начнет получать спам.

2. Используйте фильтры и ярлыки.

Это отличный способ автоматизации обработки почты. Например, вы можете создать правило, которое автоматически помечает письма от руководства как важные или складывает в папку «Проект X».

Cookie (куки)

Cookie — это небольшие фрагменты данных, которые создаются в процессе работы с сайтом и хранятся в вашем браузере. Как правило,

они используются для аутентификации пользователей, сохранения его настроек и предпочтений. Рекламные сети используют их для сбора статистики и показа целевой рекламы.

Cookie можно перехватить, если вы используете нешифрованное соединение или публичные Wi-Fi-сети. Используя перехваченные данные, злоумышленник может получить доступ к вашим личным кабинетам.

Для обеспечения минимальной безопасности следуйте рекомендациям.

1. Периодически очищайте кэш и cookie в настройках браузера:

- 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. Настройте браузер так, чтобы он блокировал сторонние (рекламные) cookie. Это можно сделать в настройках конфиденциальности.

3. При подключении к сайту проверяйте защищенность соединения. Посмотрите на значок слева от адреса сайта: он должен быть в виде закрытого замка, а адрес должен начинаться с `https://`.

- Соединение защищено.
- Соединение не защищено.
- Соединение не защищено или опасно.

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

Эффективные рабочие привычки

Горячие клавиши

Использование горячих клавиш позволяет значительно ускорить работу и меньше зависеть от мыши. Запомните основные комбинации для вашей операционной системы.

Универсальные горячие клавиши (Windows/MacOS)

Основные комбинации для Windows:

- Ctrl** + **S** — сохранить
- Shift** + **Ctrl** + **S** — сохранить как
- Ctrl** + **Z** — вернуться на шаг назад, отменить действие
- Ctrl** + **Y** — перейти 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

Shift + **O** — открыть файл

Основные комбинации для MacOS:

Cmd + **S** — сохранить

Shift + **Cmd** + **S** — сохранить как

Cmd + **Z** — вернуться на шаг назад, отменить действие

Cmd + **Shift** + **Z** — перейти на шаг вперед

Cmd + **C** — копировать

Cmd + **V** — вставить

Cmd + **Shift** + **V** — вставить без форматирования

Cmd + **X** — вырезать

Cmd + **A** — выделить все

Cmd + **F** — найти

Cmd + **P** — отправить на печать

Cmd + **O** — открыть файл

Работа с текстом (Windows):

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 справа

Shift + **Ctrl** + **←** — выделить все слово влево

Работа с текстом (MacOS):

Option + **→** — перейти в конец слова

Option + **←** — перейти в начало слова

Shift + **→** — выделить 1 символ вправо

Shift + **←** — выделить 1 символ влево

Shift + **Option** + **→** — выделить все слово справа

Shift + **Option** + **←** — выделить все слово влево

Навигация между программами:

Alt + **Tab** — переключение между открытыми приложениями (Windows)

Cmd + **Tab** — переключение между открытыми приложениями (MacOS)

Для блокировки компьютера:

Win + **L** — мгновенно заблокировать компьютер (Windows)

Cmd + **Ctrl** + **Q** — мгновенно заблокировать Mac (MacOS)

Сохранение результатов работы





Выработайте привычку часто сохранять документ, в котором работаете. Используйте для этого горячие клавиши **Ctrl** + **S**. Сохраняйтесь, если:

- Вынуждены отвлечься от документа.
- Закончили важную мысль или этап работы.
- Собираетесь перейти в другое окно или программу.

Эта привычка существенно снизит вероятность потери промежуточных результатов из-за сбоя программы или отключения электричества.

Блокировка экрана

Каждый раз, вставая с рабочего места, блокируйте экран ПК. Это значительно повысит информационную безопасность и защитит данные от посторонних глаз.

- для Windows:  + 
- для MacOS:  +  + 

Режим «инкогнито» (приватного просмотра)

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

- не сохранять историю просмотров и поисковые запросы;
- не сохранять файлы cookie и временные файлы;
- не записывать новые пароли и данные из форм.

Важно: Данный режим не делает вас анонимным в интернете — ваш системный администратор и интернет-провайдер все равно видят ваши действия. Однако он помогает не оставлять следов на самом устройстве.

Для включения режима инкогнито используйте меню браузера или комбинацию клавиш  +  +  (в большинстве браузеров).

Резервные копии

Несмотря на высокую надежность современных устройств, они могут выйти из строя. При отсутствии резервных копий поломка часто приводит к безвозвратной утрате информации.

Следуйте правилу «3-2-1» для резервных копий:

- 3 копии данных.
- 2 разных типа носителей (например, жесткий диск компьютера + внешний жесткий диск или флешка).
- 1 копия хранится в другом месте (например, в надежном облачном хранилище).

Рекомендации:

- Имейте текущую копию важных данных на основном устройстве и периодически ее обновляйте.
- Заведите отдельный внешний диск для хранения долгосрочных резервных копий.
- Используйте облачное хранилище для информации, не содержащей критически важные персональные данные.

Оптимизация работы устройства

Пустой рабочий стол

Старайтесь не захламлять рабочий стол в Windows. Каждый ярлык или файл, находящийся на рабочем столе, автоматически загружается

в оперативную память для быстрого запуска. Таким образом, большое количество объектов на рабочем столе негативно влияет на скорость работы операционной системы и время ее запуска.



Настройка автозагрузки

Автозагрузка — это функция, которая позволяет запускать программы автоматически при загрузке операционной системы. Это удобно для приложений, которые вы используете ежедневно.



Важно: Автозагрузка слишком большого количества программ может значительно замедлить загрузку системы. Рекомендуется добавлять в автозагрузку только те приложения, которые действительно необходимы сразу после включения компьютера.

Как настроить автозагрузку в Windows:

1. Нажмите на клавиши  + , чтобы открыть окно «Выполнить».
2. Введите команду `shell:startup` и нажмите . 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 «Системные настройки» и выберите «Пользователи и группы».
2. Выберите свой профиль пользователя и перейдите на вкладку «Объекты входа».
3. Нажмите на кнопку «+» и выберите приложение, которое вы хотите запускать при входе в систему.
4. Нажмите «Добавить», чтобы сохранить изменения.

Очистка кэша

При просмотре веб-сайтов или использовании приложений на устройстве сохраняется большое количество временных данных (кэш). Хотя кэш ускоряет повторную загрузку страниц, со временем эти данные устаревают и могут занимать много места, что приводит к замедлению работы устройства.

Рекомендуется периодически очищать кэш.

Android

1. Откройте «Настройки».
2. Перейдите в раздел «Приложения».
3. Выберите нужное приложение из списка.
4. Перейдите в «Хранилище» или «Использование памяти».
5. Нажмите «Очистить кэш».

Windows (очистка временных файлов)

1. Нажмите **Win** + **R**, введите %temp% и нажмите «ОК».
2. Удалите все файлы в открывшейся папке.
3. Также можно ввести temp в окне «Выполнить» и удалить файлы из этой папки.

MacOS

1. Откройте «Системные настройки» > «Основные» > «Хранилище».
2. Нажмите «Управлять» для очистки кэша и других временных файлов.

Устройство рабочего пространства

Сохранение здоровья при работе с цифровыми устройствами

Мы проводим много времени за компьютерами, телефонами и планшетами. Длительное использование цифровых устройств может вызывать проблемы со зрением, головные боли, нарушения сна и другие осложнения.

Вот несколько советов, которые помогут сохранить здоровье:

1. Давайте отдых глазам

Используйте правило «20-20-20»: каждые 20 минут делайте перерыв на 20 секунд и смотрите на объекты, находящиеся на расстоянии 6 м (20 футов).

2. Используйте правильное освещение

Чтобы избежать напряжения глаз, используйте рассеянное искусственное освещение, которое не отражается на экране. Регулируйте яркость экрана в соответствии с освещенностью помещения.

3. Соблюдайте правильную позу

Сидите прямо, с опорой на спинку стула. Держите экран на уровне глаз или чуть ниже. Ноги должны стоять на полу, колени согнуты под углом 90 градусов.

4. Ограничьте непрерывное время работы

Делайте перерывы каждые 45–60 минут. Встаньте, пройдитесь, сделайте простые упражнения для разминки.

5. Используйте специальное программное обеспечение

Существуют программы, которые автоматически регулируют цветовую температуру экрана в соответствии с временем суток (f.lux, Night Shift) или напоминают о необходимости делать перерывы.

Уход за клавиатурой и мышью

Регулярная чистка компьютерного оборудования помогает продлить срок его службы и сохранить производительность.

Клавиатура:

- для очистки используйте баллон со сжатым воздухом и салфетки из микрофибры;
- при сильном загрязнении можно аккуратно использовать мягкую щетку;
- перед чисткой обязательно выключите компьютер.

Мышь:

- протирайте корпус салфеткой из микрофибры;
- очищайте оптический датчик ватной палочкой (при необходимости).

Системный блок:

- регулярно очищайте от пыли с помощью баллона со сжатым воздухом;
- проводите чистку в хорошо проветриваемом помещении;
- перед чисткой обязательно полностью выключите компьютер из розетки.

Итоговый чек-лист

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 гигиене и принять меры, чтобы быть защищенным в сети. *Помните: безопасность в сети — это ваша личная ответственность.*

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 брандмауэр (файрвол)
- Используется ограничение прав доступа на компьютере (работа без прав администратора)
- Установлены только проверенные расширения для браузеров
- Из автозагрузки отключены ненужные и редко используемые программы
- Используется только лицензионное ПО
- Периодически проводится очистка кэша и проверяются настройки уведомлений

Смартфон / планшет

- Установлены только проверенные приложения из официального магазина
- Периодически проводится очистка кэша
- Установлены актуальные обновления приложений и прошивки устройства
- На устройстве не проводился Rooting / Jailbreak
- Используется защитная «антишпионская» пленка для экрана
- Используется «невидимый режим» в банковских приложениях
- Устройство не оставляется без присмотра в общественных местах
- На устройстве отключен вывод чувствительной информации на экране блокировки

- Вы отключаете Wi-Fi, если не планируете им пользоваться
- Отключена функция автоматического подключения к доступным Wi-Fi-сетям

Полезные цифровые привычки

- Используются сложные уникальные пароли для разных сервисов
- Активно используется менеджер паролей
- Включена двухфакторная аутентификация на всех важных сервисах
- Вы не переходите по подозрительным ссылкам в письмах и мессенджерах
- Регулярно создаются резервные копии важных данных
- Для доступа к личным аккаунтам на чужом устройстве используется режим «инкогнито»
- Вы активно используете горячие клавиши в работе
- Вы не делитесь излишней личной информацией в социальных сетях
- Вы блокируете экран устройства при покидании рабочего места
- Регулярно сохраняете промежуточные результаты работы в программах
- Не входите в интернет-банк при использовании публичных Wi-Fi-сетей
- При использовании банкомата проверяете его на наличие скиммеров
- Используете разные почтовые ящики для разных задач

Заключение

Цифровая гигиена — постоянная практика и полезные привычки. Не стоит пытаться внедрить все и сразу. Начните с самого уязвимого места — например, с создания надежных паролей и включения двухфакторной аутентификации.

Регулярно возвращайтесь к этому чек-листу и оценивайте свой прогресс. Безопасность — это не итог, а непрерывный процесс.



Каталог
методических
материалов

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

ROGWU.RU