+ Windows 10

# РУКОВОДСТВО ПО КИБЕРБЕЗОПАСНОСТИ

## Десять шагов, которые должна предпринять каждая организация для защиты от кибератак

Обеспечьте повышенную безопасность на всех этапах.

Условия кибербезопасности постоянно изменяются и расширяются. Предприятиям малого и среднего бизнеса все чаще приходится сталкиваться с кибератаками, которые угрожают их информации и персональным данным их клиентов. Это руководство призвано помочь предприятиям малого и среднего бизнеса с ограниченными ИТ-ресурсами укрепить свою кибербезопасность уже сегодня с минимальными затратами или без каких-либо затрат.

# СОДЕРЖАНИЕ

# Картина угроз

# Тенденции в области кибербезопасности для предприятий малого и среднего бизнеса

По данным института Понемон[1], существует пять основных тенденций в области кибербезопасности для предприятий малого и среднего бизнеса.

1. **Все больше предприятий подвергаются атакам.**
За последние 12 месяцев количество кибератак на предприятия малого и среднего бизнеса увеличилось на 11% — с 55% до 61%. Наиболее распространенными видами атак на малые предприятия являются фишинг/социальная инженерия (48%) и веб-атаки (43%). В то же время кибератаки становятся все более целенаправленными, агрессивными и сложными.

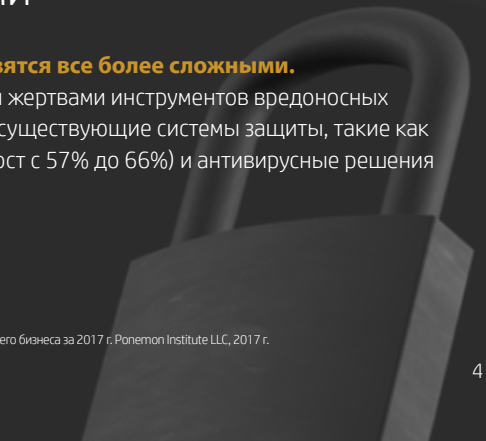
2. **Атаки обходятся компаниям дороже.**
Средняя стоимость нарушения нормальной работы увеличилась на 26% — с 955 429 долларов США до 1 207 965 долларов США. Средняя стоимость повреждений или краж ИТ-активов и инфраструктуры увеличилась с 879 582 долларов США до 1 027 053 долларов США.

3. **Основной причиной является человеческий фактор.**
54% предприятий малого и среднего бизнеса, в которых произошла утечка данных, считают, что основной причиной этого была небрежность сотрудников. По сравнению с прошлым годом количество таких предприятий увеличилось на 48%. Но, как и в прошлом году, каждая третья компания в этом исследовании не смогла определить первопричину.

4. **Надежные пароли и многофакторная проверка подлинности по-прежнему используются недостаточно.**
Пароли по-прежнему являются неотъемлемой составляющей кибербезопасности. Тем не менее, 59% респондентов заявляют, что у них нет данных об использовании паролей сотрудниками, например, об использовании уникальных или надежных паролей, а также о совместном использовании паролей с другими сотрудниками. По сравнению с прошлым годом эти данные не изменились.

> 59% респондентов заявляют, что у них нет данных об использовании паролей сотрудниками

5. **Вредоносные программы становятся все более сложными.**
Все больше предприятий становятся жертвами инструментов вредоносных кодов и программ, которые обходят существующие системы защиты, такие как системы обнаружения вторжений (рост с 57% до 66%) и антивирусные решения (рост с 76% до 81%).



1 — Отчет: Тенденции в области кибербезопасности для предприятий малого и среднего бизнеса за 2017 г. Ponemon Institute LLC, 2017 г.

# Пять наиболее распространенных атак против предприятий малого и среднего бизнеса

1 **Фишинг и социальная инженерия**

Социальная инженерия требует участия человека для получения информации об организации или ее компьютерных системах. Например, злоумышленник может представиться новым сотрудником, специалистом по ремонту или исследователем. Задавая вопросы, он/она может собрать достаточно информации для проникновения в сеть организации.[2]

Фишинг — это форма социальной инженерии. При фишинговой атаке злоумышленник представляется надежной организацией и использует электронную почту или вредоносные веб-сайты для получения персональных данных.[2]

2 **Веб-атаки**

При веб-атаках злоумышленник получает доступ к официальному веб-сайту и отправляет вредоносное ПО. Официальный сайт действует как паразитический, заражая ничего не подозревающих посетителей. Одной из самых коварных сетевых атак является так называемая «скрытая загрузка», когда вредоносный контент автоматически загружается на компьютер пользователя при простом просмотре сайта. Участие пользователя не требуется.[3]

3 **Вредоносное ПО**

Вредоносное ПО — это широкий термин, который относится к любому программному обеспечению, которое создано специально для нанесения ущерба устройству или сети.[4] К нему относятся вирусы, шпионское ПО, программы-вымогатели и все остальные аналогичные программные средства. Помимо веб-атак, такое ПО может получать доступ к компьютеру жертвы через USB-накопитель или скомпрометированное сетевое соединение.[5]

4 **Скомпрометированные и краденые устройства**

Скомпрометированное или краденое устройство может содержать важную информацию и локально сохраненные учетные данные, которые обеспечивают доступ к информации и сетям организации в будущем. Ненадежные пароли и шифрование данных могут еще более усугубить этот тип атаки.

5 **Атаки типа «отказ в обслуживании»**

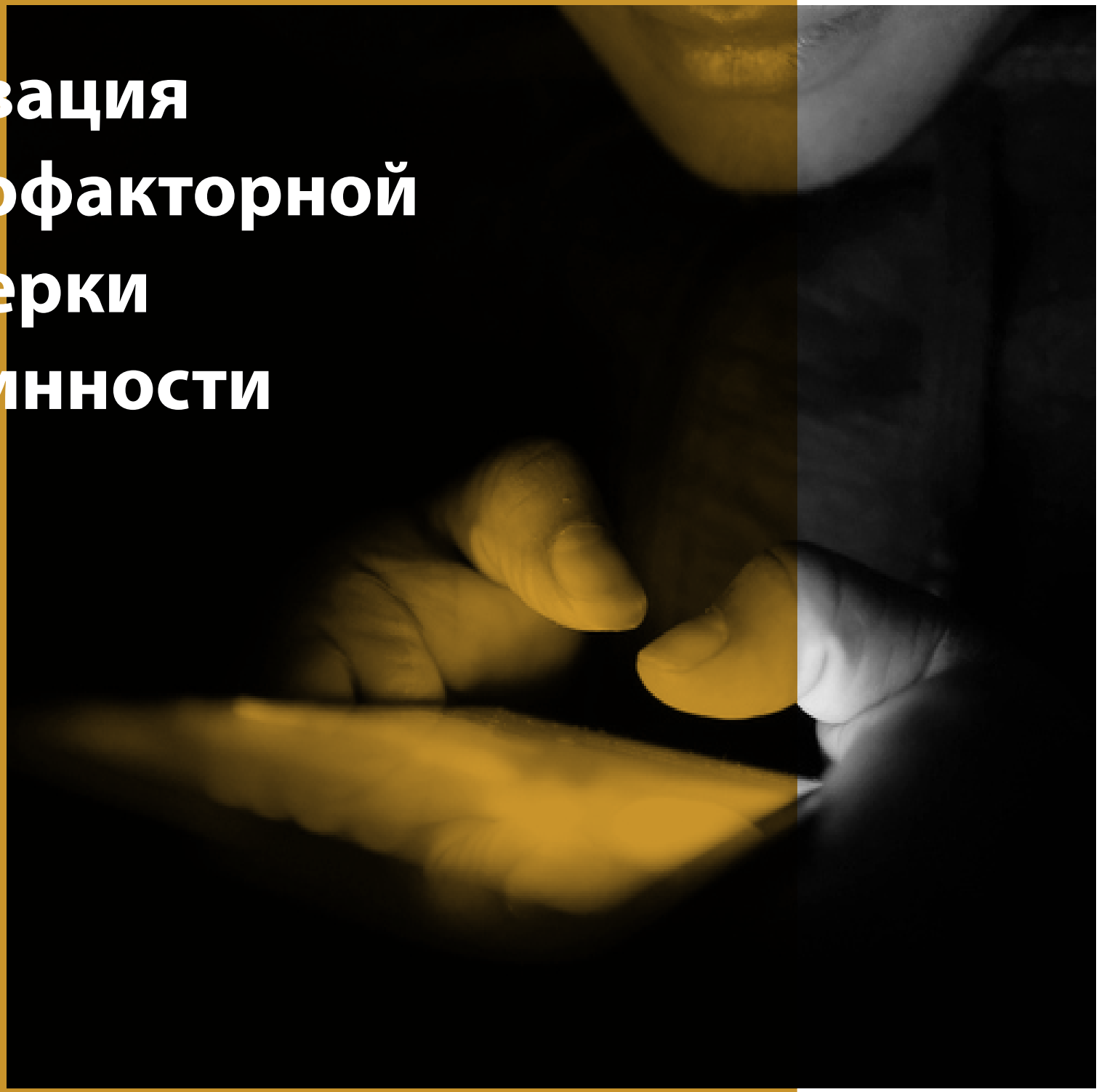
Атаки типа «отказ в обслуживании» подразумевают лавинную маршрутизацию целевой сети до тех пор, пока она больше не сможет отвечать или просто не выйдет из строя, предотвращая доступ законным пользователям. Распределенная атака типа «отказ в обслуживании» (DDoS) возникает, когда несколько компьютеров работают вместе, чтобы атаковать одну цель, увеличивая мощность атаки. При DDoS усложнен поиск настоящего источника.[6]

2—https://www.us-cert.gov/ncas/tips/ST04-014
3—https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/web-based-attacks-09-en.pdf
4—https://technet.microsoft.com/en-us/library/dd632948.aspx
5—https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/CaseStudy-002.pdf
6—https://www.us-cert.gov/ncas/tips/ST04-015

# Десять способов защитить себя

Раздел 1:

# Активация многофакторной проверки подлинности



Ключевой целью для хакеров являются имена пользователей и пароли, а также, и не без основания, ваша личность — ваш самый ценный актив. Надежные и безопасные пароли имеют большое значение, но они не являются самым безопасным механизмом проверки подлинности. И в нашем мире, где взлом систем и данных все чаще превращается в источник дохода, воры, которые не являются экспертами, могут передать эту работу другим. Хакеры могут купить специальное оборудование, предназначенное для взлома паролей, арендовать пространство у поставщиков публичных облачных серверов или создать ботнет для обработки данных.

- 90% данных, украденных с помощью фишинга, — это учетные данные пользователя[7]
- 80–90% паролей можно взломать в течение 24 часов[8]

При многофакторной проверке подлинности (MFA) следует использовать не менее двух независимых учетных данных для подтверждения вашей личности, что существенно повысит уровень безопасности. Это может быть **известная** пользователю информация (пароли или ПИН-коды), его **устройства** (Bluetooth®-телефоны или смарткарты) или **свойство** его личности (идентификация по лицу или отпечатку пальца). Если один из факторов скомпрометирован или нарушен, злоумышленник должен столкнуться со вторым барьером другого типа.

Многофакторная проверка подлинности HP и технология Intel® Authenticate позволяют одновременно использовать несколько факторов проверки подлинности при каждой попытке входа в систему.

7— Verizon, 2016 Data Breach Investigations Report, 2016
8— Источник: Brian Contos, CISO at Verodin, Inc. Цитируется с разрешения. https://www.csoonline.com/article/3236716/authentication/how-hackers-crack-passwords-and-why-you-cant-stop-them.html

## Настройка многофакторной проверки подлинности с HP.

Современные устройства HP Pro или Elite поддерживают настройку MFA через HP Client Security Manager.[9]

1. Запустите Client Security Manager (для этого вам потребуются права доступа администратора). Если вы запустите его с помощью пакета HP Manageability Integration Kit (MIK), то сможете распространить политику MFA на все свои ПК.[10]
2. Откройте панель управления и нажмите Standard User Policies (Политика обычных пользователей).
3. Выберите два или три фактора, для которых вы хотите настроить политику входа в систему, и следуйте инструкциям в соответствии с запросами о регистрации учетных данных, например сканирование отпечатка пальца с помощью считывателя отпечатков пальцев ПК или ввод ПИН-кода.

## Разнообразие при использовании Windows Hello.

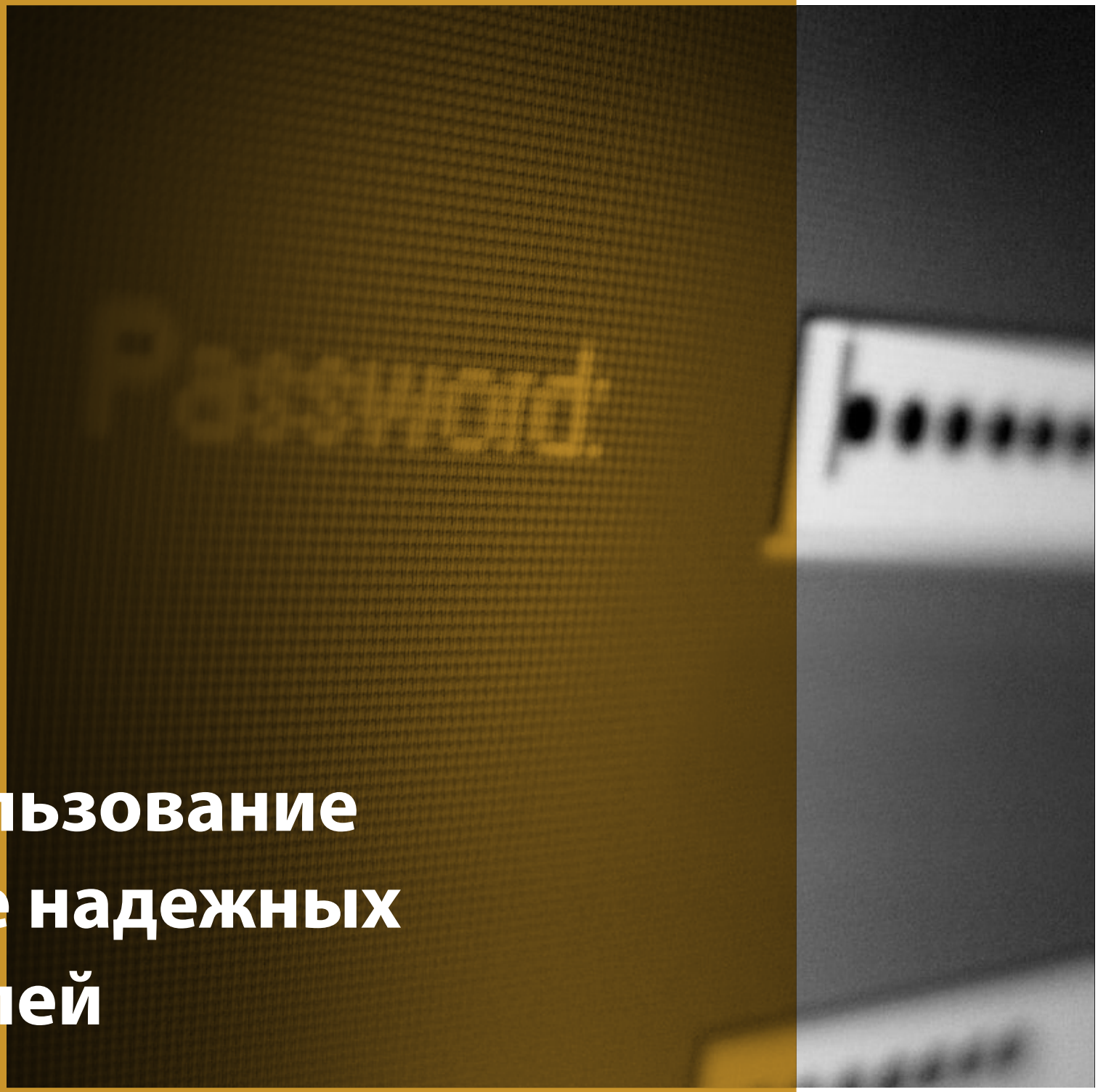
Многие современные устройства с Windows 10 Pro со встроенной веб-камерой, включая весь ассортимент ноутбуков и трансформеров HP, совместимы с Windows Hello. Сканирование лица при использовании Windows Hello — это альтернатива паролю в качестве одного из учетных данных для MFA.

1. Откройте Settings> Accounts> Sign-in options (Настройки> Учетные записи> Опции входа в систему).
2. В окне PIN (ПИН-код) выберите Add (Добавить), если эта опция еще не была установлена.
3. В разделе Windows Hello выберите Set up (Настроить) и следуйте инструкциям на экране, чтобы выполнить сканирование своего лица.

9— Для HP Client Security Manager Gen4 требуется ОС Windows и процессоры Intel® или AMD 8-го поколения.
10— Пакет HP Manageability Integration Kit можно загрузить с сайта http://www.hp.com/go/clientmanagement.

Раздел 2:

# Использование более надежных паролей



В повседневной жизни пароли используются везде. Мы используем их практически на всех личных или профессиональных устройствах, сервисах и учетных записях. Поскольку они являются первым (и слишком часто — единственным) средством защиты личности и данных, последствия использования ненадежных паролей могут быть катастрофическими. Несмотря на это, большинство людей не используют надежные и уникальные пароли.

- 59% пользователей знают, что безопасный пароль важен, и все же 41% выбирают пароль, который легко запомнить
- 91% пользователей понимают риск повторного использования паролей, но 55% делают это в любом случае
- Представители поколения 2000-х, как правило, используют более надежные пароли, чем люди послевоенного поколения «беби-бумеры» (65% и 45% соответственно)[11]

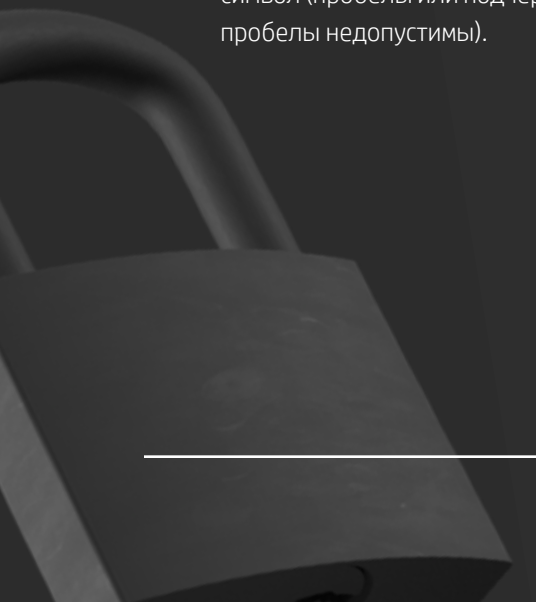


Если ваше устройство или услуга не поддерживает MFA, то необходимо сделать так, чтобы один пароль был максимально надежным. У большинства людей нет надежных паролей, потому что они просто не понимают, как их создавать, предполагая, что это, вероятно, будет произвольная комбинация букв, цифр и символов. Но существуют более надежные и простые способы значительно повысить уровень защиты паролем.

11— Источник: LastPass, "New Research: Psychology of Passwords, Neglect is Helping Hackers Win", Katie Petrillo, 1 мая 2018 г.

# Мнемонические пароли вместо цифровых.

Мнемонические кодовые фразы более безопасны, чем простые пароли, и их легче запомнить, чем числовые.
Если мнемонические кодовые фразы используются вместо простых паролей, их практически невозможно взломать.



## 1 Начните с запоминающейся фразы.

Например, первые шесть слов известной Геттисбергской речи Авраама Линкольна «Four score and 7 years ago» — это простая кодовая фраза. Цитата соответствует основным требованиям к паролям: имеет длину от 8 до 32 символов, включает в себя заглавные и строчные буквы, по крайней мере одну цифру и один специальный символ (пробелы или подчеркивания, если пробелы недопустимы).

## 2 Сделайте пароль как можно более странным.

Увеличьте количество цифр и специальных символов. Например, измените буквы в предыдущем примере:
«4 $core @nd 7 Ye@rs ago».

## 3 Адаптируйте, но не копируйте.

Просто добавив простой суффикс в конец каждой фразы, вы можете легко использовать свой основной пароль без опасности дублирования. Для учетной записи Facebook попробуйте добавить «FB» в конце фразы, а для Instagram — «IG».

# Использование менеджера паролей.

Менеджеры паролей являются одной из лучших мер безопасности, рекомендованных экспертами по безопасности. Они позволяют создавать и хранить длинные сложные пароли для каждой из ваших учетных записей в Интернете, устраняя необходимость запоминать их. В целом, нужно запомнить только один пароль — основной пароль для вашего «хранилища». Менеджер паролей настраивается, как правило, с использованием одного и того же простого процесса.

1. Загрузите и установите программное обеспечение и расширение для своего браузера. Можно также загрузить приложение для своего мобильного устройства.
2. Настройте свою учетную запись, указав адрес электронной почты и свой основной пароль.
3. Введите данные различных учетных записей.

Большинство менеджеров паролей потребуют обновления старых паролей вручную: войдите в свою учетную запись, перейдите в настройки и позвольте менеджеру паролей сгенерировать новый, более безопасный пароль. Замена старых ненадежных паролей может занять некоторое время, но значительное повышение уровня вашей безопасности того стоит.

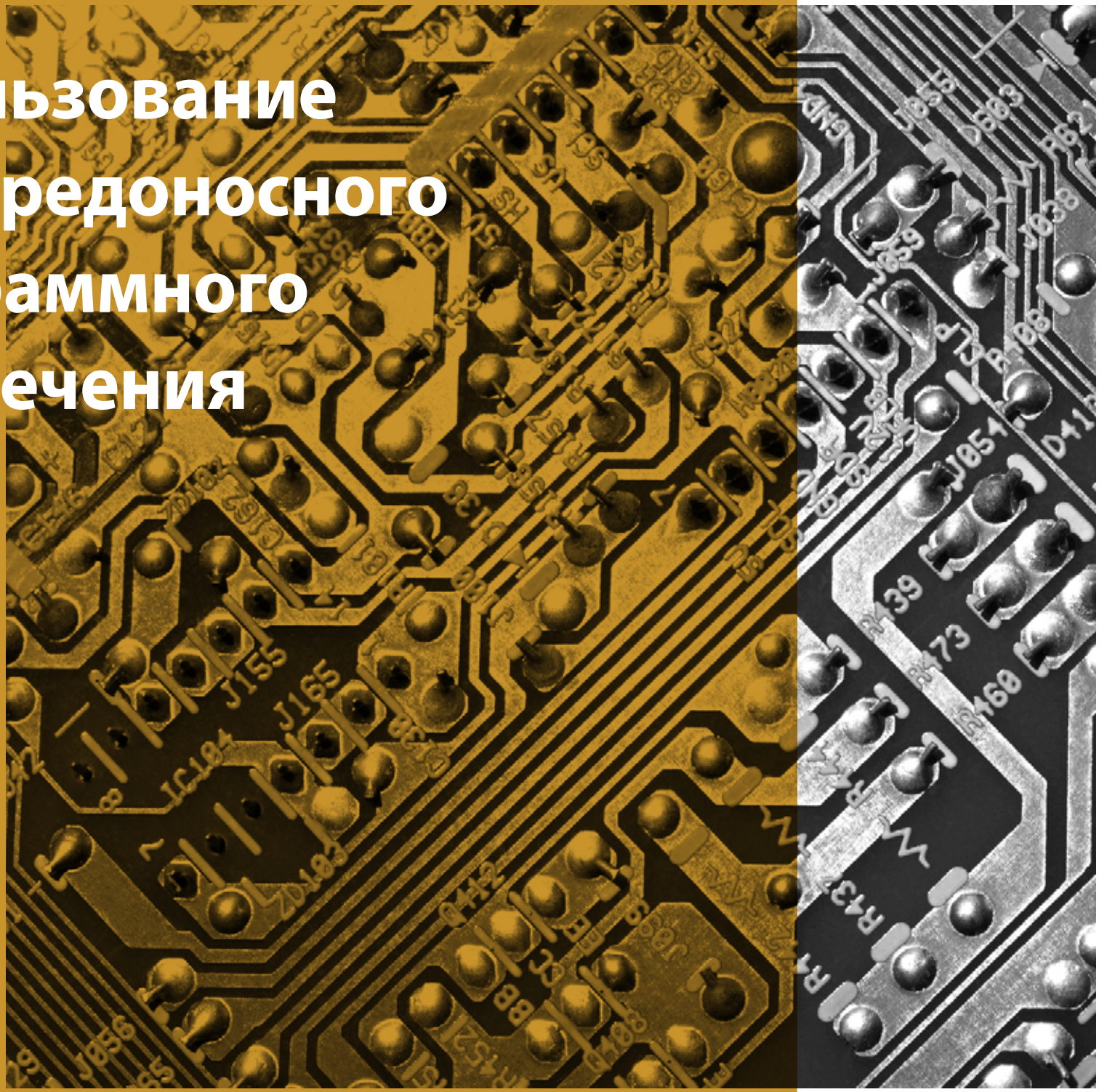
## Выбор менеджера паролей.

Существует множество бесплатных менеджеров паролей, такие как Bitwarden, Dashlane и Enpass. Просто выберите тот менеджер паролей, который обеспечивает следующее:

- легко интегрируется в наиболее часто используемый вами браузер;
- позволяет сохранять файл паролей в виде зашифрованного файла, который не может быть прочитан без проверки подлинности пользователя. В частности, выберите менеджер паролей, который использует шифрование AES-256 или более надежное;
- разрешает двухфакторную проверку подлинности для доступа к хранилищу паролей;
- позволяет назначить контактное лицо при чрезвычайных ситуациях, у которого также может быть доступ к хранилищу паролей;
- хранит дополнительную информацию для входа вместе с паролем (например, секретные вопросы, номера телефонов, данные учетной записи и т.д.).

Раздел 3:

# Использование антивредоносного программного обеспечения



# Компьютер, на котором не установлена антивирусная защита, можно заразить вредоносным ПО в течение нескольких минут после подключения к Интернету.

Вредоносные программы всех форм могут размещаться на сайтах, имеющих на первый взгляд хорошую репутацию, или могут быть получены во вложениях электронной почты. Кроме того, каждый день создаются все новые и новые вредоносные программы. На ваш ПК постоянно пытаются проникнуть вирусы, поэтому инструмент, который его защищает, должен быть мощным, глубоко внедренным и регулярно обновляться. Хорошее антивредоносное ПО должно обладать всеми тремя качествами.

В общем, антивредоносное программное обеспечение представляет собой программу или набор программ, предназначенных для предотвращения проникновения, поиска, обнаружения и удаления программных вирусов (и других вредоносных программ, таких как черви, трояны, рекламное ПО и т.д.). Типичная программа для защиты от вредоносных программ будет регулярно сканировать вашу систему и автоматически удалять обнаруженные вредоносные программы, а также предупреждать вас об опасных загрузках и обновлениях программного обеспечения.

# Она должна быть у вас обязательно. Если нет — установите ее.

Существует множество продуктов для защиты от вредоносных программ. Если вы используете Windows 10 Pro на своем ПК, у вас уже установлена и запущена программа антивирусной защиты Windows Defender. Кроме того, вы можете приобрести стороннюю программу защиты от вредоносных программ. Но не следует забывать о необходимости следовать инструкциям поставщика при настройке автоматических обновлений для установки самых актуальных средств антивирусной защиты.

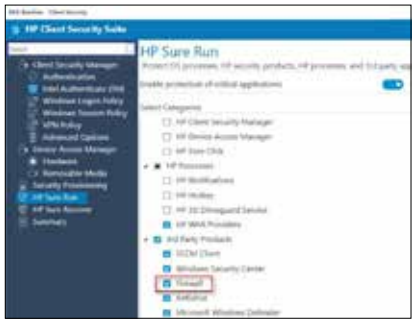
# Всегда должно быть запущено.

Особенно важно, чтобы антивредоносное ПО всегда работало: это позволит ему оставаться эффективным. Это не так просто, как может показаться, так как действия злоумышленников в этом случае направлены в первую очередь на программы обеспечения безопасности, такие как антивредоносное ПО. В Windows 10 Pro можно проверить, включена ли антивирусная программа в центре защиты Windows Defender Security Center.

1. В меню Start (Пуск) запустите Windows Defender Security Center и перейдите на главную страницу (Home).


2. Вы увидите зеленую отметку рядом с опцией «Virus & threat protection» (Защита от вирусов и угроз), если антивирусная защита работает. Если вы используете антивирусную программу стороннего разработчика, нажмите «View antivirus providers» (Просмотреть провайдеров антивирусных программ), чтобы просмотреть на панели управления Windows дополнительную информацию о статусе вашей антивирусной программы.

# Постоянная работа.



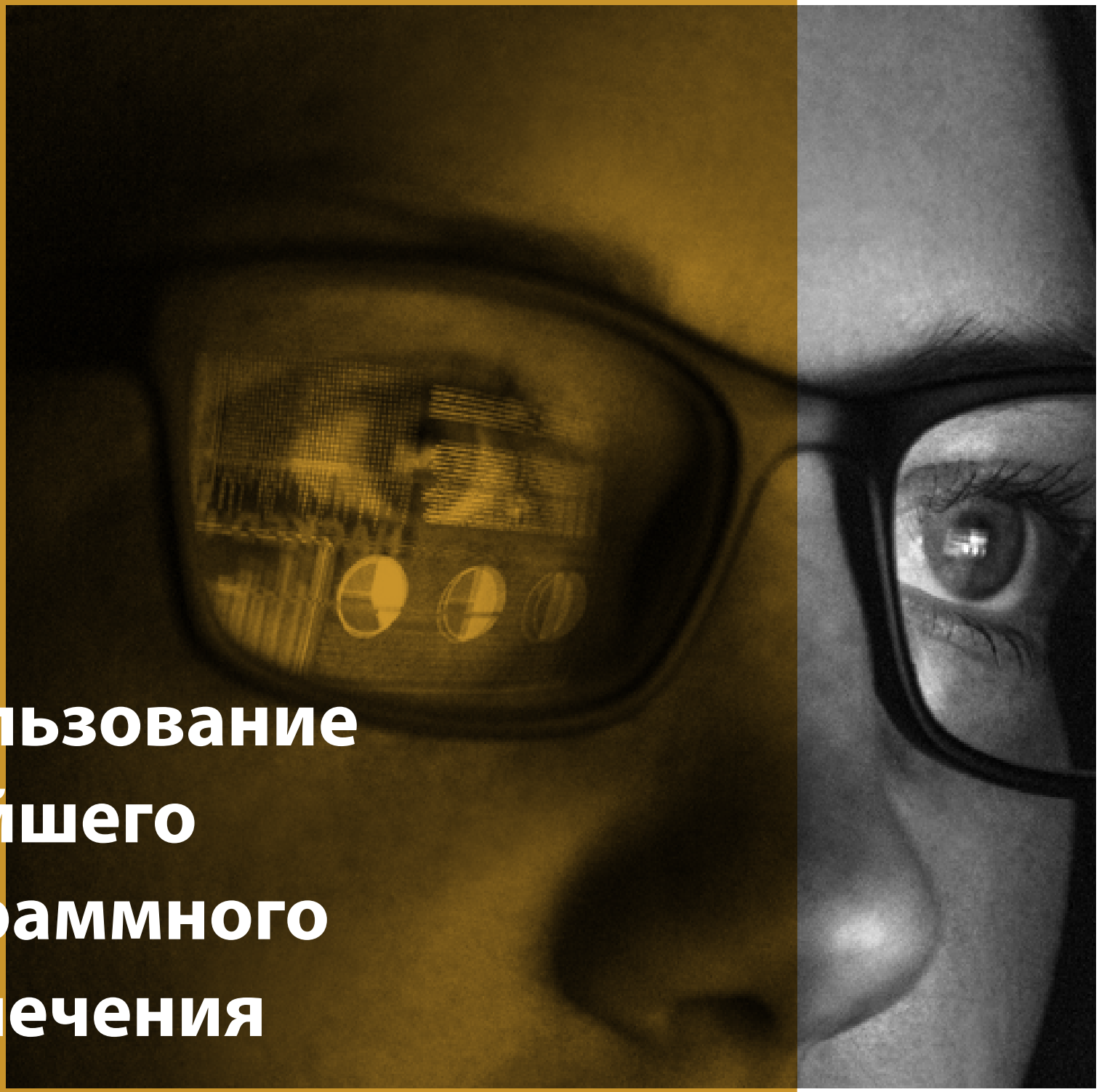

Продукты HP Elite также включают в себя HP Sure Run[12] — дополнительный уровень безопасности, который гарантирует рабочее состояние всех критических процессов на вашем ПК, в том числе антивирусного программного обеспечения. Любой процесс, который контролирует Sure Run, будет автоматически перезапущен, если он отключен. Это означает предотвращение отказа или сбоя антивирусного программного обеспечения и, соответственно, недопущение вашей уязвимости.

HP Sure Run должен быть включен локально в HP Client Security Manager Gen4.

12—Технология HP Sure Run доступна на продуктах HP Elite, оснащенных процессорами Intel® или AMD® 8-го поколения.

Раздел 4:

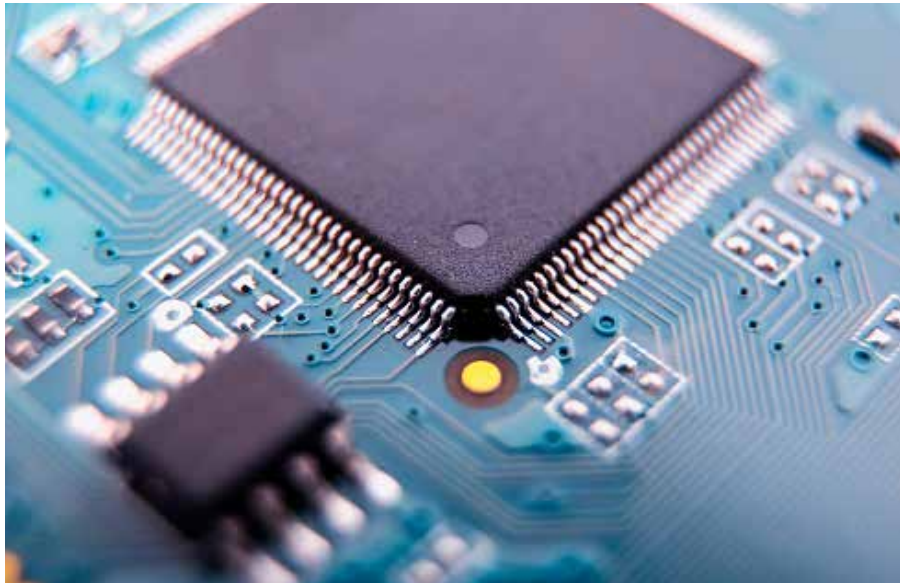
# Использование новейшего программного обеспечения



Под угрозой оказывается не только антивредоносное программное обеспечение, поэтому важно использовать текущие версии всего программного обеспечения. Если ваше программное обеспечение не обновлено, то могут отсутствовать важные обновления системы безопасности для недавно обнаруженной уязвимости системы. Это относится к операционной системе (ОС), например Windows®, а также ко всем приложениям, установленным на ПК, таким как интернет-браузеры, офисные приложения, программное обеспечение для ведения бухгалтерского учета, антивирусное программное обеспечение и т. д.

Пользователь также должен помнить, что обновления системы безопасности для программного обеспечения предыдущих версий или больше не выпускаемого ПО отсутствует. Со временем киберпреступники находят уязвимые места в опубликованном программном обеспечении и используют эти результаты. Если взять в качестве примера ОС, то проверка обновления для Windows 7 Pro может показать отсутствие нового программного обеспечения, но при этом не учитывается, что Windows 7 Pro больше не является самой последней версией Windows. Исправление устаревшего программного обеспечения — это не то же самое, что обновление до последней версии. Чем старше версия вашего программного обеспечения, тем менее оно безопасно.

> Чем старше версия вашего программного обеспечения, тем оно менее безопасно.



## Убедитесь, что ваше ПО обновляется.

По мере того как поставщики поставщики программного обеспечения находят решения для устранения уязвимости системы, они реализуют эти решения в обновлениях программного обеспечения. В большинстве приложений есть встроенная служба обновления, и в этом случае вас будут уведомлять о наличии обновления или исправления. Некоторые поставщики программного обеспечения даже автоматически устанавливают обновления при их наличии. В Windows 10 Pro — самой последней версии Windows (и, следовательно, самой безопасной) — есть механизм автоматического обновления программного обеспечения для обновления операционной системы и всех других приложений Microsoft, например, Microsoft Office.

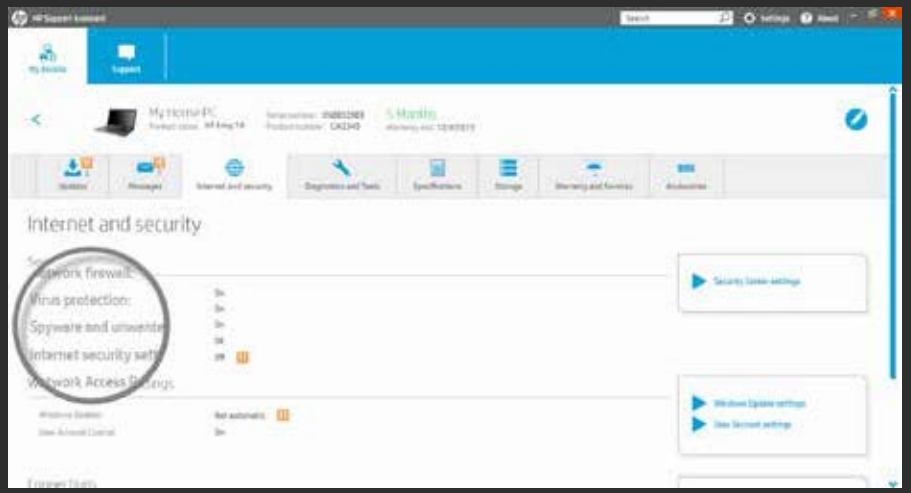
### Как проверить, что автоматические обновления включены:

1. Перейдите в настройки и выберите «Update security» (Обновить систему безопасности).
2. В разделе «Windows Update» (Центр обновления Windows) выберите «Advanced options» (Дополнительные параметры) и убедитесь, что в разделе «Choose how updates are installed» (Выберите способ установки обновлений) выбрана опция «Automatic» (Автоматически).
3. Убедитесь, что в разделе «Choose how updates are installed» (Выберите способ установки обновлений) выбрана опция «Automatic» (Автоматически).

## Используйте менеджер обновлений.

Разнообразие программного обеспечения, поставляемого вместе с ПК, может затруднить установку *самых* последних версий. Поэтому многие поставщики ПК предоставляют предустановленные инструменты для автоматического сбора информации о программном обеспечении и обновления прошивки системы. В системах HP используется инструмент HP Support Assistant.

Для сторонних приложений функция обновления часто выполняется небольшим приложением обновления, которое запускается во время загрузки. Эти вспомогательные инструменты немного увеличивают время загрузки (на несколько секунд), но при этом вам не нужно искать обновления на веб-сайтах поставщиков приложений. Если у вас есть программное обеспечение, которое не проверяет наличие обновлений автоматически, или если вы не уверены, проверьте номер версии на веб-сайте разработчика и обновите ее, если необходимо.



Раздел 5:

# Защита браузера

Такие браузеры, как Internet Explorer или Chrome™, являются основным способом доступа в Интернет, что делает их главной целью для хакеров. Эти атаки обычно происходят при случайном или намеренном переходе по ссылке, при котором запускается вредоносный код, известный как вредоносное ПО.

Существует несколько простых шагов, которые можно предпринять, чтобы значительно снизить вероятность атаки вредоносного ПО через браузер.

## Используйте безопасный браузер.

Internet Explorer, Edge и Chrome предлагают мощные средства защиты для Windows. Например, в Edge и Internet Explorer 11 используется Microsoft SmartScreen для проверки репутации на каждом сайте и блокирования подозрительных фишинговых сайтов. Кроме того, на коммерческих компьютерах HP в Internet Explorer есть дополнительный уровень безопасности благодаря HP Sure Click: всякий раз, когда открывается вкладка, HP Sure Click запускает ее на изолированной виртуальной машине. Это означает, что любой вредоносный код попадает в ловушку на вкладке и уничтожается при закрытии вашего браузера.[13]

## Обеспечьте наличие самых последних версий.

Включите автоматическое обновление браузера с помощью настроек. Как уже было сказано выше, это обеспечит применение всех обновлений системы безопасности к вашему браузеру, что повысит уровень его безопасности и увеличит вероятность того, что атаки вредоносных программ будут неудачными.

В Edge обновления применяются при обновлении Windows. Чтобы проверить, требуется ли обновление для Edge, откройте

- Start (Пуск)
- Settings (Настройки)
- Updates and Security (Обновления и безопасность)
- Windows Update (Центр обновления Windows)
- Check for updates (Проверить наличие обновлений)

13— HP Sure Click доступен на большинстве ПК компании HP и поддерживает Microsoft® Internet Explorer и Chromium™. Поддерживаемые вложения включают Microsoft Office (Word, Excel, PowerPoint) и PDF-файлы в режиме только для чтения, если установлены Microsoft Office или Adobe Acrobat.

## Реагируйте на предупреждения.

Большинство основных и современных браузеров имеют базовый порог для обнаружения вредоносных веб-сайтов и будут отображать предупреждение, если подозревают наличие обоснованной угрозы. Некоторые из них также имеют функции «автокоррекции» URL-адресов, чтобы предотвратить переход к обычному домену, в названии которого имеются орфографические ошибки (где часто размещаются вредоносные программы и сайты).

В Edge перейдите в раздел Advanced Settings> Privacy (Дополнительные параметры> Конфиденциальность), а затем включите параметры «Use a web service to help resolve navigation errors» (Использовать веб-службу для устранения ошибок навигации).

## Ограничьте контент и подключаемые модули.

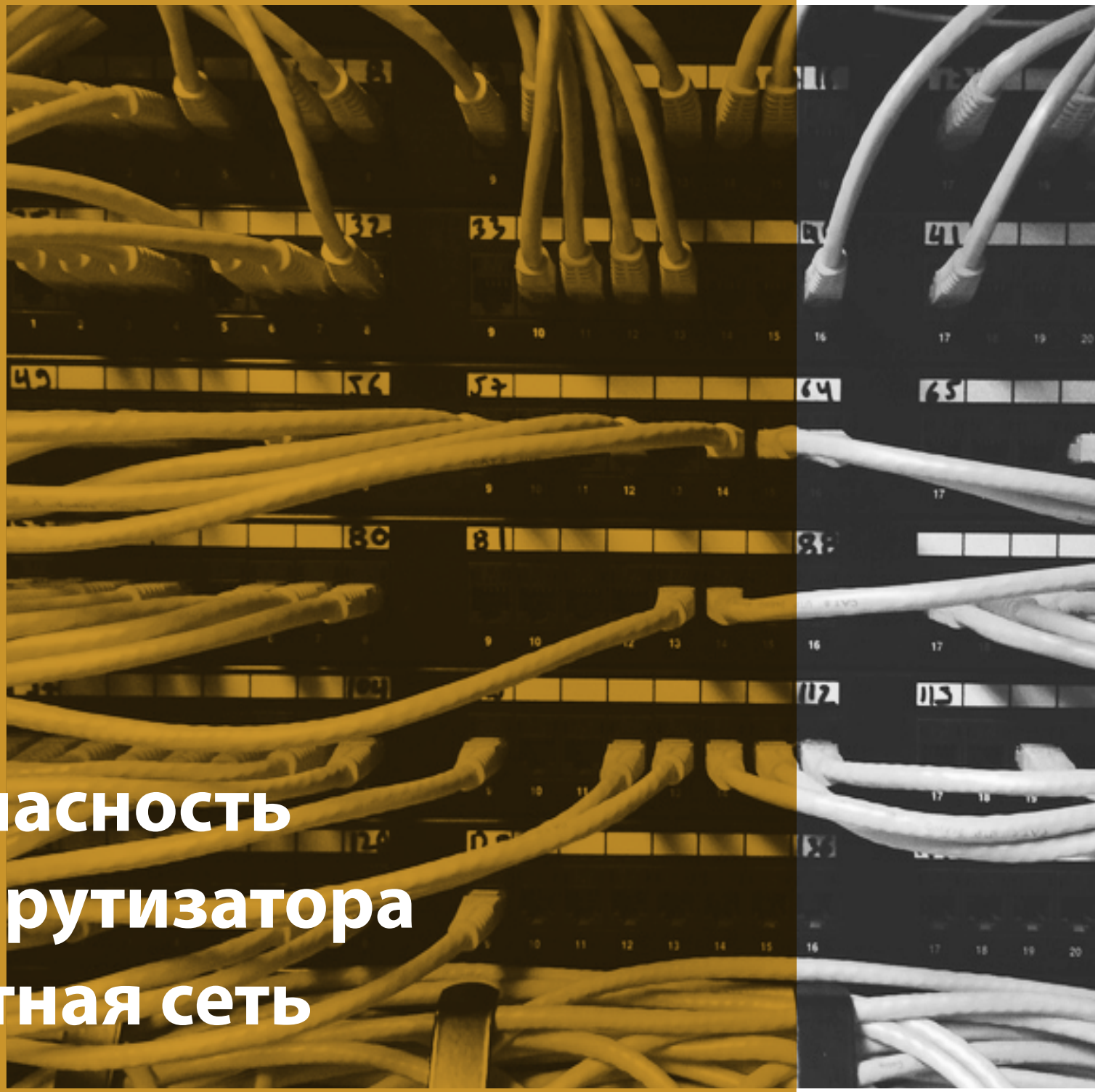
Многие из этих надстроек браузера (например, Flash или JavaScript) необходимы для работы сайтов и веб-программ, но повышенный уровень доступа к вашей системе делает их уязвимыми.

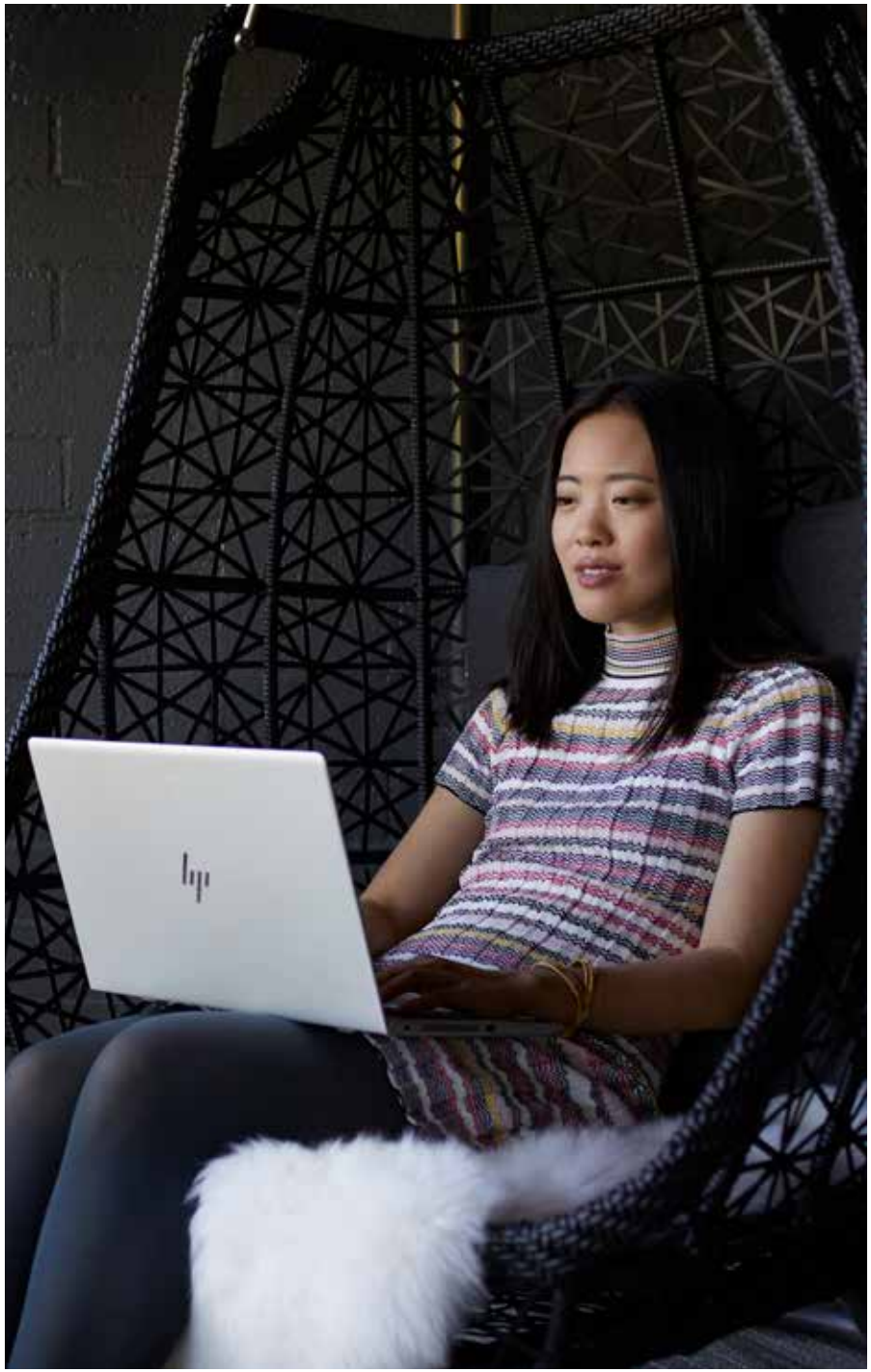
При их отключении по умолчанию требуется, чтобы сайт запрашивал разрешение на их использование, и гарантируется, что использовать свои функции могут только сайты, которым вы доверяете.

В IE перейдите к Tools (gear icon)> Internet Options> Security Internet> Custom level...> Scripting (> Инструменты (значок шестеренки)> Свойства обозревателя> Безопасность Интернета> Пользовательский уровень ...> Сценарии). Можно отключить JavaScript, просто выбрав «Disable» (Отключить), или выбрать запрос в IE, прежде чем сайт попытается использовать его, выбрав «Prompt» (Запрос).

Раздел 6:

# Безопасность маршрутизатора и частная сеть





Маршрутизатор является первой линией обеспечения безопасности при вторжении в любую сеть. Любой, кто подключается к Интернету, делает это через маршрутизатор. Это аппаратное устройство, проводное или беспроводное (Wi-Fi®), позволяет устанавливать связь между Интернетом и вашей локальной сетью (т.е. вашим ПК и другими подключенными устройствами). Таким образом, обеспечение наивысшего уровня безопасности на маршрутизаторе — это лучший способ защитить ваши компьютеры, принтеры и данные от вредоносных атак.

> Утверждалось, что маршрутизаторы наиболее часто из всех устройств подвергаются атакам IoT.[14]

Поскольку маршрутизаторы передают ВСЕ данные, которые поступают из вашего дома или предприятия, включая электронную почту и информацию о кредитной карте, маршрутизаторы уже давно являются излюбленной целью для хакеров. В отчете об угрозах безопасности в Интернете компании Symantec, опубликованном в 2018 году, говорилось, что маршрутизаторы наиболее часто подвергаются атакам IoT. Хакеры могут использовать вредоносное ПО или недостатки дизайна, чтобы скрыть свою личность, ограничить пропускную способность, превратить ваши устройства в зомби-ботнетов или даже хуже. Они также могут воспользоваться любыми незащищенными устройствами.

14—Источник: Symantec Corporation, 2018 Internet Security Threat Report, 2018

## Защитите свою сеть.

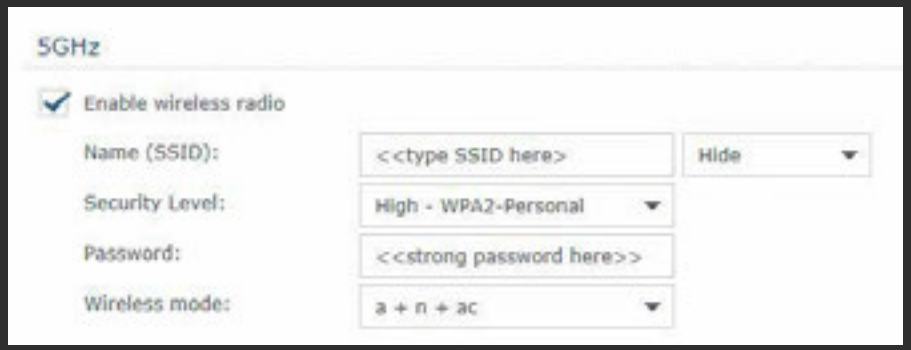
К сожалению, многие поставщики продолжают предлагать как защищенные, так и незащищенные конфигурации маршрутизаторов. Если маршрутизатор не защищен (то есть разрешает подключение к нему без пароля администратора), любой может подключиться к маршрутизатору и тем самым перейти в вашу локальную сеть. Хакер может менять ваши пароли, шпионить за вами или даже получать доступ к файлам на жестком диске, подключенном к сети.

Всегда защищайте маршрутизаторы паролями администратора, которые отличаются от паролей по умолчанию, используя советы из раздела 2 — «Повышение надежности ваших паролей». Ниже приведен снимок экрана, демонстрирующий установку паролей для маршрутизаторов для их защиты в сети.


## Сконфигурируйте параметры шифрования.

При использовании беспроводных маршрутизаторов пароли — это только половина дела. Выбор правильного уровня шифрования не менее важен. Большинство беспроводных маршрутизаторов поддерживают четыре стандарта беспроводного шифрования: WEP (ненадежный), WPA (надежный), WPA2 (более надежный), and WPA3 (самый надежный). Используйте самый высокий уровень шифрования, поддерживаемый вашим маршрутизатором.

Ниже приведен снимок экрана, демонстрирующий установку соответствующего уровня шифрования на вашем маршрутизаторе. Для этого необходимо войти в систему как администратор маршрутизатора и перейти к настройкам шифрования (зависит от поставщика маршрутизатора).



## Используйте последнюю версию микропрограммного обеспечения.

Многие производители маршрутизаторов выпускают обновления программного обеспечения в течение года для решения проблем безопасности. Аналогично ПО для ПК, маршрутизатор с последними обновлениями гораздо реже заражается вредоносными программами. Большинство поставщиков маршрутизаторов автоматически обновляют микропрограммное обеспечение, и клиентам не нужно выполнять эту операцию. Для более новых моделей маршрутизаторов могут также выпускать мобильное приложение. Его можно загрузить на телефон, как и любое другое приложение, и использовать для проверки обновлений. Но если поставщик маршрутизатора не предлагает автоматические обновления микропрограммного обеспечения, надо зайти на веб-сайт производителя маршрутизатора, перейти в службу поддержки и определить правильное обновление в соответствии с именем и идентификатором вашего конкретного маршрутизатора (как правило, указываются на самом маршрутизаторе).

## Используйте виртуальные частные сети.

Виртуальная частная сеть (VPN) — это сервер, с которым вы соединяетесь, чтобы перенаправить свои внешние действия в Интернете. При этом безопасность оборудования внутри вашей компании не ограничивается. VPN могут защитить и обеспечить безопасность ваших личных данных и информации. VPN предназначены для обеспечения конфиденциальности (но не всегда анонимности) просмотра информации в Интернете. Весь трафик, проходящий через ваше VPN-соединение, защищен и теоретически не может быть никем перехвачен, что означает, что эти сети отлично подходят для использования, как в локальных, так и в публичных сетях. Подробнее о VPN и их преимуществах см. в разделе 7.

Раздел 7:

# Защита в общественных сетях Wi-Fi®

Сегодня общественная сеть Wi-Fi® есть практически везде. Бесплатный доступ в Интернет через точки доступа есть в аэропортах, местных барах, торговых центрах, даже в парках. Это невероятно удобно… и опасно.

Пользователи, подключенные к этим точкам доступа, используют одну и ту же сеть. Это означает, что есть шанс, что кто-то сможет воспользоваться незащищенным трафиком. Хакер может даже настроить точку доступа и попытаться заманить людей в свою обманную сеть (с таким же названием). Таким образом можно перехватывать незашифрованные потоки данных или выполнять атаки через посредника для обхода шифрования.

**При использовании открытой сети важно всегда предполагать, что ваши сообщения не защищены и общедоступны. Но если у вас нет другого варианта, есть способы уменьшить вашу уязвимость.**

---

**Ограничьте свою активность.**
Не передавайте особо важные материалы, например, документы компании, электронные письма или пароли, и не используйте банковские или бухгалтерские приложения или порталы.

**Предусмотрите план B.**
Если возможно, используйте полуоткрытые сети, которые, по крайней мере, защищены паролем. Обычно это управляемая сеть, то есть поставщик заинтересован в обеспечении безопасности сети (например, в залах ожидания бизнес-класса в аэропорту).

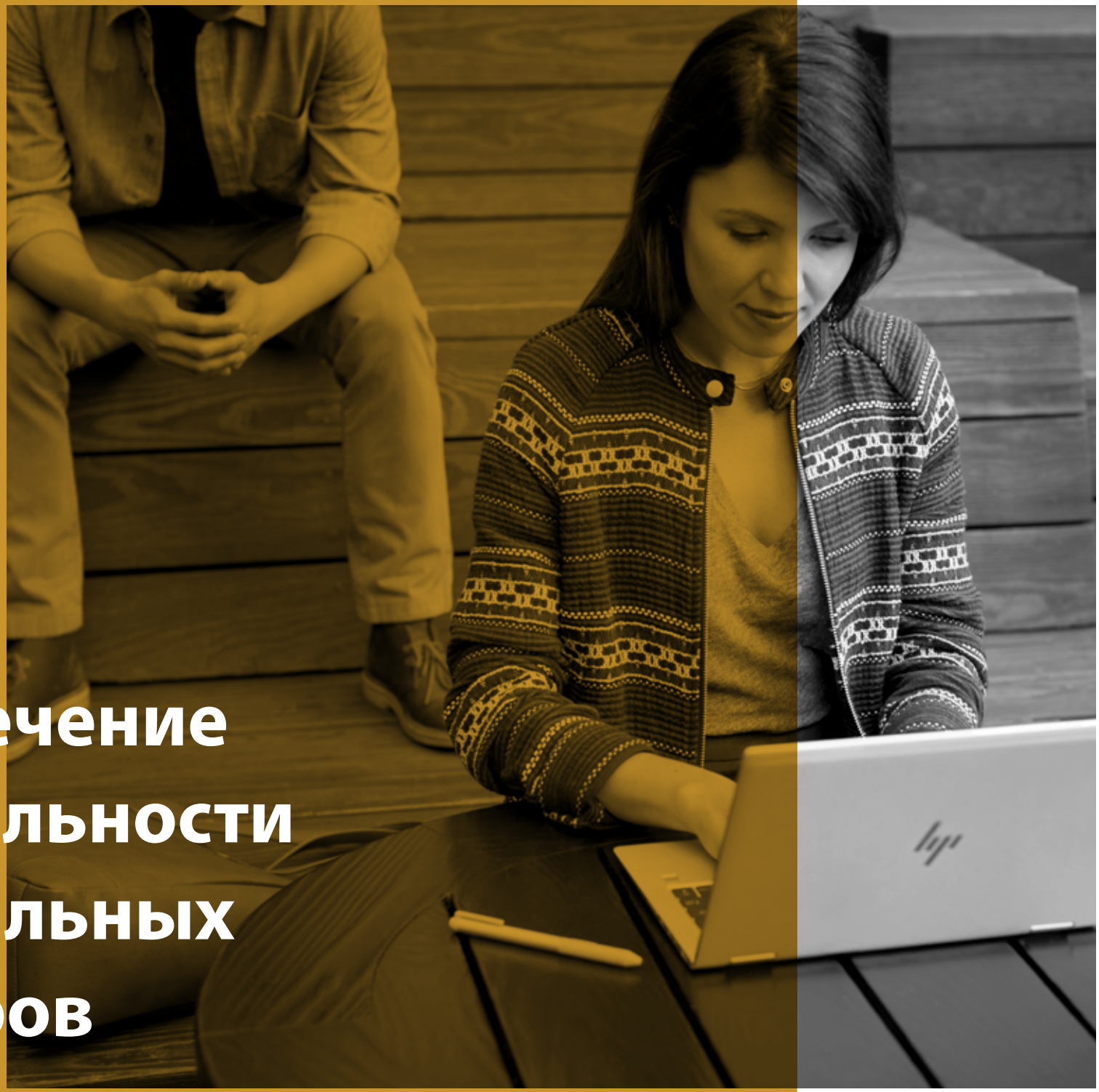
**Посещайте сайты с шифрованием.**
Убедитесь, что вы подключены к веб-серверу, который поддерживает зашифрованный трафик через протокол HTTPS (https://), в отличие от незащищенного протокола HTTP с обычным текстом. Проверьте заголовок URL-адреса сайта — в строке URL-адреса современного браузера обычно появляется значок, указывающий на наличие протокола HTTPS и действительность сертификата (часто значок замка или зеленый цвет). Если вы щелкнете по этому участку, откроется диалоговое окно с подробной информацией об уровне шифрования.

**Используйте VPN во всех случаях.**
Как уже упоминалось в предыдущем разделе, VPN может защитить ваши данные, если вы не доверяете своему сетевому соединению, и общедоступная сеть Wi-Fi® является прекрасным тому примером. VPN-туннель шифрует ваши данные от начала до конца, гарантируя, что потенциальный перехватчик не сможет интерпретировать вашу деятельность. Не все сети VPN одинаковы, поэтому нужно выбрать ту, которая соответствует вашей ценовой категории и типу устройства. Бесплатные VPN часто имеют ограниченную доступную пропускную способность и простые протоколы шифрования, что означает, что вы будете использовать сеть с более медленной скоростью и все равно можете подвергаться опасности. Тем не менее, надежная бесплатная сеть VPN лучше, чем ее отсутствие.

---

Раздел 8:

# Пресечение деятельности визуальных хакеров



Визуальный взлом происходит, когда конфиденциальная информация отображается на экране в общественных местах и у деловых конкурентов. Похитители персональных данных или недобросовестные люди видят, захватывают и используют ее. Даже случайный любопытный зритель является потенциальной угрозой. Все — от паролей и номеров счетов до финансовых данных и собственных данных компании — находится под угрозой, и никакое программное обеспечение безопасности не может помешать этим случайным людям подсмотреть ваши данные.

Поскольку современное рабочее место продолжает перемещаться за пределы традиционных офисов в удаленные и общественные места, возможность «визуального взлома» стала реальностью. По сути, визуальный взлом может быть самой недооцененной, низкотехнологичной угрозой для современного бизнеса. Это можно сделать просто, эффективно и часто незаметно, пока не стало слишком поздно.

По данным, опубликованным институтом Понемон[1]:

- 91% попыток визуального взлома успешны
- 68% попыток визуального взлома остались незамеченными жертвой
- 52% конфиденциальной информации было зафиксировано непосредственно с экранов устройств

## Не забывайте об окружении.

Работая в общественных местах, всегда помните, что кто-то может смотреть через плечо, и выбирайте задачи соответственно.

## Ограничьте свою уязвимость.

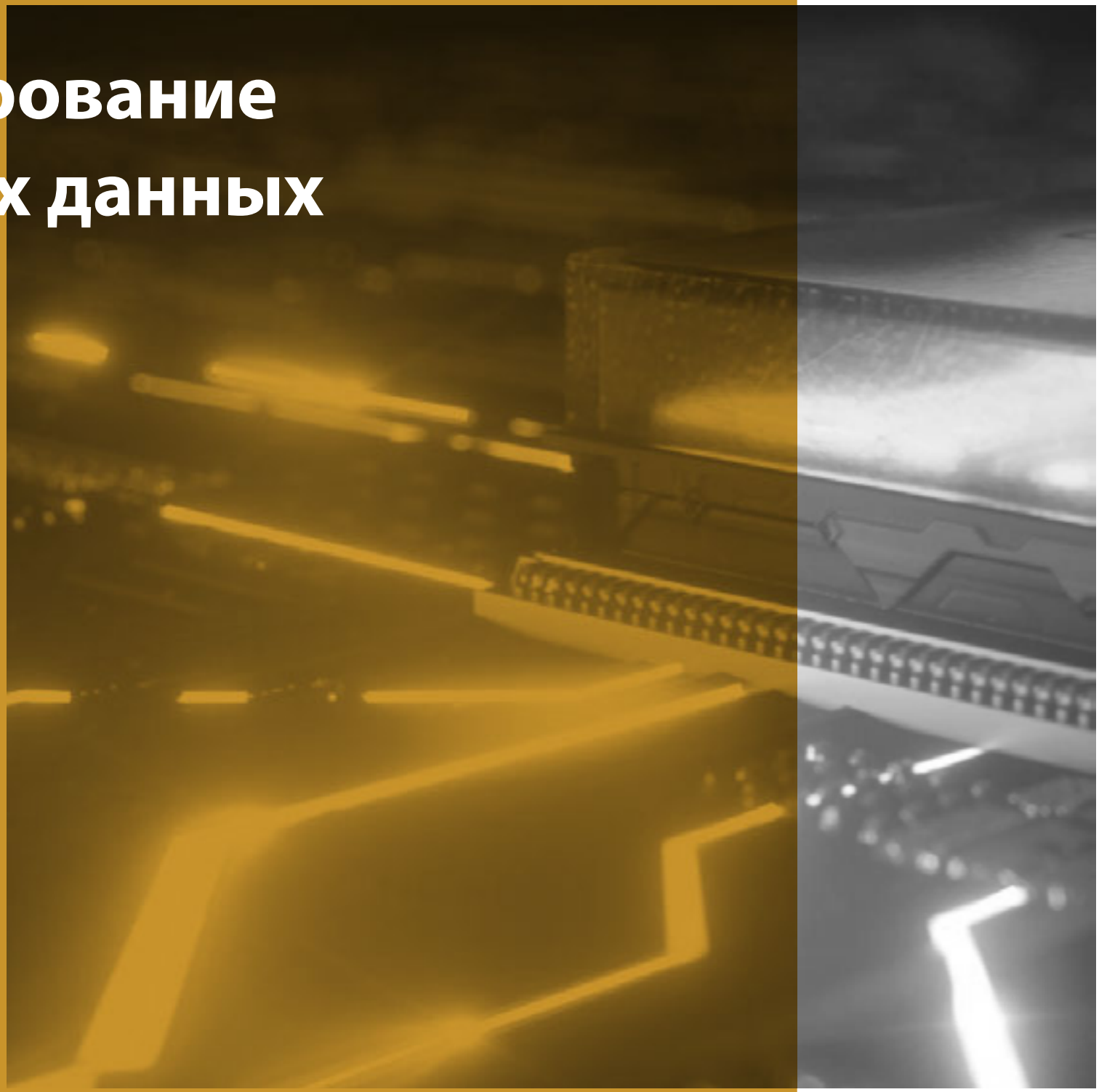
Экраны, защищенные от считывания информации посторонними лицами, предназначены для уменьшения углов обзора экрана, так что потенциальный визуальный хакер не может видеть, что отображается, не находясь непосредственно за ним. Внешний фильтр — это простой способ добавить этот уровень безопасности. Он крепится к дисплею и его можно снять, когда нужно поделиться информацией на экране с более широкой аудиторией.

Кроме того, встроенный защищенный экран упрощает этот процесс, устраняя необходимость использования, хранения и замены внешней защиты. На многих ПК компании HP опционально устанавливается HP Sure View Gen2[15] — встроенный защищенный экран, предназначенный для предотвращения визуального взлома. Он работает путем динамического изменения структуры пикселей ЖК-дисплея на молекулярном уровне, что позволяет включать или отключать его нажатием кнопки и улучшать производительность как при ярком, так и приглушенном освещении.

15—Встроенный защищенный экран HP Sure View является дополнительной функцией, которая должна быть сконфигурирована при покупке и предназначена для работы в альбомной ориентации.

Раздел 9:

# Шифрование ваших данных



Если компьютер потерян или украден, то в первую очередь атаке подвергается жесткий диск. Он крепится всего несколькими винтами, и после снятия его можно запустить на другом ПК. Если вы не защитили свои данные надлежащим образом, прочитать и взломать диск будет так же просто, как открыть книгу.

Шифрование гарантирует, что вся получаемая информация остается совершенно непонятной. Шифрование — это процесс кодирования данных, чтобы сделать их нечитаемыми для любого, у кого нет секретного ключа дешифрования. Таким образом, компьютер с зашифрованным жестким диском можно украсть, но не получить к нему доступ. Это гораздо лучше, чем ваша корпоративная или личная информация в чужих руках.

## Обеспечьте шифрование программного обеспечения.

Windows 10 Pro поддерживает шифрование паролем жесткого диска, используя ваши учетные данные для входа в качестве ключа. В этом случае хакеру понадобится ваше имя пользователя и пароль для доступа к вашим данным.

Убедитесь, что у вас есть надежный пароль для учетной записи пользователя:

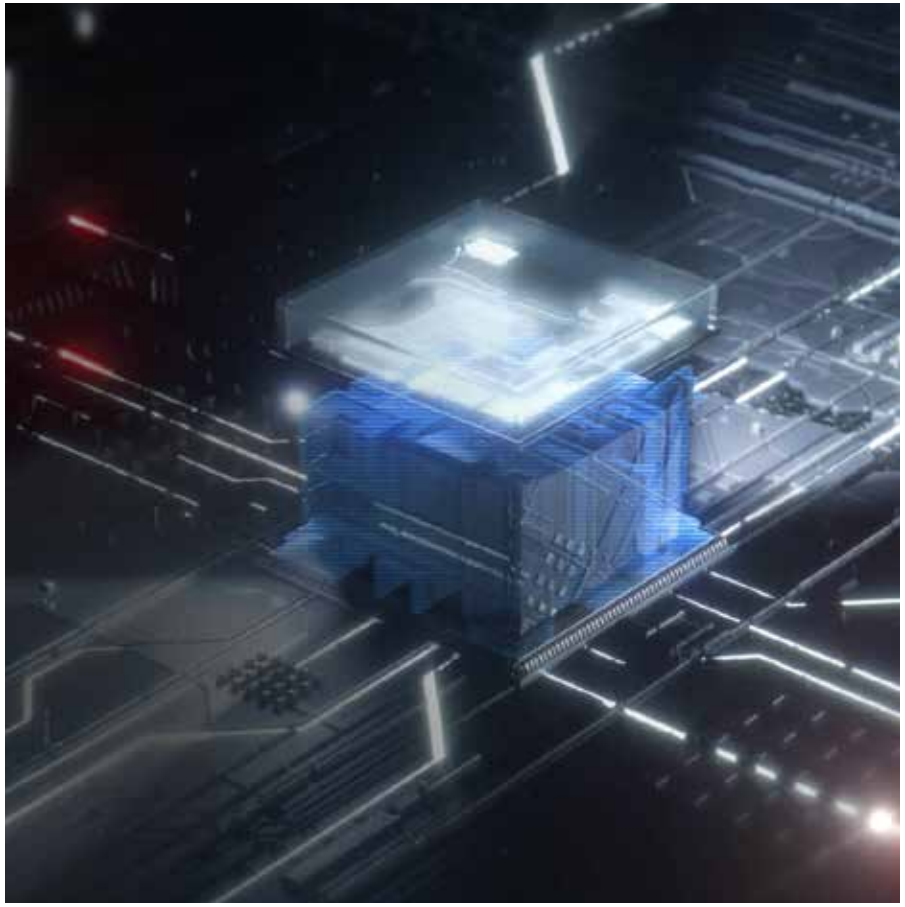
1. 
   - Settings> Accounts> Sign-in options> Password (Настройки> Учетные записи> Опции входа в систему> Пароль)

2. Если да, включите Trusted Platform Manager (TPM), который активирует чип для системы безопасности на вашем ПК для шифрования новых паролей и данных на диске:
   - Settings> Update & Security> Windows Security> Device Security> Processor (Настройки> Обновление и безопасность> Безопасность Windows> Безопасность устройств> Процессор)

3. Включите шифрование, чтобы ваши данные не могли быть просмотрены или скопированы без ваших учетных данных:
   - Settings> Update and Security> Drive Encryption (Настройки> Обновление и безопасность> Шифрование диска)

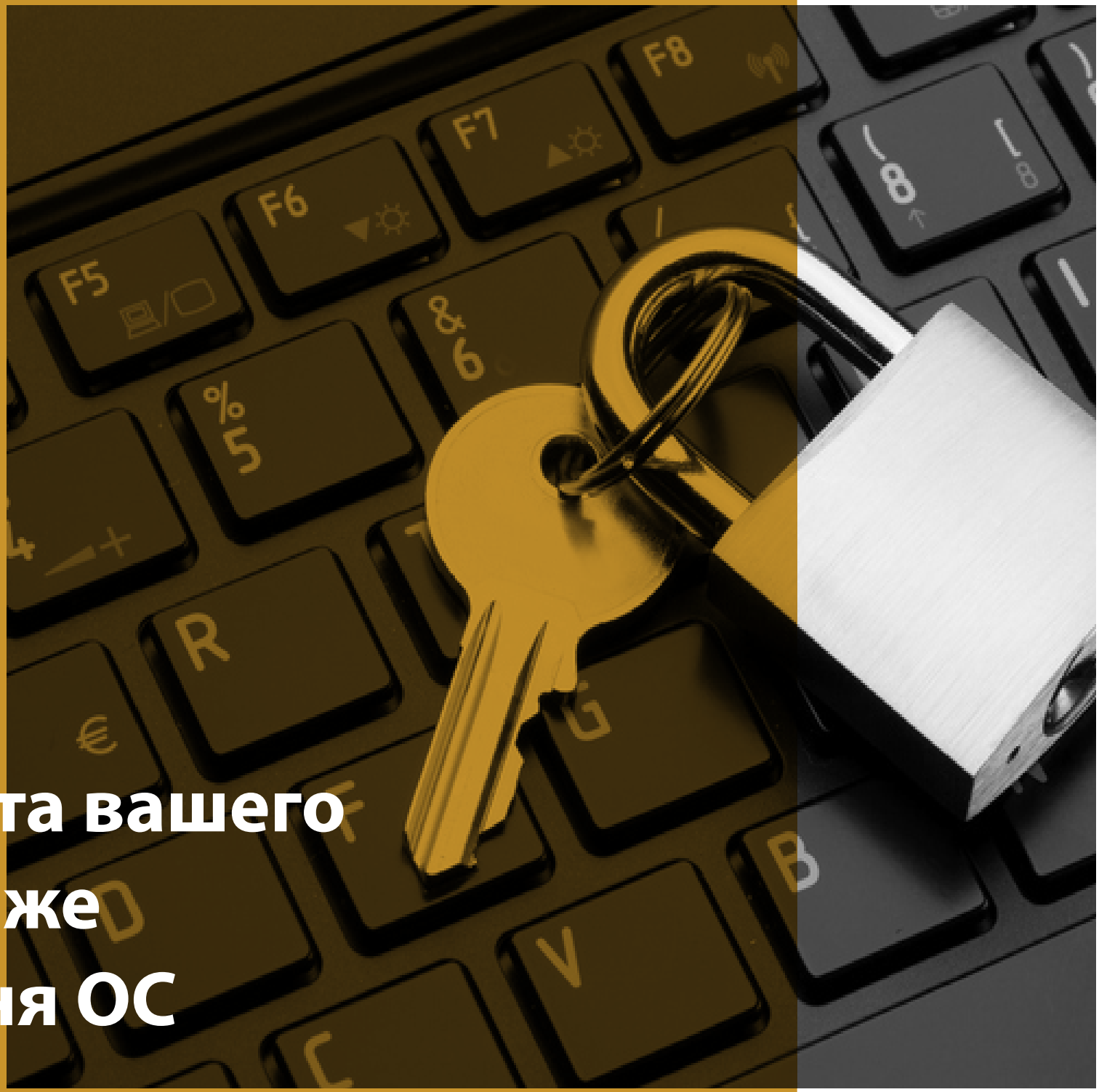
## Используйте аппаратное шифрование.

BitLocker — это функция Windows 10 Pro, обеспечивающая шифрование программного обеспечения, которое разблокируется с помощью аппаратного ключа. Устройства с чипом TPM, такие как ноутбуки HP, могут шифровать без дополнительного оборудования. TPM предотвращает доступ к зашифрованным данным, обнаружив, что система была подделана в выключенном состоянии. Устройства без TPM также могут использовать BitLocker, но для использования в качестве ключа требуется съемное устройство, например USB-накопитель.



Раздел 10:

# Защита вашего ПК ниже уровня ОС



BIOS (Basic Input Output Software) — это программное обеспечение, которое загружает компьютер и помогает загрузить операционную систему. Заражая это основное программное обеспечение, шпионы могут устанавливать вредоносное ПО, которое сохраняется и не обнаруживается антивирусом. Оно остается даже при удалении информации с жесткого диска или при повторной установке операционной системы.

## Если хакер получает доступ к вашему BIOS, он, по сути, получает полный доступ к вашему ПК.

Это дает злоумышленнику возможность просмотра данных или блокирования системы путем изменения микропрограммного обеспечения, что потребует замены всей системной платы.
В компьютерах HP Elite и Pro функция HP Sure Start может автоматически удалять из BIOS вредоносные программы, руткиты или устранять повреждения, добавляя дополнительный уровень защиты и создавая надежную основу для безопасности вашего ПК.[16]

## Не пропускайте обновление.

Как упоминалось ранее в разделе 4, обновления программного обеспечения гарантируют исправление обнаруженных уязвимых мест, и BIOS не является исключением. Поскольку в большинстве версий BIOS используется один и тот же исходный код для рабочих ресурсов или базы пользователей, любая обнаруженная уязвимость, скорее всего, присутствует на многих ПК от поставщика. OEM-инструменты, такие как HP Support Assistant, будут проверять наличие обновлений автоматически, или вы можете проверить сайт своего производителя на наличие обновлений BIOS.

## Откройте BIOS изнутри.

Заводские настройки BIOS можно рассматривать как баланс между безопасностью и удобством использования. Но чтобы защитить систему от множества возможностей передачи вредоносного кода, можно удалить некоторые из этих функций.

Доступ к настройкам BIOS может незначительно отличаться для различных производителей, но обычно это делается путем нажатия функциональной клавиши во время начальной загрузки (F10 или FN-10 на ноутбуках HP).

16—Технология HP Sure Start Gen4 доступна в продуктах HP Elite и HP Pro 600, оснащенных процессорами AMD или Intel 8-го поколения.

## Установите пароль BIOS.

Чтобы защитить настройки BIOS от изменений неавторизованными пользователями, рекомендуется установить пароль BIOS:

- Например: Security> Administrator Tools> Create BIOS Administrator Password

Важно помнить пароль BIOS, поскольку его нельзя обойти или восстановить.

## Установите пароль для включения питания.

Чтобы повысить уровень безопасности, можно создать пароль для включения питания. Каждый раз при включении ПК, перед запуском системы, запрашивается пароль для включения питания. Как и пароль BIOS, его тоже нельзя просто восстановить или сбросить. Если забыть этот пароль, компьютер будет непригоден для использования.

## Ограничьте неиспользуемые функции.

В BIOS есть несколько параметров для обеспечения максимальной безопасности. Несмотря на возможность удалить некоторые функциональные возможности или уменьшить их доступность, обеспечиваемую ими защиту ниже уровня ОС нельзя воспроизвести в той же мере с помощью программного обеспечения.

1. Удалите внешние и оптические устройства из загрузки (например, Advanced> Boot Options). Особенно это касается загрузки с USB-накопителя, из сети (PXE) и с оптического диска, так как они позволяют загружать вредоносное ПО из внешних источников. Если требуется выполнить загрузку с этих устройств, ее можно включить в каждом конкретном случае.
2. Отключите поддержку устаревших версий (например: Advanced> Secure Boot Configuration) и включите безопасную загрузку.
3. Активируйте функцию «Save/Restore GPT of System Hard Drive» (например, Security> Hard Drive Utilities).
4. Включите DriveLock и установите пароль.

# Заключение

Сегодня предприятия малого и среднего бизнеса подвергаются цифровым угрозам больше, чем раньше Хорошо то, что основная часть имеющегося у вас аппаратного и программного обеспечения, содержит недостаточно используемые функции безопасности, которые помогают бороться с этими угрозами. Существует также невероятное количество продуктов и услуг с инновационными разработками в области безопасности для защиты от неизвестных угроз завтрашнего дня. Благодаря аппаратной безопасности на современных устройствах для самообновления программного обеспечения, инвестиции в подключенные и защищенные устройства теперь будут давать значительные результаты. Компания HP разрабатывает решения для обеспечения безопасности на основе преимуществ Windows 10 Pro, поддерживая встроенные функции безопасности с дискретными аппаратными дополнениями и постоянно обновляемой поддержкой программного обеспечения. Ежедневно появляются новые угрозы, и правильная стратегия безопасности существенно увеличивает ваши шансы устоять против них.

# СПАСИБО!

Для получения дополнительной информации посетите сайт:
ww.hp.com/go/windows10now

+ Windows 10

Обеспечьте повышенную безопасность на всех этапах.