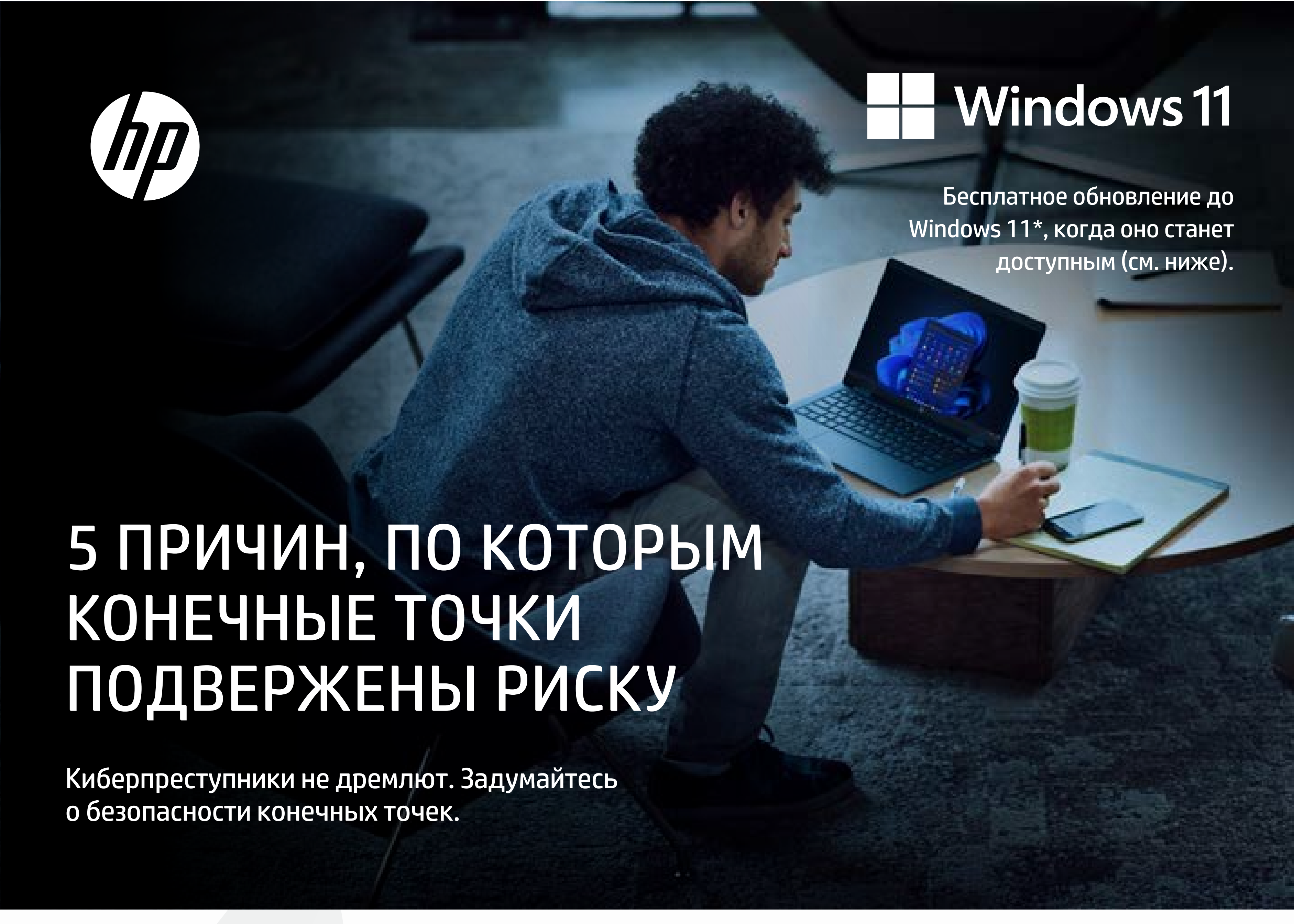


Бесплатное обновление до Windows 11*, когда оно станет доступным (см. ниже).

5 ПРИЧИН, ПО КОТОРЫМ КОНЕЧНЫЕ ТОЧКИ ПОДВЕРЖЕНЫ РИСКУ

Киберпреступники не дремлют. Задумайтесь о безопасности конечных точек.

СИСТЕМА БЕЗОПАСНОСТИ ДОЛЖНА АДАПТИРОВАТЬСЯ К ДЕЦЕНТРАЛИЗОВАННОЙ СТРУКТУРЕ ПЕРСОНАЛА.

Обеспечение безопасности конечных точек — задача нетривиальная, и она стала еще сложнее, когда сотрудники массово перешли на удаленную работу — причем не только обычные пользователи, но и ИТ-специалисты. В настоящее время 90% специалистов в сфере кибербезопасности работают удаленно[1], и более трети из них утверждают, что гибридная схема работы в большей степени подвергает их компанию угрозам безопасности[2].

КОНЕЧНЫЕ ТОЧКИ СТАНОВЯТСЯ ОБЪЕКТАМИ ДЛЯ АТАКИ ЧАЩЕ, ЧЕМ КОГДА-ЛИБО РАНЕЕ.

Когда пользователи и устройства разнесены друг от друга на сколь угодно большие расстояния, это открывает для хакеров новые возможности: 68% респондентов заявили, что частота атак возросла[2], а за последние два года по крайней мере одна атака на конечные точки увенчалась успехом[3]. Это означает, что система безопасности всегда должна быть начеку. В то время как более половины организаций признаются в нехватке компетенций и ресурсов для защиты конечных точек[3], 57% профессионалов в сфере кибербезопасности прогнозируют увеличение расходов на защиту конечных точек[2].

В БУРНО РАЗВИВАЮЩЕМСЯ МИРЕ КИБЕРБЕЗОПАСНОСТИ ВАШИ КОНЕЧНЫЕ ТОЧКИ ПОДВЕРГАЮТСЯ РИСКУ ПО ПЯТИ НАПРАВЛЕНИЯМ...

ПЕРВОЕ—

РАБОЧИЕ МЕСТА СТАЛИ ДЕЦЕНТРАЛИЗОВАННЫМИ — И УГРОЗЫ ТОЖЕ.

Сотрудники, которые раньше были ограничены стенами офиса, сейчас могут работать даже в разных часовых поясах: не менее половины сотрудников 100% времени работают из дома[4]. Подобная гибридная среда расширяет возможности для атаки[4]; 23% опрошенных ИТ-специалистов заявили, что после перехода на удаленную работу количество инцидентов, связанных с нарушением безопасности, возросло; в отдельных случаях количество подобных инцидентов удвоилось[1].

НЕ МЕНЕЕ

50 %

СОТРУДНИКОВ 100% ВРЕМЕНИ работают из дома.

ВТОРОЕ—

НЕОСВЕДОМЛЕННЫЕ СОТРУДНИКИ — ОТКРЫТАЯ ДВЕРЬ ДЛЯ ХАКЕРОВ.

Хотя кибератаку можно провести разными способами, в большинстве случаев злоумышленники эксплуатируют главную уязвимость: низкий уровень грамотности сотрудников в сфере кибербезопасности[5]. Чтобы активировать вредоносную программу, распространяющуюся по электронной почте, в более чем 99% случаев требуется вмешательство со стороны пользователя — например перейти по ссылке, открыть документ, принять предупреждение системы безопасности и т. д.[6] После заражения киберпаразит начинает распространяться между пользовательскими системами.

В 60 %

ОРГАНИЗАЦИЙ СКОМПРОМЕТИРОВАННЫЙ КОМПЬЮТЕР ОДНОГО СОТРУДНИКА ЗАРАЗИЛ КОМПЬЮТЕРЫ ДРУГИХ ПОЛЬЗОВАТЕЛЕЙ

ТРЕТЬЕ—

АНТИВИРУСНЫХ ПРОГРАММ УЖЕ НЕДОСТАТОЧНО.

Каждый месяц появляется 102 миллиона новых вредоносных программ. Т. е. 360 000 каждый день или 4,2 каждую секунду[8]. 80% этих атак представляют собой угрозы нулевого дня, но это еще полбеды, беда в том, что 60% атак не отражаются антивирусами[3]. Именно поэтому 85% организаций предпочитают развертывать системы безопасности, поддерживающие такие передовые технологии, как искусственный интеллект, машинное обучение, мониторинг поведения и упреждающая изоляция[5].

ОКОЛО

33 %

ОРГАНИЗАЦИЙ ПЛАНИРУЮТ УВЕЛИЧИТЬ ВЛОЖЕНИЯ В СОВРЕМЕННЫЕ РЕШЕНИЯ ДЛЯ ЗАЩИТЫ ОТ ВИРУСОВ И ИНЫХ ВРЕДОНОСНЫХ ПРОГРАММ

ЧЕТВЕРТОЕ—

НЕВОЗМОЖНО БОРОТЬСЯ С НАРУШЕНИЕМ, О КОТОРОМ ВЫ НЕ ЗНАЕТЕ.

Без мониторинга безопасности устройств о наличии проблемы вы узнаете только спустя некоторое время. Как правило, организации в среднем требуется 315 дней, чтобы выявить и локализовать нарушение в результате хакерской атаки[9] — и только 97 дней из этого срока уходит на фактическое устранение уязвимости[3].

Однако с переходом на удаленную работу организации ожидают, что время на выявление и локализацию утечки данных увеличится, а расходы на устранение уязвимости вырастут на 70%[9].

СРЕДНИЙ УЩЕРБ ОТ УТЕЧКИ ДАННЫХ[9]:

ПЯТОЕ—

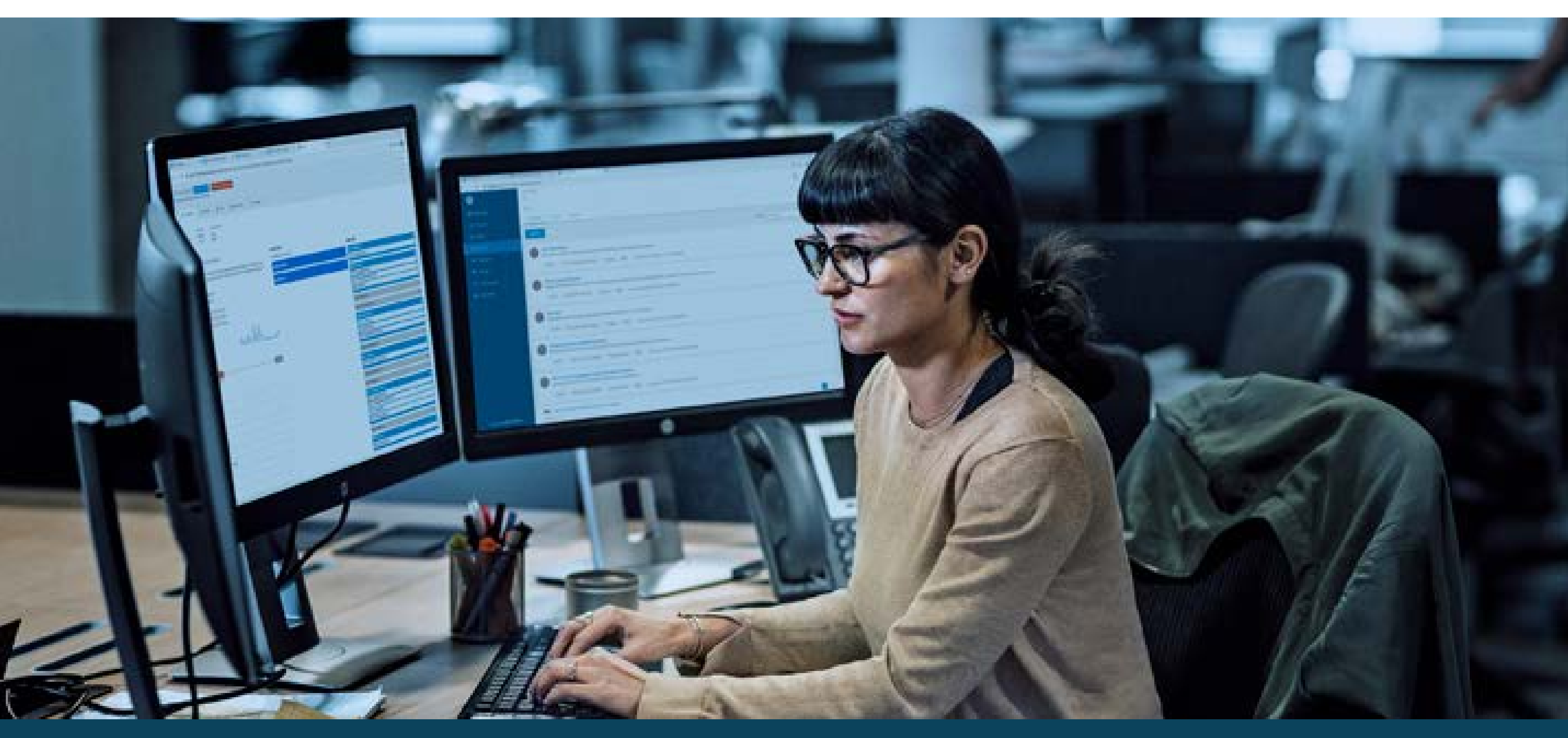
СПЕЦИАЛИСТЫ ПО КИБЕРБЕЗОПАСНОСТИ - В ДЕФИЦИТЕ.

Звучит парадоксально, но компании нанимают намного меньше экспертов по кибербезопасности, чем необходимо, даже несмотря на массовое распространение угроз[1]. Примерно 85% организаций сообщают о нехватке квалифицированных специалистов по информационной безопасности[5]. Среди специалистов, работавших в период пандемии, 32% сообщили о возросшей нагрузке[2], а 47% — об изменении повседневной рабочей деятельности в результате возложения на них дополнительных обязанностей, не связанных с информационной безопасностью[1,2].

НЕХВАТКА

3 МИЛЛИОНОВ

СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ ПО ВСЕМУ МИРУ[1]



ПРИОРИТЕТНАЯ ЗАЩИТА НА БАЗЕ ПК HP С РАСШИРЕННЫМИ СРЕДСТВАМИ БЕЗОПАСНОСТИ [10]

Благодаря слаженной работе аппаратных средств безопасности, обеспечивающих бесперебойную защиту, ноутбуки HP EliteBook 800 полностью отвечают вызовам сегодняшнего дня. Эти постоянно развивающиеся решения надежно защищают ваш ПК от угроз на всех уровнях — от BIOS и аппаратных компонентов до браузера и операционной системы. Ноутбуки EliteBook 800 серии серии оснащены такими средствами безопасности, как камера приватности HP Privacy и BIOS с автоматическим восстановлением, а благодаря современному высокоскоростному модулю Wi-Fi [6], емкому аккумулятору и высокой производительности они обеспечивают максимальное удобство удаленной совместной работы. Вместе с ОС Windows 11 вы получаете новейшее программное обеспечение и аппаратные средства безопасности, обеспечивающие надежную защиту ваших устройств и вашего бизнеса.

Подробнее :
https://www.hp.com/ru-ru/security/pc-security.html

HP ELITEBOOK 840 G8

---

*Обновление до Windows 11 будет предоставлено для соответствующих устройств в конце 2021 года и далее в 2022 году. Сроки зависят от модели устройства. Для работы некоторых функций требуется определенное оборудование (см. aka.ms/windows11-spec).

[1] ((SC)^2 Исследование персонала в сфере кибербезопасности, 28 апреля 2019 г.

[2] Влияние пандемии COVID-19 на кибербезопасность, ISSA, 30 июля 2020 г.

[3] Отчет о состоянии безопасности конечных точек на 2020 г., Ponemon Institute по заказу Morphisec, январь 2020 г.

[4] Внутреннее исследование HP, май 2020 г.

[5] Отчет о защите от киберугроз CyberEdge 2020, март 2020 г.

[6] Отчет Proofpoint о влиянии человеческого фактора за 2019 г., сентябрь 2019 г.

[7] Состояние безопасности электронной почты на 2020 г., Mimecast, июнь 2020 г.

[8] Отчет о безопасности AV-Test за 2019/2020 гг., 26 августа 2020 г.

[9] 15-й ежегодный отчет «Цена утечки данных в 2020 г.: глобальный анализ IBM Security и Ponemon Institute», июль 2020 г.

[10] По данным внутреннего анализа HP услуг по обеспечению безопасности конечных точек с поддержкой технологий машинного обучения, в том числе SaaS (ПО как услуга).

HP рекомендует Windows 11 Pro для бизнеса