**Соблюдение кибергигиены поможет обеспечить безопасность в сети**



**Определение кибергигиены**

**Кибергигиена представляет собой набор действий, выполняемых пользователями компьютеров и других устройств для повышения сетевой безопасности и обеспечения работоспособности системы. Кибергигиена – это образ мышления и привычки с фокусом на безопасность, помогающие пользователям и организациям снизить количество нарушений в интернете. Основополагающий принцип кибергигиены – войти в повседневную жизнь.**

**Что такое кибергигиена?**

**Кибергигиена – это формирование полезных привычек в отношении кибербезопасности, позволяющих не стать жертвой киберугроз и избегать проблем сетевой безопасности. Кибергигиену иногда сравнивают с личной гигиеной: в обоих случаях это регулярные меры предосторожности для обеспечения здоровья и благополучия.**

**Кибергигиена направлена на поддержание работоспособности и безопасности оборудования и программного обеспечения и защищает от таких угроз, как**[**вредоносные программы**](https://www.kaspersky.ru/resource-center/threats/types-of-malware)**. Соблюдение кибергигиены помогает хранить данные в безопасности. Как и любые действия, которые нужно закрепить в качестве привычки, кибергигиенические процедуры требуют регулярного повторения.**

**Соблюдение кибергигиены поможет не допустить нарушения безопасности и кражи личных данных киберпреступниками, а также быть в курсе обновлений программного обеспечения и операционных систем.**

**Актуальность кибергигиены как концепции возросла с момента начала пандемии Covid-19, когда увеличение количества работающих удаленно людей**[**привело к росту киберпреступлений**](https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime)**.**

**Проблемы, решаемые с помощью кибергигиены**

**Проблемы, для решения которых предназначена кибергигиена, включают:**

* **Нарушения безопасности, в том числе угрозы со стороны злоумышленников, [фишинг](https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips), вредоносные программы и вирусы.**
* **Потеря данных: если для жестких дисков и облачных онлайн-хранилищ не созданы резервные копии, они могут подвергнуться взлому, быть повреждены, или с ними могут возникнуть прочие проблемы, ведущие к потере данных.**
* **Устаревшее программное обеспечение, использование которого может повысить уязвимость устройств для сетевых атак.**
* **Устаревший антивирус: не поддерживаемое в актуальном состоянии программное обеспечение безопасности менее эффективно защищает от новых киберугроз.**

**Как обеспечить соблюдение кибергигиены?**

**Есть два важных аспекта кибергигиены для пользователей: выполнение регулярных действий и выработка привычек, а также использование надлежащих инструментов. Рассмотрим каждый из них.**

**Регулярные действия и привычки**

**Кибергигиена – это не разовое мероприятие, ее нужно соблюдать постоянно. Можно вырабатывать привычки, устанавливать автоматические напоминания и добавлять в календарь даты выполнения разных задач. Такие задачи могут включать выполнение антивирусной проверки с помощью соответствующего программного обеспечения, изменение паролей, поддержку в актуальном состоянии приложений, программного обеспечения и операционных систем, а также очистку жесткого диска. Как только вы освоите кибергигиену, ее соблюдение войдет в ваши стандартные действия по обеспечению кибербезопасности.**

**Использование надлежащих инструментов**

**К ним относятся:**

* [**Сетевой экран**](https://www.kaspersky.ru/resource-center/definitions/firewall)**, предотвращающий несанкционированный доступ пользователей к вашим веб-сайтам, почтовым серверам и другим источникам информации, к которым можно получить доступ из интернета.**
* **Программное обеспечение для удаления данных. Каждый раз при использовании нового программного обеспечения, добавлении оборудования или изменении системных файлов, существует риск потери личных данных. Использование программного обеспечения для удаления данных позволяет удалить ненужные данные и полностью стереть их с жесткого диска.**
* [**Менеджер паролей**](https://www.kaspersky.ru/resource-center/preemptive-safety/power-of-a-password-manager)**. Использование надежных сложных паролей, которые необходимо регулярно менять – это важный аспект безопасности в интернете. Менеджер паролей помогает контролировать и работать с несколькими паролями.**
* **Высококачественное антивирусное программное обеспечение, выполняющее регулярную автоматическую проверку устройства по расписанию, обнаруживающее и удаляющее вредоносные программы, а также защищающее от сетевых угроз и нарушений безопасности.**

**Соблюдение кибергигиены помогает поддерживать цифровую среду в рабочем состоянии, не в последнюю очередь благодаря обновлению программ. Устаревшие программы могут иметь уязвимости, используемые злоумышленниками, поэтому, чтобы избежать проблем с безопасностью, необходимо регулярно обновлять веб-приложения, мобильные приложения и операционные системы. В результате регулярных обновлений устанавливаются новые патчи для программ, устраняющие их уязвимости. Обновления оборудования могут предотвратить проблемы с производительностью.**

**Выполнение регулярной антивирусной проверки позволяет избежать проблем, не допуская их возникновения. При надлежащем обслуживании цифровые устройства будут защищены от постоянно возникающих онлайн-угроз, а файлы – от разбиения на фрагменты, влекущего потерю данных.**

**Иногда возникает вопрос, как безопасно утилизировать старые компьютеры. При продаже или утилизации компьютера, ноутбука, планшета или смартфона, важно, чтобы на нем не остались личные и конфиденциальные данные. Недостаточно просто удалить личные файлы и данные. Необходимо отформатировать, а затем очистить жесткий диск. Чистый жесткий диск гарантирует, что передачи личных данных не произойдет.**

**Помните, что, как и с личной гигиеной, для достижения эффекта требуется регулярное соблюдение кибергигиены.**