

# ОСНОВЫ

# кибергигиены

tet



# Сеть

## Конфигурация сети Wi-Fi и настройки безопасности

В настоящее время почти у каждого человека есть хотя бы одно устройство, подключенное к интернету, обычно к сети Wi-Fi. С увеличением количества этих устройств возрастает необходимость обеспечения хотя бы минимальной безопасности и правильной конфигурации домашней и рабочей сетей Wi-Fi. Приняв необходимые меры, можно повысить общую безопасность беспроводной сети и снизить риски взлома.

## Рекомендации

- Измени на Wi-Fi-роутере пароли, установленные по умолчанию.
- Создай для Wi-Fi длинный пароль из различных символов.
- Ограничь количество устройств, которые могут подключаться к Wi-Fi-сети, – включи фильтрацию по MAC.
- Шифруй трафик данных в Wi-Fi (WPA2, WPA3).
- Выбери уникальное имя Wi-Fi-сети.
- Включи функцию брандмауэра.
- Регулярно обновляй операционную систему Wi-Fi-роутера.

## Риски при использовании публичных сетей

Почти четверть публичных сетей Wi-Fi в мире не используют никакой вид шифрования, что делает их пользователей легкой добычей для хакеров. Наибольшую угрозу для безопасности публичных и бесплатных сетей Wi-Fi создает возможность хакера находиться между твоим устройством и точкой доступа Wi-Fi. В результате вместо того, чтобы поддерживать прямую связь с публичной сетью Wi-Fi, ты отправляешь свою информацию хакеру, который сохраняет ее и использует во вред тебе.

## Рекомендации

- Открытые (публичные) сети Wi-Fi используй только в развлекательных целях, но не для финансовых операций.
- Если возможно, используй VPN-соединение для защиты от перехвата данных/вмешательства в трафик.
- Проверь, работает ли HTTPS, и все ли символы и буквы в www-адресе правильные.

# Удаленная работа и доступ к сети

## Аутентификация, пароли и данные пользователя

Чтобы ослабить защиту и получить доступ к системам, хакеры используют различные методы. Один из них – взлом слабых паролей с помощью технологии Brute Force. Это означает, что пароль из восьми простых символов может быть взломан за пять часов. Кроме того, хакеры также используют стандартные пароли (установленные по умолчанию), которые пользователи не меняют на своих устройствах.

## Рекомендации

- Регулярно меняй пароли для доступа как к рабочей среде, так и к личным аккаунтам.
- Создай для Wi-Fi достаточно длинный пароль из различных символов.
- Используй многофакторную аутентификацию – с помощью приложения, SMS или звонка.
- Используй для сохранения паролей менеджер паролей.
- Убедись, что вводишь пароль на правильном сайте и что используешь правильный www-адрес.

## Удаленные сессии (VPN, работа дома)

Если устройства, используемые для удаленной работы, подключаются к системе компании посредством публичной или незащищенной домашней сети Wi-Fi, хакеры могут проникнуть в сеть и использовать ее для незаконных действий. При каждом использовании интернета для работы или развлечений твой поставщик услуг интернета присваивает твоему устройству IP-адрес. Этот адрес – все, что необходимо злоумышленникам для проведения атак и других незаконных действий на удаленных ресурсах. VPN-туннель создает безопасное соединение с другой сетью, поэтому, подключая из дома компьютер к системе компании, ты защищаешь свои действия и информацию.

## Рекомендации

- Для удаленных сеансов связи с ИТ-инфраструктурой работодателя используй VPN.
- Для установления удаленной связи используй многофакторную аутентификацию.
- Не используй для удаленного подключения Remote Desktop Protocol, TeamViewer и подобные инструменты без дополнительной защиты, например, без ограничения доступа по IP-адресам.

# Электронная почта и коммуникация

## Безопасность

### электронной почты

Электронная почта, созданная 30 лет назад, по своей сути небезопасна, что позволяет злоумышленникам использовать ее в целях наживы (для подмены счетов, распространения вирусов-шифровальщиков, вирусов-вымогателей и т. д.).

## Рекомендации

- Не открывай подозрительные письма и файлы. Внимательно читай содержимое электронных писем.
- Помни, что вирусы также могут распространяться посредством электронных документов .edoc и .asice. Не открывай письмо, поступившее от неизвестного отправителя.
- Не нажимай на ссылки в эл. письме, если не знаешь, куда они ведут.
- Если письмо получено от известного отправителя, но у тебя возникли сомнения в безопасности письма, свяжись с отправителем по другому каналу.
- Используй антивирусную программу, которая проверяет эл. почту на наличие вирусов.

## Фишинг

Фишинг — это вид мошенничества с использованием электронной почты, который позволяет получить доступ к персональной информации. Киберпреступники используют фишинг для получения конфиденциальных сведений (данных платежных карт, паролей, информации о заказах, имен пользователей и т. д.), выдавая себя за представителей авторитетных организаций или частных лиц.

## Рекомендации

- Убедись, что веб-сайт и электронное письмо, где требуется ввести данные (особенно это касается конфиденциальных данных), является подлинным.
- Удаляй ненужные расширения браузера не используй права администратора при выполнении повседневных задач или обычном поиске в интернете.

# Оборудование для работы и личного использования

## Конфигурация и безопасность оборудования

Устройство, настроенное производителем (по умолчанию), конфигурировано так, чтобы можно было быстро и просто приступить к его использованию. Но такое устройство позволяет киберпреступникам быстро и относительно легко взломать его.

## Рекомендации

- Позаботься о том, чтобы ПО твоего личного и рабочего компьютера регулярно обновлялось.
- Если ты, работая удаленно, не можешь установить обновления на своем рабочем компьютере, посети офис.
- Регулярно обновляй свой браузер, даже если включено автоматическое обновление. Делай рестарты программ, чтобы обновления начали действовать.
- Для комплексной защиты используй платные антивирусные программы.
- Не устанавливай неизвестные приложения.
- Не устанавливай приложения по неизвестным ссылкам, полученным по электронной почте.
- Удаляй ненужные приложения и профили пользователей.
- Используй в повседневной работе не права администратора, а ограниченные права обычного пользователя.

## Чрезмерная эксплуатация

### (использование одного компьютера и для работы, и для личных целей)

Работа дома все больше стирает границы между рабочей и личной средой – как физически, так и технически. Устройства, которые раньше использовались только для работы, теперь могут служить для учебы, развлечений и других целей. Кроме того, рабочим компьютером часто пользуются члены семьи работника, что затрудняет контроль над тем, что устанавливается и удаляется на нем. Такая ситуация снижает безопасность данных, усиливает риск несанкционированного доступа к ним.

## Рекомендации

- Не используй рабочие устройства для личных целей, и наоборот, личные устройства – для работы.
- Соблюдай политику конфиденциальности компании, не устанавливай программное обеспечение на рабочие компьютеры без согласования с ИТ-специалистами компании.
- Не храни на рабочем компьютере личную информацию – копии документов, конфиденциальные данные (например, результаты анализов), частные фотографии и т. д.
- Не синхронизируй данные браузера между личными и рабочими устройствами.

# Мобильные и смарт-устройства

## Смарт-устройства

### и данные пользователя

В условиях удаленной работы, распространенность которой возросла в связи с пандемией COVID-19 и локдауном, расширилось использование смарт-устройств. Это также увеличивает риск безопасности данных, независимо от того, используются ли мобильные устройства для работы или в личных целях. Вирусы, подозрительные приложения, ПО без обновлений создают угрозу безопасности и делают твои данные доступными для киберпреступников.

## Рекомендации

- Просмотри разрешения, предоставленные приложениям, например, доступ к контактам, определение места нахождения, камера и т. д., а также то, как они используют интернет: сколько потребляют, нет ли подозрительных случаев использования.
- Используй антивирусные программы.
- Внимательно анализируй нетипичные запросы в социальных сетях.
- Не устанавливай приложения из неизвестных источников.
- Обновляй ПО.
- Используй надежные пароли и биометрическую защиту.

## Подключение

### смарт-устройств к интернету.

## Интернет вещей (IoT)

Около 80% IoT-устройств не защищены от всевозможных кибератак. Доступны для хакеров и подключенные детские мониторы. Известны случаи, когда родители с опозданием обнаруживали коммуникацию детей со злоумышленниками, взломавшими незащищенные или плохо защищенные IoT-устройства.

## Рекомендации

- Выбери правильное устройство – узнай о производителе и жизненном цикле устройства.
- Создавай длинные пароли, используй многофакторную аутентификацию.
- Используй IoT-устройства только в частной сети.
- Регулярно обновляй устройства.
- Разрешай только авторизованным пользователям получать доступ к домашней сети и подключай к сети только авторизованные устройства.

# Данные

## Хранение данных (где и как хранить)

Хотя облако является одним из самых эффективных и современных видов хранилищ данных, необходимо убедиться в его кибербезопасности. Несмотря на то, что большинство облачных сервисов имеют достаточный уровень безопасности, сервисы могут различаться. Кроме того, иногда конечный пользователь активирует или использует их неправильно.

## Рекомендации

- Доступ к облаку разрешай только известным пользователям и устройствам.
- Используй многофакторную аутентификацию для доступа к своим облачным ресурсам данных.
- Используй шифрование данных как для их передачи, так и для хранения.
- Не используй незащищенную публичную сеть Wi-Fi для отправки данных в облако.

## Резервное копирование данных

Неполадки в работе компьютера, вирус или другие причины могут вызвать полную потерю хранившихся в памяти старых, актуальных, личных и рабочих данных. Кража данных может привести к попыткам шантажа и вымогательства. Поэтому так важно обеспечить резервное копирование данных!

## Рекомендации

- Создавай резервные копии важной информации.
- Не храни и не обрабатывай личную информацию третьих лиц, если у тебя нет для этого юридических оснований.
- Рассмотрю возможность хранения информации в облачных сервисах от известных и надежных провайдеров, но при этом оцени безопасность облака.

# Киберзнания против кибермошенничества

## Кибермошенничество и киберзнания

### (выкуп, социальная инженерия, криптовалюта)

Активность киберпреступников ширится. Во всем мире отмечают значительное увеличение количество фишинговых эл. писем, распространение вирусов, а также атак вирусов-вымогателей на компании и частные лица. Фишинг – это самый эффективный способ получения доступа к твоим личным данным и вымогательства у тебя денег. Нынешняя ситуация, вызванная COVID-19, и удаленная работа создают благоприятную почву для всех видов кибермошенничества и атак.

## Рекомендации

- Создавай резервные копии.
- Не храни конфиденциальную информацию в электронной почте, в незащищенном облаке или на компьютере, не имеющем надлежащей киберзащиты.
- Регулярно меняй пароли, используй длинные пароли.
- Используй антивирусные программы.
- Внимательно читай электронные письма и оценивай необходимость нажимать на ссылки и открывать файлы от неизвестных отправителей.
- Внимательно анализируй нетипичные запросы в социальных сетях.
- Следи за новостями экспертов по безопасности и регулярно совершенствуй свои знания.
- Не бойся поднимать тревогу по поводу подозрительных действий (например, подозрительных звонков, электронных писем и запросов в социальных сетях).

