Кибербезопасность стоит на одном уровне с физической безопасностью. Вопросы киберугроз обсуждают передовые технологические компании, Европейская комиссия и главы стран мира. Разберемся, что включает понятие кибербезопасности и как защитить себя от угроз.

Что такое кибербезопасность

Киберугрозы постоянно присутствовали в жизни человечества все 50 лет технологических изменений. С появлением интернета и цифровой трансформации понятие кибербезопасности стало привычным в профессиональной и личной жизни. После распространения вирусов в 1990-х годах, 2000-е годы ознаменовались институционализацией киберугроз и кибербезопасности, которую сегодня изучают в школах и институтах. Сессия, организованная Уиллисом Уэром на Весенней объединенной компьютерной конференции (апрель 1967 года), и более поздняя публикация отчета Уэра стали основополагающими в истории области компьютерной безопасности. Работа Уэра пересекалась с материальными, культурными, политическими и социальными проблемами. Что такое кибербезопасность? Кибербезопасность — это практика защиты критически важных систем и конфиденциальной информации от цифровых атак. Меры кибербезопасности, известные как безопасность информационных технологий, предназначены для борьбы с угрозами в отношении сетевых систем и приложений, независимо от того, исходят ли эти угрозы из организации или извне.

В чем разница между кибербезопасностью и информационной безопасностью? В научной работе «Кибербезопасность и информационная безопасность: сходства и отличия» ученые Козлова Наталья и Довгаль Виталий пишут, что кибербезопасность отвечает за безопасность киберсферы и связанными с ней данными. Информационная безопасность ориентирована на информацию, гарантирует ее конфиденциальность, целостность и доступность. Рассмотрим другие отличия кибербезопасности и информационной безопасности: Домен. Кибербезопасность означает защиту всего и вся, что присутствует в киберсфере. Информационная безопасность касается защиты как цифровой информации, так и аналоговой. Процесс. Кибербезопасность связана с защитой киберпространства и предотвращения кибератак. Информационная защита защищает информацию от любой формы угрозы. Кибербезопасность касается киберпреступлений, кибермошенничества и правоохранительных органов.

Актуальность кибербезопасности

Зачем нужна кибербезопасность? Киберпреступники нацеливаются на личную информацию пользователей — имена, адреса, национальные идентификационные номера и информацию о кредитной карте — и затем продают эти записи на подпольных цифровых рынках. Это часто приводит к потере доверия клиентов, наложению штрафов со стороны регулирующих органов и даже к судебным искам. Кибербезопасность нацелена на то, чтобы подобные случаи предотвращать и наказывать киберпреступников. Где используется кибербезопасность? Кибербезопасность должна защищать от киберпреступлений, включая кибератаки, которые пытаются получить доступ, изменить или уничтожить данные, вымогать деньги у пользователей или организации, стремиться нарушить нормальную деловую деятельность. Контрмеры должны быть направлены на такие виды защиты:

- Безопасность критической инфраструктуры — методы защиты компьютерных систем, сетей и других активов, от которых зависит национальная безопасность, экономическое благополучие и / или общественная безопасность.
- Сетевую безопасность — меры безопасности для защиты компьютерной сети от злоумышленников, включая как проводные, так и беспроводные (Wi-Fi) соединения.
- Безопасность приложений — процессы, помогающие защитить приложения, работающие локально и в облаке.
- Облачную безопасность, в частности настоящие конфиденциальные вычисления, которые шифруют облачные данные в состоянии покоя (в хранилище), в движении (по мере их перемещения в облако, из него и внутри облака) и при использовании (во время обработки) для

обеспечения конфиденциальности клиентов, бизнес-требований и соблюдения нормативных требований.

- Информационную безопасность — меры по защите любой информации.
- Аварийное восстановление / планирование непрерывности бизнеса — инструменты и процедуры для реагирования на незапланированные события, такие как стихийные бедствия, перебои в подаче электроэнергии или инциденты кибербезопасности, с минимальным нарушением основных операций.
- Безопасность хранения — включает в себя шифрование и неизменяемые и изолированные копии данных.
- Мобильную безопасность — безопасность данных, хранящихся на мобильных устройствах.

К основным киберугрозам относят: вредоносное ПО; программы-вымогатели; фишинг; внутренние угрозы; распределенные атаки типа «отказ в обслуживании» (DDoS); расширенные постоянные угрозы (APT); атака с прослушиванием. Из этого можно сделать вывод, что кибербезопасность касается каждого человека и компании, которые используют интернет-технологии.

Как обезопасить себя в киберпространстве

Бренда Кей Видерхольд в работе «Роль психологии в повышении кибербезопасности» пишет, что человеческий фактор — самое слабое звено в безопасности в киберпространстве. Поэтому каждому человеку нужно научиться защищать себя от киберугроз.

Правила кибербезопасности

Жертвы киберпреступности страдают не только финансово, но и испытывают симптомы, сходные с симптомами посттравматического стрессового состояния. Чтобы не стать потерпевшим, придерживайтесь таких основных правил:

Обновляйте системное программное обеспечение.

Реализуйте защиту конечных точек — компьютеров и других устройств, подключенных к интернету, которые имеют доступ к Сети.

Используйте безопасные интернет-соединения.

Запаролите веб-браузеры и электронную почту.

Реализуйте сохранение данных, возможность восстановления после потери.

Шифруйте данные и устройства.

Активируйте удаленное стирание данных на других устройствах (поможет при потере ноутбука или мобильного гаджета).

Убедитесь в безопасности облачного хранилища. Контролируйте доступ к своей сети.

Создайте надежную сегментацию сети (разделите ее на сегменты, чтобы хакер при взломе не получил доступ ко всей сети сразу).

Внедрите журнал аудита — мониторинг того, что происходит и не происходит в Сети.

Создайте черный и белый список для ПО.

Обезопасьте мобильные устройства.

Обезопасьте устройства, которые сохраняют данные, например флеш-накопители.

Храните логины и пароли в надежном месте.

Европейская комиссия внедрила регламент о кибербезопасности, который создает основу контроля и управления рисками в области кибербезопасности. Это ведет к созданию нового межведомственного совета по кибербезопасности, расширяет возможности защиты от киберугроз и стимулирует регулярную оценку зрелости и улучшение кибергигиены.

Кибербезопасность детей

Чтобы обезопасить детей в интернете, открыто поделитесь с ними опасениями, расскажите о безопасном поведении, дайте советы, которые помогут избежать угроз. Вот несколько подсказок:

Научите детей не нажимать на кнопки и ссылки в электронных письмах.

Установите на все гаджеты качественные антивирусники.

Найдите и установите ПО, которое может проверять и обновлять настройки конфиденциальности в социальных сетях.

Посоветуйте детям скачивать приложения и программы только из официальных магазинов.

Настройте программный родительский контроль, которые блокирует неприемлемый контент.

Научите детей осознанно подходить к выбору контента.

Обсудите с подростками секстинг (пересылка личных фото) и его последствия. ЮНИСЕФ было установлено, что 80% детей чувствуют опасность сексуального насилия в интернете. Организацией была разработана платформа, которая оказывает помощь жертвам насилия в интернете WePROTECT.

Расскажите детям, что публичный Wi-Fi и в колледже может быть небезопасным.

Кроме этого, поговорите с детьми о троллинге, буллинге (травля), хейтинге (негативные комментарии о человеке), сталкинге (преследование) и флейминге (разжигание ненависти) в интернете. Треть детей, по утверждению ЮНИСЕФ, поддается в интернете агрессивным нападкам такого рода. Объясните, что лучше не поддаваться на провокации и отправлять агрессоров в бан. Существуют специальные средства защиты от фишинговых писем и сайтов, инструменты защиты смартфонов и планшетов от почтовых и веб-угроз, вредоносного ПО. Детям будет полезен менеджер паролей, который поможет генерировать сложные коды. Используйте все это, чтобы обезопасить себя и своих детей в киберпространстве