

Кибербезопасность

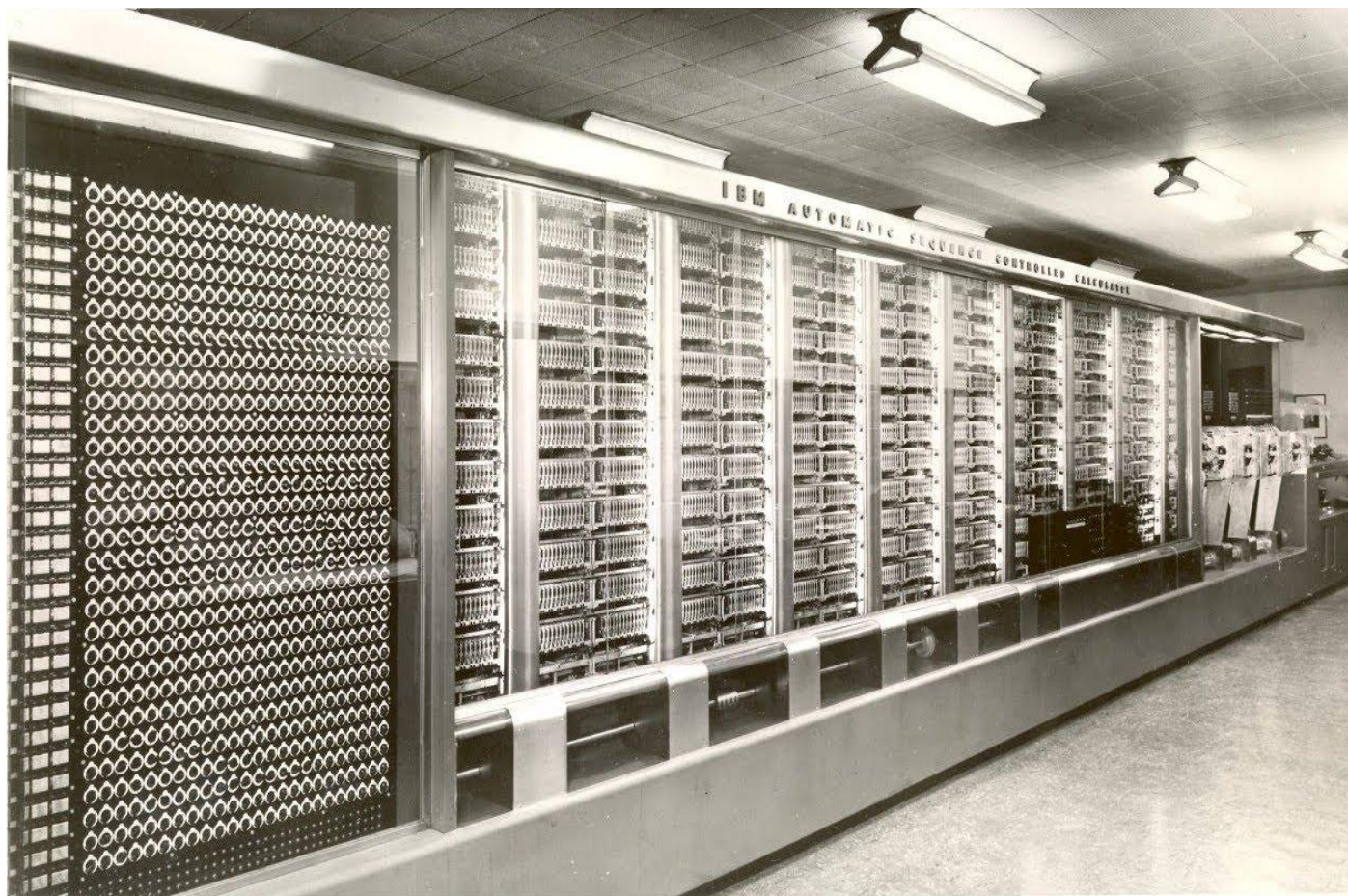


Прекрасный, опасный,
кибербезопасный мир

Немного истории

- Первый компьютер
- Первый вирус
- ARPANET
- Первая самовоспроизводящаяся программа

Первый американский программируемый компьютер



Боб Томас



I'M THE CREEPER. CATCH ME IF YOU CAN!

Я крипер. Поймай
меня если сможешь

Стив Крокер



Член
КОМАНДЫ
СОЗДАВШАЯ
ARPANET

Рэй Томлинсон



Изобретатель
электронной
почты, создатель
ARPANET,
написал
программу Reaper

Что такое кибербезопасность?

Кибербезопасность является собой набор средств, стратегий, принципов обеспечения безопасности, гарантий безопасности, подходов к управлению рисками, действий, профессиональной подготовки, страхования и технологий, которые используются для защиты киберсреды, ресурсов организаций и пользователей. Кибербезопасность подразумевает достижение и сохранение свойств безопасности у ресурсов организации или пользователей, направленных против соответствующих киберугроз.

Основными задачами обеспечения безопасности считаются: доступность, целостность, включающая аутентичность, а также конфиденциальность. Кибербезопасность является необходимым условием развития информационного общества.



Меры обеспечения кибербезопасности

Конкретные меры обеспечения кибербезопасности могут быть определены по результатам оценки рисков и в рамках планирования действий по повышению безопасности активов. Стандарт представляет ряд базовых мер, направленных на решение задач:

- Обеспечения безопасности приложений;
- Обеспечения безопасности серверов;
- Обеспечения безопасности конечных пользователей;
- Защиты от атак методами социальной инженерии;
- Повышения готовности

Опасность устройств

Несмотря на популярность и удобство «умных» устройств и облачных технологий, не стоит забывать, что их подключение к системе безопасности может нести определенные угрозы вам и вашим близким при неправильном обращении с ними. Особенно это касается самостоятельно собранных систем, которые в сочетании со слабой защитой сети подвергают ваш дом сетевым атакам или физическим нападениям.

Киберугроза



Компьютерные вирусы

Вирус

DDoS

Фишинг

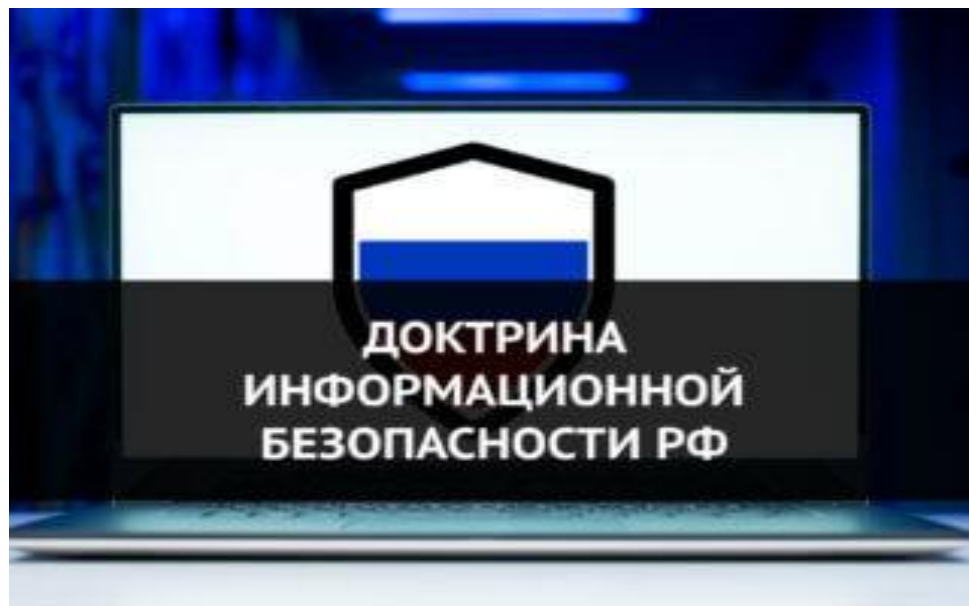




Основой кибератак являются зараженные компьютеры пользователей либо зараженные серверы. В дальнейшем объединяются в сеть под управлением какого-то злоумышленника, и впоследствии они используют компьютеры жертв, чтобы рассылать спам, осуществлять хакерские атаки.



Доктрина РФ



Доктрина информационной безопасности России – это изложение систем официальных взглядов на место РФ в современном мире информационных технологий, на угрозы суверенитету страны, а также средств, которые используются для выстраивания взаимодействия между государствами в цифровом обществе.

Документ выступает основой для формирования госполитики в области обеспечения информационной безопасности (ИБ), разработки целевых программ обеспечения ИБ.

Влияние на всемирную ИБ

Создание защиты от вероятных посягательств на систему организационных структур

Функционирование каждого объекта информационной инфраструктуры

Развитие производственной отрасли ПО

Проблема кибербезопасности в нашей стране стоит особенно остро во многом из-за слабой нормативно-правовой базы. Фактически, сформулированный и закрепленный целостный подход к национальной проблематике кибербезопасности на сегодняшний день отсутствует.



В каждой стране определение кибербезопасности и других ключевых терминов может значительно различаться.



Спасибо за внимание!