Міністерство освіти та науки України
КНУБА

Тема: кібербезпека “простими” словами

Виконав студент
Групи БІКС-11
Ревунов Нікіта

Київ 2016

Вступ

- Мы живем в век развития киберпространства, и ежедневно каждый из нас сталкивается с необходимостью использования информационных технологий. От социальных сетей, размещения информации о своих персональных данных в интернете в пользование банкоматами, банковскими счетами и т. П. В связи с этим возникает необходимость защиты всего этого. Этим и занимаются специалисты по кибербезопасности.
- **Кибербезопасность** - это безопасность информации и инфраструктуры в цифровой среде. Кибербезопасность предполагает достижение и сохранение свойств безопасности в ресурсах организации или пользователей, которые направлены на предотвращение соответствующим киберугрозами.
- Специалист по кибербезопасности занимается разработкой охранных систем для различных коммуникационных сетей и электронных баз данных, тестирует и совершенствует собственные и сторонние разработки для избежания рисков утечки сведений, составляющих государственную или коммерческую тайну, конфиденциальную информацию. Такая профессия является сравнительно молодой и получила широкое распространение в связи с внедрением компьютерных и сетевых технологий практически во всех организациях - от небольших коммерческих фирм в органы госбезопасности.

Отношения между Кибербезопасностью и другими доменами безопасности

- Возвращаясь к теме стратегии кибербезопасности, хочу обратиться к очень интересному стандарту, который описывает это понятие и его связь с другими, более привычному российскому уху терминами их области информационной безопасности. Речь идет о стандарте ISO/IEC 27032:2012 Information technology -- Security techniques -- Guidelines for cybersecurity, который был принят в июле прошлого года.
  Он дает четкое понимание связи термина cybersecurity (кибербезопасность) с сетевой безопасностью, прикладной безопасностью, Интернет-безопасностью и безопасностью критичных информационных инфраструктур с точки зрения западных специалистов. В стандарте приводится вот такая картинка, которая визуализирует связь различных терминов.

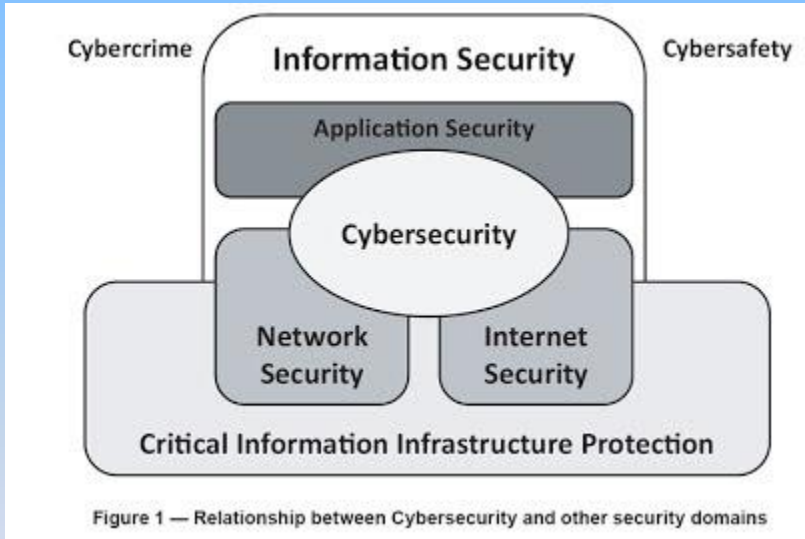
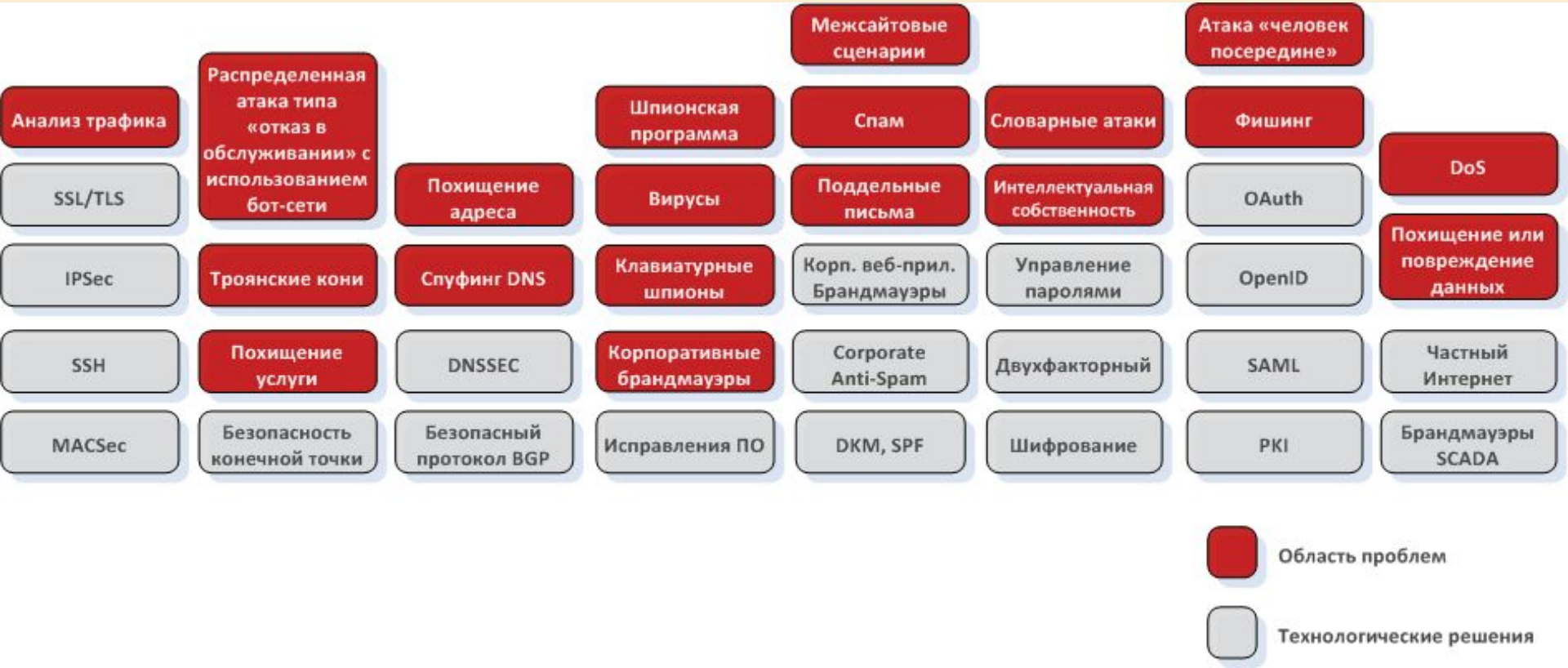


Figure 1 — Relationship between Cybersecurity and other security domains

Программно-технические способы и средства обеспечения информационнойбезопасности

- Средства защиты от несанкционированного доступа (НСД):
- Средства авторизации;
- Мандатное управление доступом;
- Избирательное управление доступом;
- Управление доступом на основе ролей;
- Журналирование (так же называется Аудит).
- Системы анализа и моделирования информационных потоков (CASE-системы).
- Системы мониторинга сетей:
- Системы обнаружения и предотвращения вторжений (IDS/IPS).
- Анализаторы протоколов.
- Антивирусные средства.
- Межсетевые экраны.
- Криптографические средства:
- Шифрование;
- Цифровая подпись.
- Системы резервного копирования.
- Системы бесперебойного питания:
- Источники бесперебойного питания;
- Резервирование нагрузки;
- Генераторы напряжения.
- Системы аутентификации:
- Пароль;
- Сертификат;
- Биометрия.
- Средства предотвращения взлома корпусов и краж оборудования.
- Средства контроля доступа в помещения.
- Инструментальные средства анализа систем защиты:
- Мониторинговый программный продукт.

Области проблем кибербезопасности и их решения



Исторические аспекты возникновения и развития информационной безопасности

- Объективно категория «информационная безопасность» возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человеком наличия у людей и их сообществ интересов, которым может быть нанесен ущерб путем воздействия на средства информационных коммуникаций, наличие и развитие которых обеспечивает информационный обмен между всеми элементами социума. Учитывая влияние на трансформацию идей информационной безопасности, в развитии средств информационных коммуникаций можно выделить несколько этапов[4]:

- I этап — до 1816 года — характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.
- II этап — начиная с 1816 года — связан с началом использования искуственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).
- III этап — начиная с 1935 года — связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.
- IV этап — начиная с 1946 года — связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.
- V этап — начиная с 1965 года — обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединенных в локальную сеть путем администрирования и управления доступом к сетевым ресурсам.
- VI этап — начиная с 1973 года — связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее. Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.
- VII этап — начиная с 1985 года — связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, очевидно, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

•Кінець

- Дякую за увагу