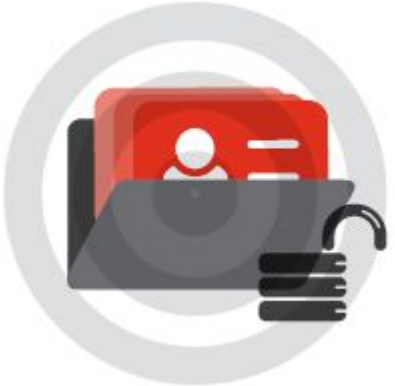
Становление специалиста по информационной безопасности



План повествования

1. Основные направления безопасности информации.
2. Основные навыки необходимые специалисту по информационной безопасности.
3. Рассмотрение основных задач безопасника.
4. Немного о провалах.
5. Есть ли смысл заниматься информационной безопасностью?

Немного терминологии

- ИБ – информационная безопасность.
- СЗИ – средства защиты информации.
- СКЗИ – средства криптографической защиты информации.
- СОИБ (ПОИБ) – система (подсистема) обеспечения информационной безопасности.
- ЭП – электронная подпись.
- PKI – public key infrastructure.

Основные направления

- Аудит
- Проектирование
- Аналитика
- Юридические аспекты
- Разработка СЗИ
- Разработка СКЗИ (PKI/ЭП/УЦ/защита каналов)

Основные направления

- Интеграция и эксплуатация СЗИ
- Интеграция и эксплуатация СКЗИ
- Анализ вредоносного ПО
- Испытание на проникновение (пентест)
- Организация защиты физических каналов
- Администрирование СОИБ

Основные направления

- Рентгенография
- Защита государственной тайны
- Нейронные сети в ИБ
- Антифрод (противодействие мошенничеству)

Минута размышлений

Какие ещё можно выделить направления?

Основные навыки

- Сбор информации
- Поверхностные знания о всех способах/методах обеспечения защищенности информации (лучшие практики)
- Проектирование СОИБ (ПОИБ)
- Анализ угроз и рисков

Основные навыки

- Знание нормативной базы (зарубежной тоже)
- Написание скриптов / кода
- Умение читать чужой код
- Знание основ криптографии
- Знание способов применения криптографии

Основные навыки

- Знание основных продуктов ИБ, их установки и настройки
- Чтение эксплуатационной документации
- Знание возможностей вредоносного ПО
- Знание основных инструментов анализа защищенности

Основные навыки

- Знание возможностей утечки информации по техническим каналам
- Знание основных моментов эксплуатации СОИБ (ПОИБ)
- Умение оценить тенденции развития отрасли

Минута размышлений

Возможно я что-то забыл?

Я перечислил более 15 навыков (их было 16), сколькими нужно точно обладать?

Основные задачи

Основной задачей всегда является сохранение состояния **защищенности**!

Все вышеперечисленные направления нацелены на достижение состояния защищенности.

Подход с рациональным сочетанием различных методов обеспечения безопасности называется **комплексным**.

Минута размышлений

Как считаете всегда ли нужно проводить полный комплекс мероприятий для защиты?

Как вы думаете почему банк тратит миллионы на поддержание состояния защищенности, а МТКП МГТУ им. Н.Э. Баумана нет?

Почему только комплексный подход дает бОльшую вероятность остановить злоумышленника?

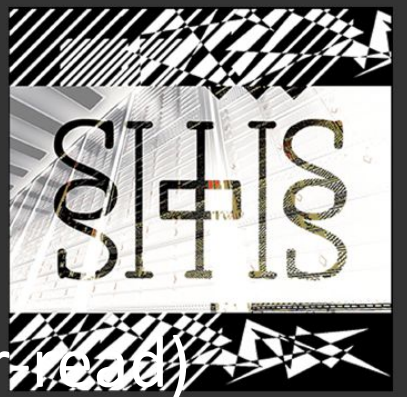
Провал на миллиард $

Вирус Carbanak затронул около 100 финансовых организаций по всему миру. Первой жертвой стал украинский банк, потом — российский, позже хакеры добрались до банков США, Европы, Китая и Юго-Восточной Азии, Ближнего Востока, Африки... Как минимум в половине случаев хакерам удавалось вывести деньги: от 2,5 млн до 10 млн долларов из одного банка. Вирус прятался во вложенном файле в электронных письмах. От момента заражения первого компьютера в корпоративной сети до кражи денег проходило 2—4 месяца. Впрочем, говорить об этих событиях в прошедшем времени не совсем верно: группировка хакеров работает до сих пор. Приведенные выше цифры — это то, что удалось выяснить «Лаборатории Касперского». Первые случаи заражения относятся к декабрю 2013 года, но пик активности вируса пришелся на июнь 2014 года.

Провал

Биткоин-биржа Mt.Gox была основана в Токио в 2010 году, к 2013 году стала крупнейшей в мире — через нее проходило 70% всех операций по купле-продаже биткоинов, а в феврале 2014 года объявила о банкротстве. Причиной печального конца стало исчезновение 850 тыс. биткоинов — это 7% всех биткоинов, которые были на тот момент в обороте. В переводе на доллары — около 480 млн.

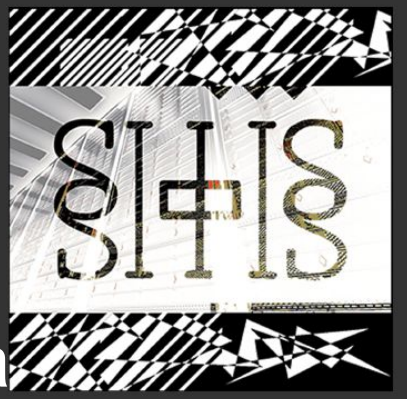
Провал



Heartbleed (CVE-2014-0160) — ошибка (англ. buffer overread) в криптографическом программном обеспечении OpenSSL, позволяющая несанкционированно читать память на сервере или на клиенте, в том числе для извлечения закрытого ключа сервера. Информация об уязвимости была опубликована в апреле 2014 года, ошибка существовала с конца 2011 года.

На момент объявления об ошибке количество уязвимых веб-сайтов оценивалось в 0.5 миллиона, это составляло около 17% защищённых веб-сайтов Интернета.

Провал



28 сентября основатель Facebook Марк Цукерберг за день лишился $2 млрд после того, как соцсеть призналась в обнаружении проблемы с безопасностью. В компании не уточнили, произошла утечка личных данных пользователей или нет (50 миллионов учетных записей).

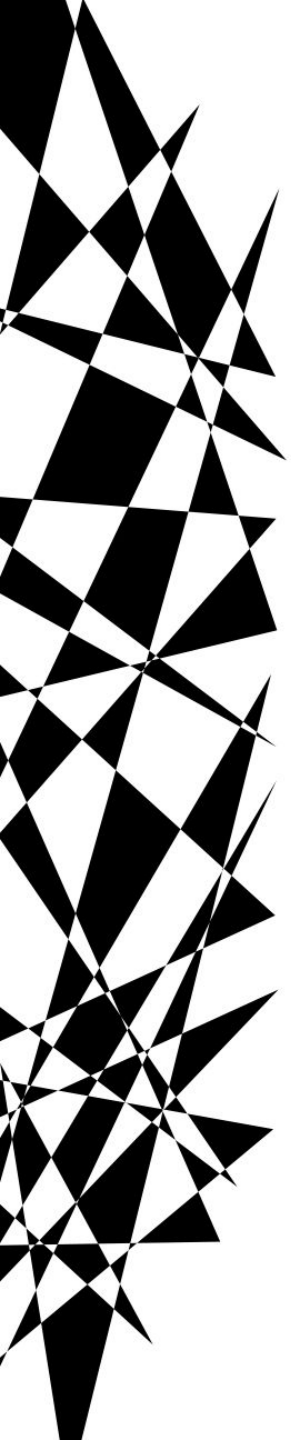
Минута размышлений

Стоит ли вообще защищать информацию, раз даже такие крупные компании не могут с этим справиться?

Зачем люди учатся на безопасников?

Много ли получают безопасники?

Исчезнет ли данная специальность в будущем?



Вопросы?

Султанов Денис Радикович