infotecs®

PKI-FORUM
РОССИЯ

Практика безопасной разработки средств PKI

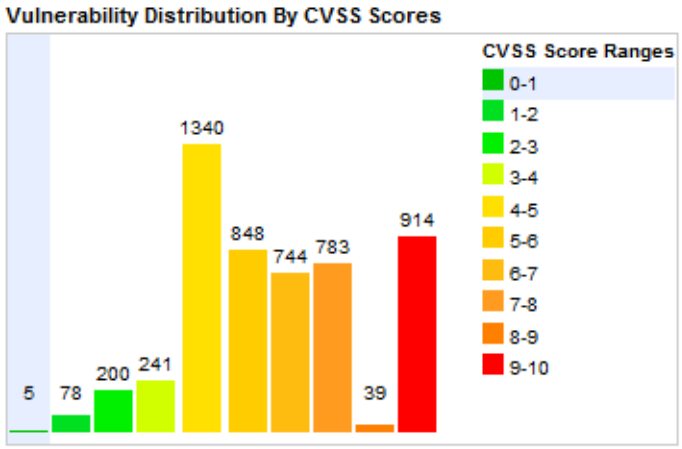
Дмитрий Гусев
Зам. генерального директора ОАО «ИнфоТеКС»
gusev@infotecs.ru

Немного общих соображений

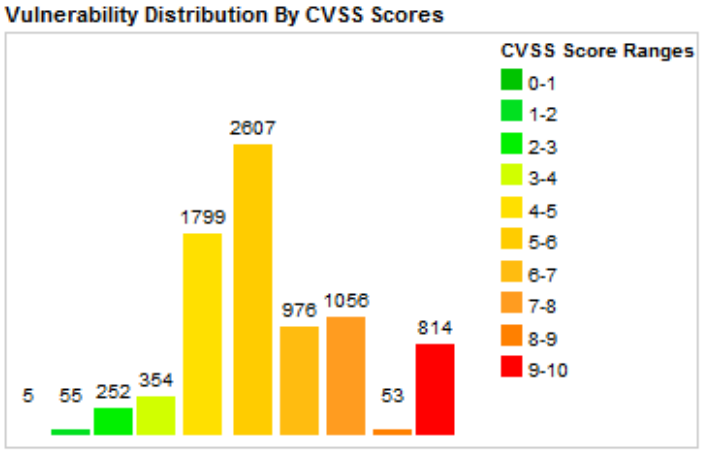
- Причиной всех достоинств и недостатков современных информационных технологий является кардинальное снижение стоимости копирования информации
- Любой бизнес развивается тогда и только тогда, когда имеются разумные механизмы и средства страхования рисков
- Любая PKI является еще одним типом информационной системы и к ней должны применяться общие подходы по реализации мер информационной безопасности

"*Сосредоточение на криптографических алгоритмах, сопряжённое с игнорированием остальных аспектов безопасности, похоже на защиту дома не постройкой забора вокруг него, а установкой огромного столба в надежде, что противник налетит прямо на него. Сообразительный нападающий просто обойдёт алгоритмы.*"
(C) Security Pitfalls in Cryptography by Bruce Schneier

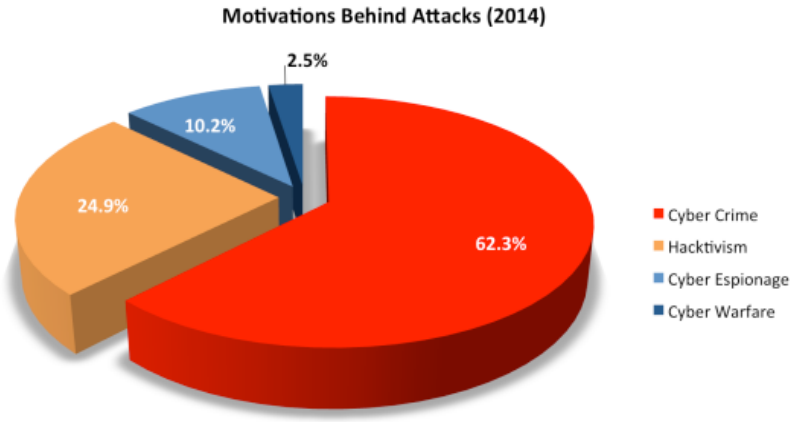
Про современные киберугрозы

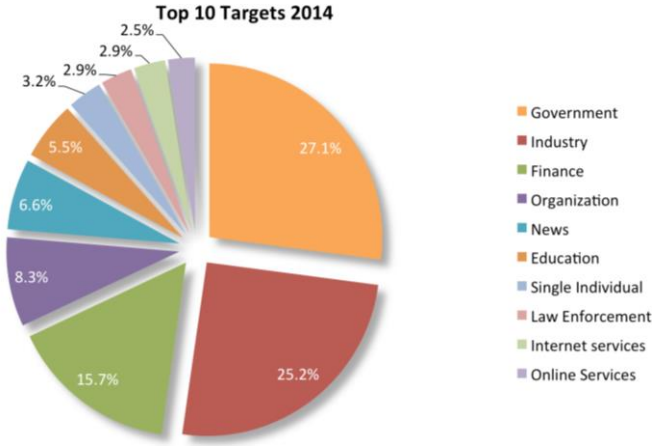


Статистика по уязвимостям, 2013
(всего - 5191)



Статистика по уязвимостям, 2014
(всего – 7946)





Про безопасность современных ИС и PKI

- Любая современная ИС не может считаться полностью надежной и безопасной (доверенной) – в любой момент может быть выявлена и проэксплуатирована новая уязвимость
- ИС постоянно развивается: на уровне сети передачи данных, вычислительных ресурсов, сервисов, задач и целей – изменяется модель нарушителя и угроз, условия функционирования
- PKI, являясь частью ИС, подвержены уязвимостям и атакам со стороны нарушителя в той же степени, что и все остальные компоненты ИС

- ИС должна находиться под постоянным мониторингом уровня защищенности
- Элементы PKI должны на всех этапах разработки и эксплуатации проверяться на наличие уязвимостей
- Разработчик элементов PKI должен иметь эффективные механизмы устранения уязвимостей в своих продуктах и доведения обновлений до потребителей

Регулирование в области безопасной разработки

- **ПРИКАЗ ФСТЭК России от 11 февраля 2013 г. N 17 "Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"**
  - П.16. - анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;
  - П.16.6. Анализ уязвимостей информационной системы проводится в целях оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации.
  - Анализ уязвимостей информационной системы включает анализ уязвимостей средств защиты информации и технических средств и программного обеспечения информационной системы.
- ГОСТ Р ИСО/МЭК 15408-2002 «Общие критерии» (понятие «Общего уровня доверия»)
- Находятся в работе:
  - Проект нового ГОСТ «Разработка защищенного программного обеспечения»
  - Проект требований и рекомендаций по обновлению сертифицированных СЗИ
- Банк данных угроз безопасности информации ФСТЭК России

Практики безопасной разработки ИТ-продуктов (Security Development Lifecycle)

Microsoft

Корпоративный центр мониторинга ГК ИнфоТеКС (ЗАО «Перспективный мониторинг»)

Действует с мая 2015 г.

Технические системы

Система защищенного взаимодействия

VPN/ViPNet

АРМ Аналитика уязвимостей

АРМ Сигнатурного Аналитика

АРМ Аналитика СОА

АРМ Аналитика Инцидентов

АС анализа вредоносного трафика, ПО и атак

АС поиска и анализа Информации по типовым форматам в публичных (анонимных) источниках Интернета

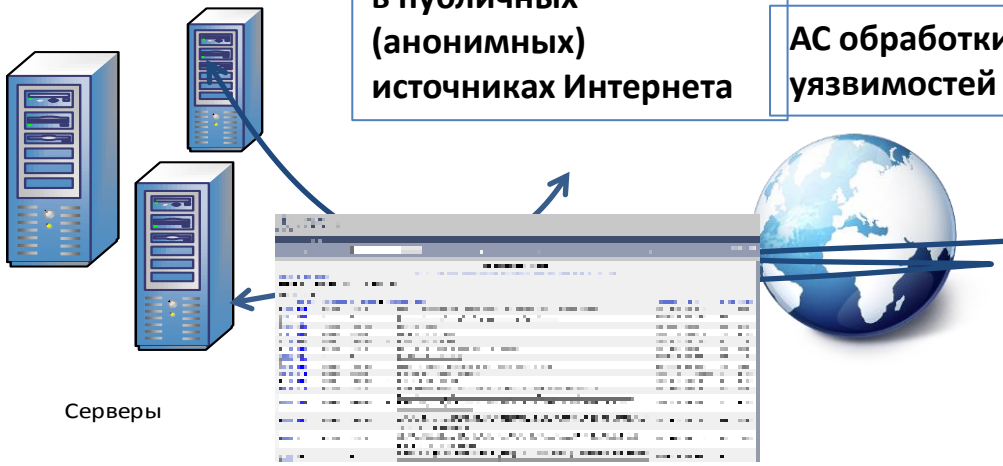
АС мониторинга Уязвимостей ПО и оборудования

АС обработки уязвимостей

АС анализа Событий ИБ от разных источников (Система обнаружения атак)

АС обработки Инцидентов

АС статического антивирусного анализа



Серверы

Серверы

Применяемые меры контроля безопасности продуктов ViPNet

1. Проведение экспертизы новых версий продуктов на наличие уязвимостей
2. Постановка продуктов на мониторинг уязвимостей
3. Извещение разработчиков о новых уязвимостях в продукте и среде его функционирования
4. Выявление компьютерных атак на продукты ViPNet в ИС заказчиков
5. Подготовка рекомендаций по устранению уязвимостей
6. Выпуск обновлений продуктов, устраняющих выявленные уязвимости

Внедряемые меры безопасной разработки продуктов ViPNet

1. Учет практик Microsoft SDL в процессах разработки и эксплуатации продуктов
2. Включение исследовательской лаборатории ИнфоТеКС (аккредитована ФСБ России) в разработку продуктов ViPNet на стадиях проектирования требований, реализации методов защиты и тестирования продуктов
3. Расширение вовлеченности Центра мониторинга и экспертов в области практической ИБ в этапы разработки продуктов
4. Расширение практик мониторинга защищенности информационных систем заказчиков, в т.ч. в рамках ГосСОПКИ
5. Расширение взаимодействия с ФСБ и ФСТЭК по выработке эффективных механизмов разработки и контроля защищенности СЗИ

Спасибо за внимание!

Дмитрий Гусев
Зам. генерального директора ОАО «ИнфоТеКС»
gusev@infotecs.ru