Эшелон
комплексная безопасность

Проблемы при подключении к сетям общего пользования

Алексей Марков, к.т.н, CISSP
Генеральный директор ЗАО «НПО «Эшелон»

План

1. Что такое ИСОП?
2. Современные угрозы
3. Нормативные требования
4. Белые и серые пятна по защите от Интернет-угроз

Эшелон
комплексная безопасность

Определения

Надо различать:

- Проблемы защиты общедоступной информации в государственных информационных системах общего пользования
- Проблемы защиты информации ограниченного доступа государственных ИС, ИТКС, СВТ при подключению к информационно-телекоммуникационные сети международного информационного обмена («сетей связи общего пользования»)

Эшелон
комплексная безопасность

Что такое ИСОП?

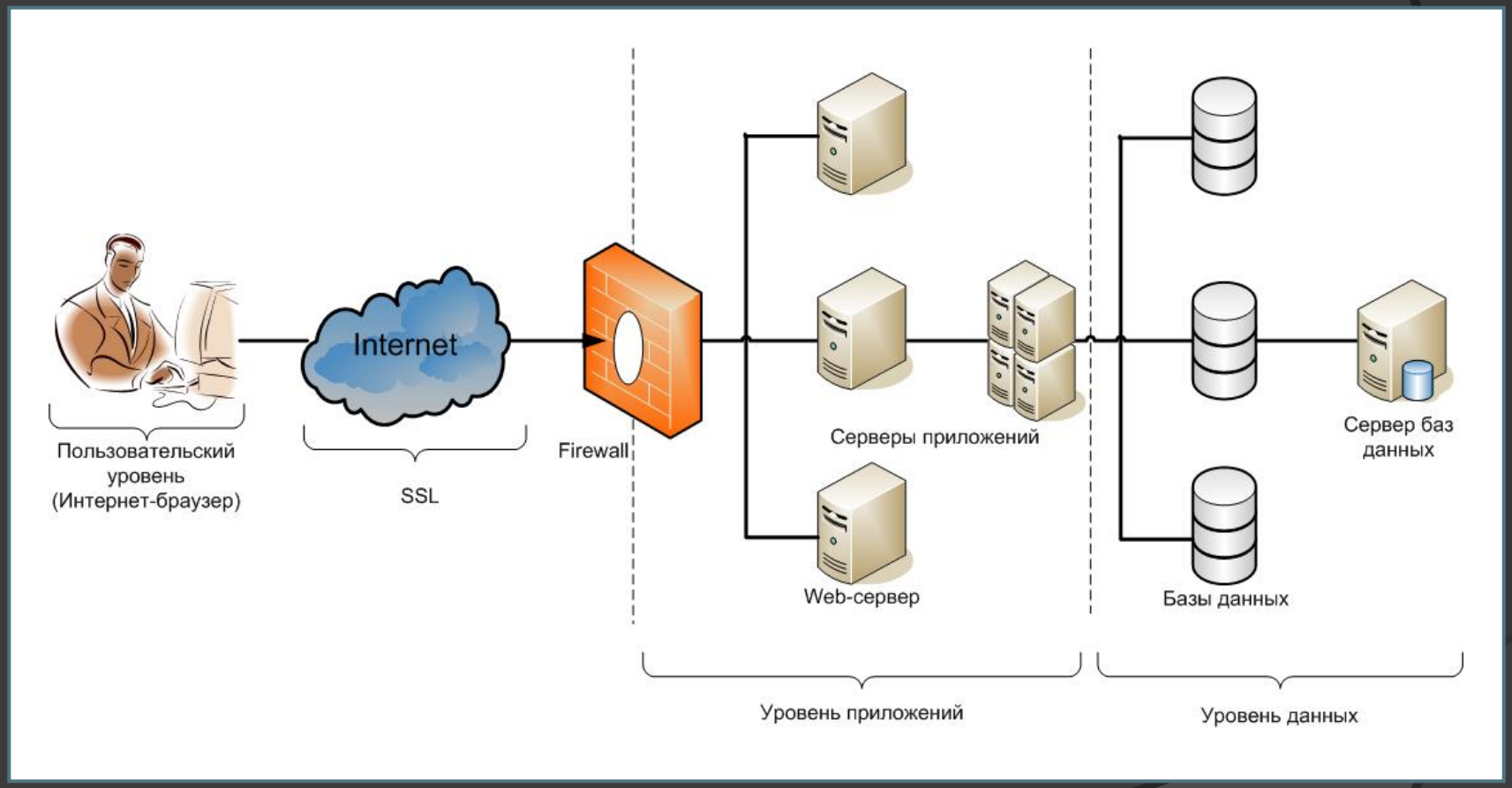
Информационная система общего пользования - государственная информационная система, которая открыта для использования всеми физическими и юридическими лицами и в услугах которой этим лицам не может быть отказано.

На Урале более 1000 ИСОП попало во внимание ФСТЭК России в 2011 г.

Классы систем: политическая и техническая классификация

- I класс: Правительства Российской Федерации, федеральных министерств, федеральных служб и федеральных агентств, руководство деятельностью которых осуществляет Президент Российской Федерации, федеральных служб и федеральных агентств, подведомственных этим федеральным министерствам.
- II класс: ВСЕ ОСТАЛЬНЫЕ информационные системы общего пользования федеральных органов исполнительной власти

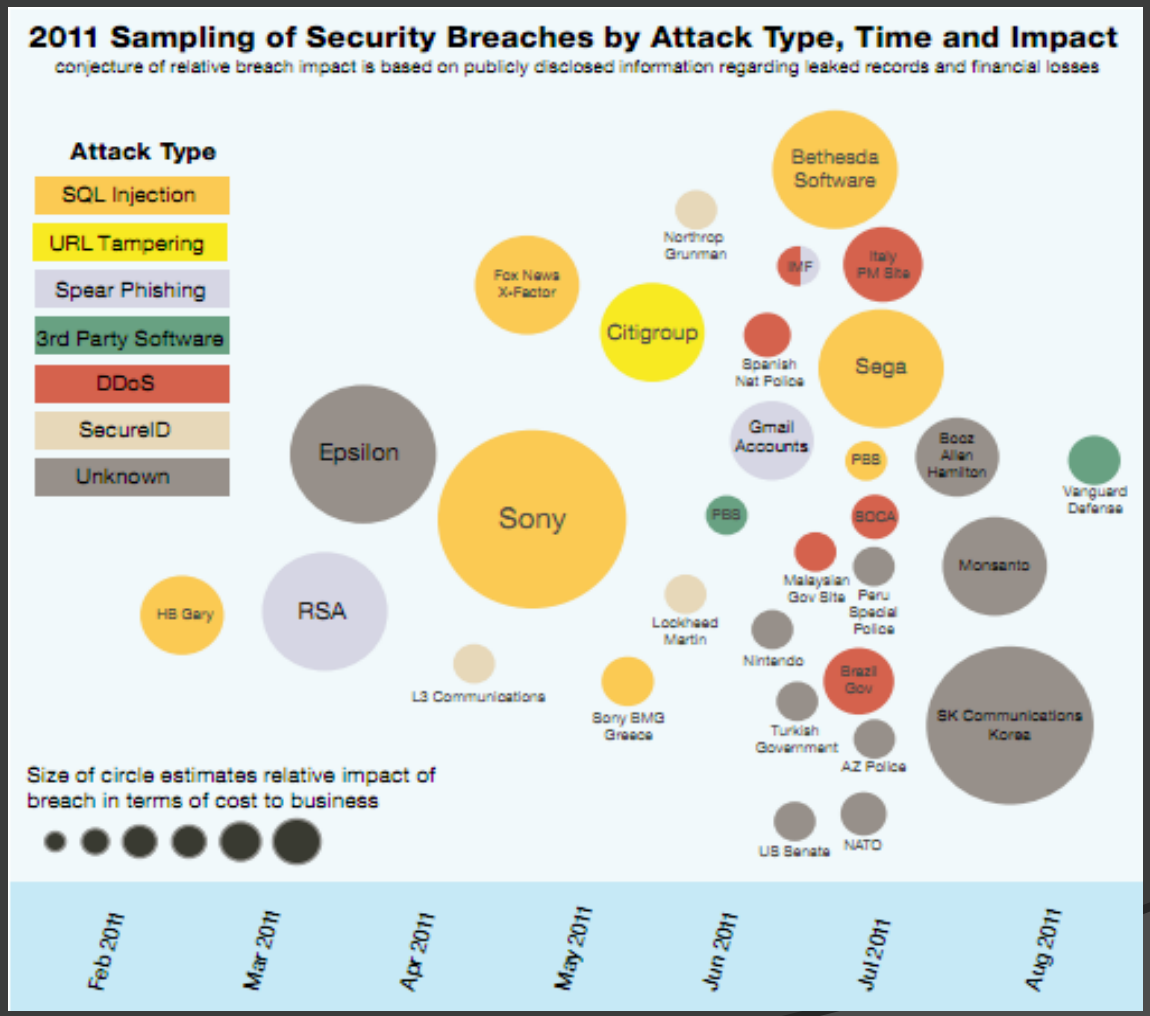
Архитектура современного интернет-портала



- Общедоступная информация и не только!
- Межсетевое и межсегментное разграничение

Эшелон
комплексная безопасность

Современные атаки

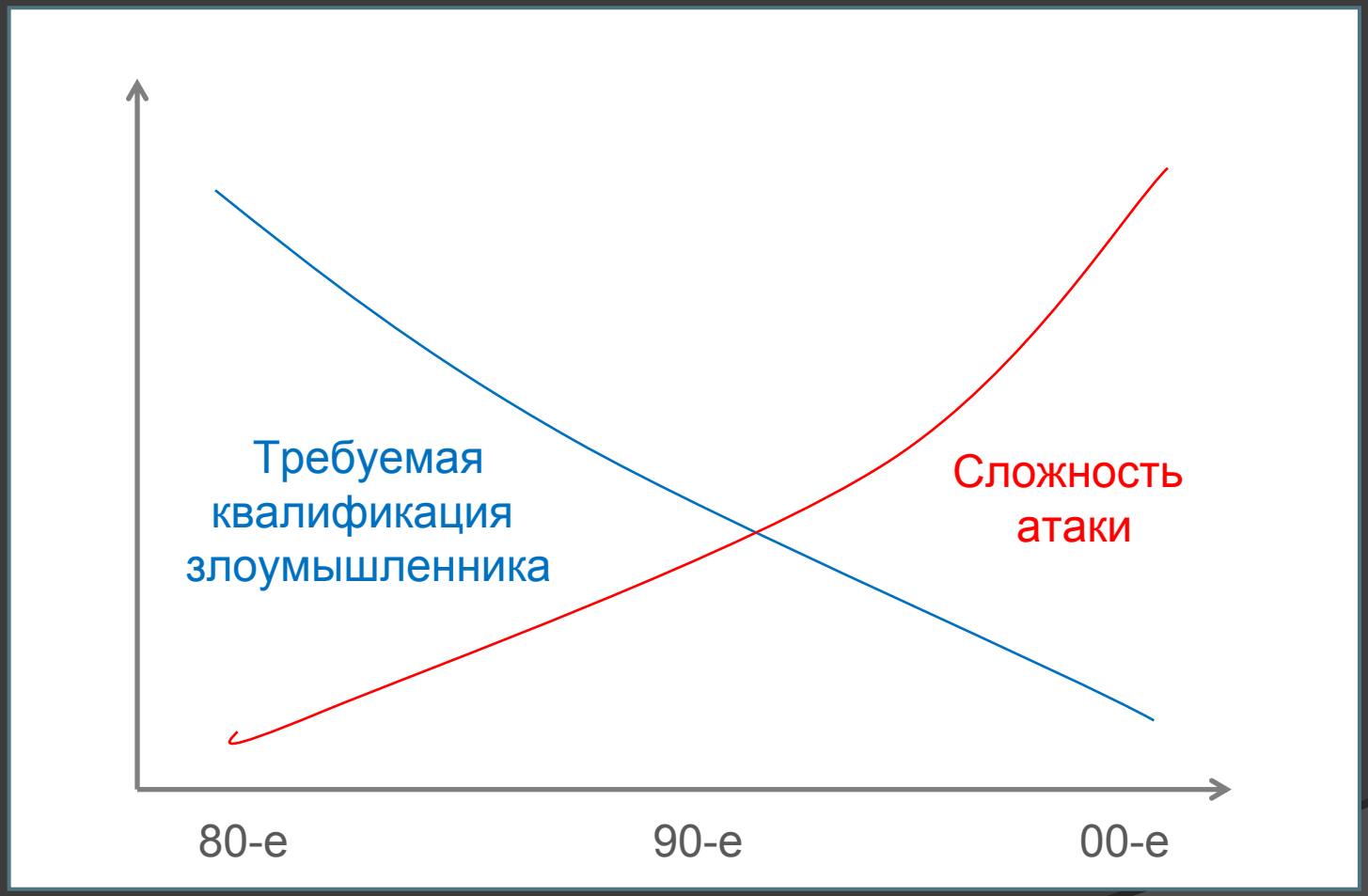


Данные из отчета IBM X-Force 2011 Mid-year Trend and Risk Report

Современные атаки -> Современные СЗИ

- DDoS
- Эксплуатация уязвимостей (SQL-инъекция, XSS)
- Атаки на администратора ресурса с использованием методов социальной инженерии
- Подбор паролей к FTP

Хакером может стать каждый!



Межсетевой экран может остановить только лобовые атаки!

Эшелон
комплексная безопасность

«Как защититься?» или прописные истины…

- Определение гибких требований к составу и классам СЗИ на основе актуальных угроз
- Внедрение корректных настронных технических решения (МЭ, IDS, Antivirus…)
- Мониторинг и регулярный контроль защищенности информационных ресурсов (сканеры)
- Обучение пользователей и администраторов

Эшелон
комплексная безопасность

Нормативные документы

- Приказ ФСБ России и ФСТЭК России 2010 г. N 416/489 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования»

Другие документы

- Приказ Минкомсвязи 2009 г. N 104 «Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования»
- Указ Президента РФ 2008 г. N351 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена»
- Приказ ФСТЭК России 2010г. N 58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных»
- Специальные нормативные документы

Как выбрать СЗИ?

- Нормативные требования, включая использование модели угроз
- Классификация информации: открытая общедоступная, ПДн, служебная (профессиональная тайна и др.)
- Технические особенности реализации

СЗИ ИСОП

Классы средств защиты информации	Сертификация	
	I класс	II класс
СКЗИ (ЭЦП)	ФСБ	ФСБ
СЗИ от неправомерных действий	ФСБ	ФСБ или ФСТЭК
Антивирусные средства	ФСБ	ФСБ или ФСТЭК
Средства контроля доступа	ФСБ	ФСБ или ФСТЭК
Системы обнаружения компьютерных атак	ФСБ	ФСБ или ФСТЭК
Межсетевые экраны	ФСБ	ФСБ или ФСТЭК

А если есть ПДн, то ситуация усложняется…

Класс ИСПДн	Соответствующий класс АС	Класс МЭ при подключении ИСПДн к сетям ОП**	Класс МЭ при разделении ИСПДн	Уровень контроля отсутствия НДВ
К1	3А 2А- 1Г-	3	5	4
К2	3Б 2Б 1Д	4	5	*
К3	3Б 2Б 1Д	5	5	*
К4	*	*	*	*

Эшелон
комплексная безопасность

А что в США?

- Защита государственных интернет-ресурсов осуществляется в рамках Federal Information Security Management Act of 2002
- Анализ рисков: NIST SP 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- Выбор контрмер: NIST SP 800-53 Recommended Security Controls for Federal Information Systems
- В 2010 г на ИБ в государственных агентствах США было потрачено 12 000 000 000 USD.

Без конкретных требований и контроля ничего не делается!

Белые и серые пятна

- Необходимость в новых гибких требованиях к новым классам СЗИ (СОВ, антивирусный контроль, экраны безопасности уровня программных приложений, DLP, средства анализа защищенности и др.)
- Безопасность мобильных устройств: смартфоны, планшеты
- Построение процессов управления информационной безопасностью (например, с применением ISO 27001).
- Контроль эффективности процессов и защищенности систем;
- Регулярное обучение пользователей.

Эшелон
комплексная безопасность

Спасибо за внимание!

Алексей Марков, к.т.н., CISSP
Генеральный директор
mail@npo-echelon.ru