Особенности контроля защищенности информационных систем, взаимодействующих с сетями связи общего пользования

Евгения Поцелуевская, CISA, CISSP
Ведущий консультант
epotseluevskaya@ptsecurity.ru

POSITIVE TECHNOLOGIES

Positive Technologies – это:

- **MaxPatrol** – уникальная система анализа защищенности и соответствия стандартам
- **XSpider** – инновационный сканер безопасности
- **Positive Research** – один из крупнейших исследовательских центров в Европе
- **Positive Hack Days** – международный форум по информационной безопасности

Мы

- Проводим более 20-ти крупномасштабных тестирований на проникновение в год
- Анализируем защищенность веб-приложений на потоке
- Участвуем в ПК 3, разработке СТО БР ИББС
- Развиваем SecurityLab.ru – самый популярный интернет-портал, посвященный информационной безопасности
- Лицензиаты ФСТЭК, ФСБ, Министерства обороны РФ

Есть много требований по защите информации

СПЕЦИАЛЬНЫЕ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

(СТР-К)

РУКОВОДЯЩИЙ ДОКУМЕНТ
АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ
ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Положение по аттестации объектов информатизации по требованиям безопасности информации

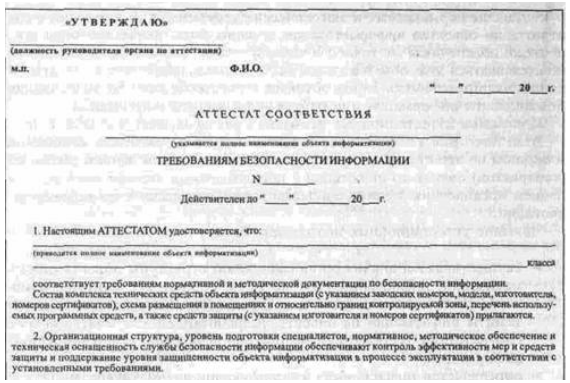
Приложение к
приказу ФСТЭК России
от 5 февраля 2010 г. № 58

Положение
о методах и способах защиты информации в информационных системах персональных данных

Однако на практике…

- **Аттестация покрывает фиксированный набор требований**

- **Аттестация прошла, а система живет своей жизнью**



«УТВЕРЖДАЮ»

(должность руководителя органа по аттестации)

м.п. Ф.И.О.

"____"_____ 20___г.

АТТЕСТАТ СООТВЕТСТВИЯ

(указывается полное наименование объекта информатизации)

ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

N_____

Действителен до "____"_____ 20___г.

1. Настоящим АТТЕСТАТОМ удостоверяется, что:

(проводится полное наименование объекта информатизации)

_____класса

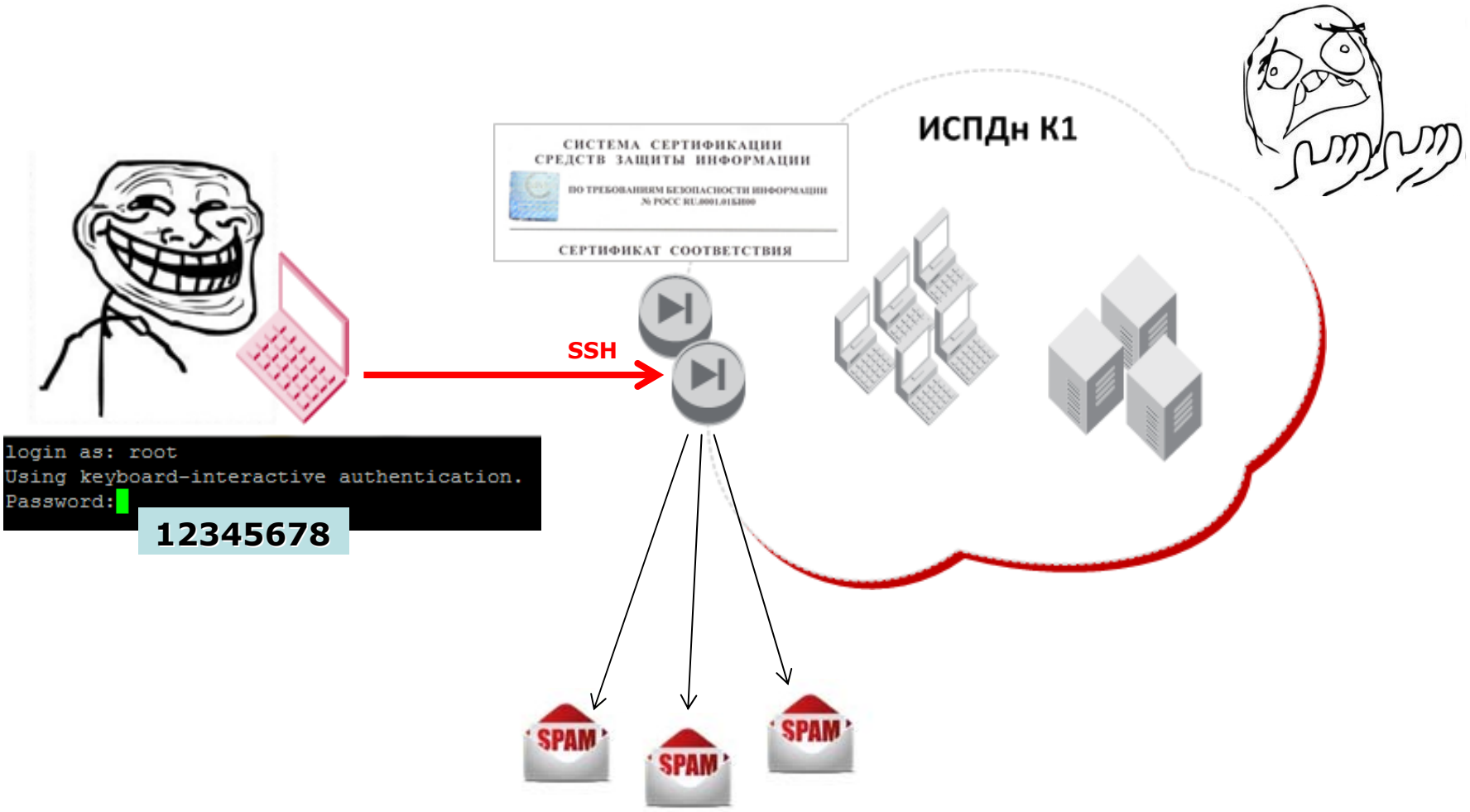
соответствует требованиям нормативной и методической документации по безопасности информации.

Состав комплекса технических средств объекта информатизации (с указанием заводских номеров, модели, изготовителя, номеров сертификатов), схема размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств, а также средств защиты (с указанием изготовителя и номеров сертификатов) прилагаются.

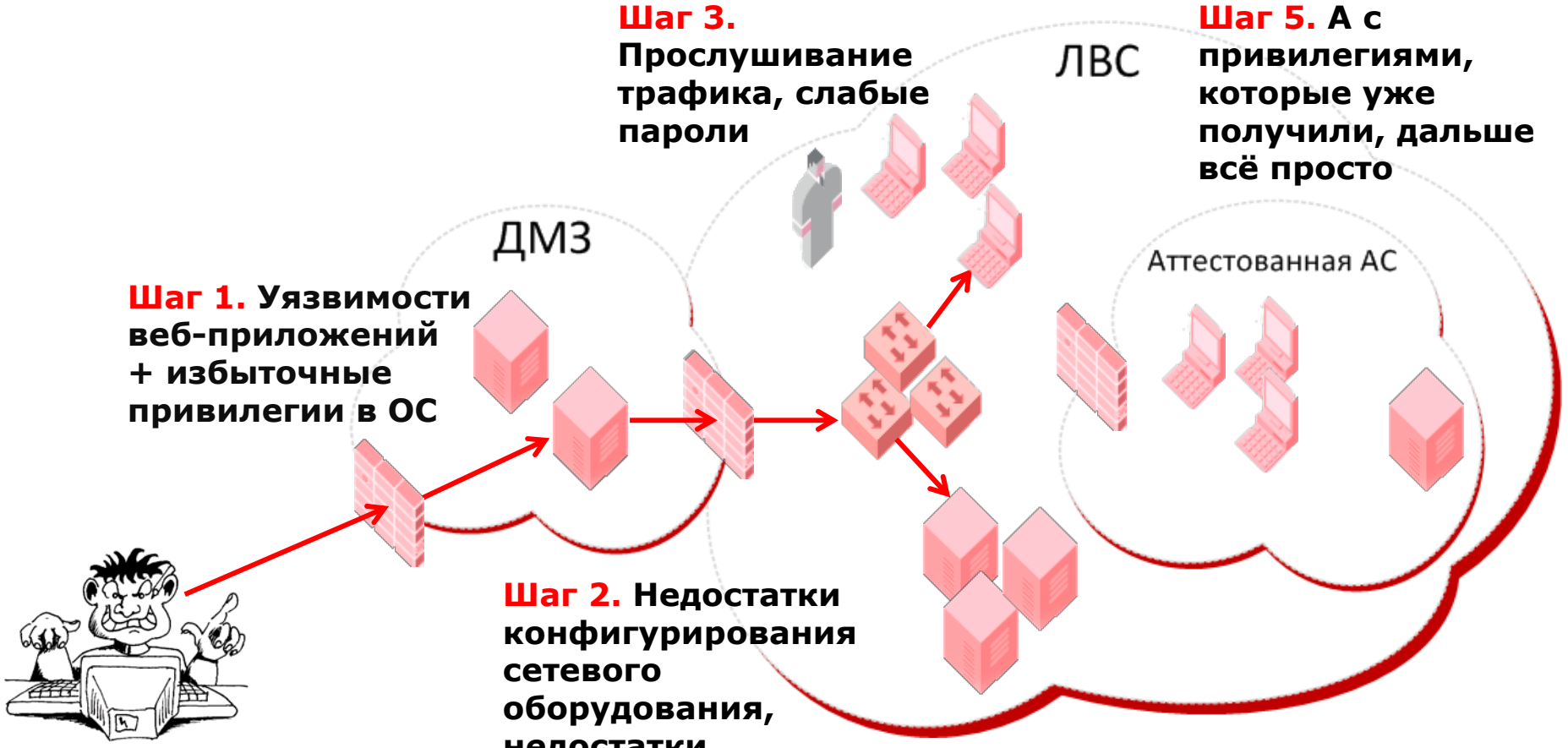
2. Организационная структура, уровень подготовки специалистов, нормативное, методическое обеспечение и техническая оснащенность службы безопасности информации обеспечивают контроль эффективности мер и средств защиты и поддержание уровня защищенности объекта информатизации в процессе эксплуатации в соответствии с установленными требованиями.

≠

Например


СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
СЕРТИФИКАТ СООТВЕТСТВИЯ
ИСПДн К1
SSH
login as: root
Using keyboard-interactive authentication.
Password:
12345678
SPAM
SPAM
SPAM

Типовой сценарий атаки



Шаг 1. Уязвимости веб-приложений + избыточные привилегии в ОС

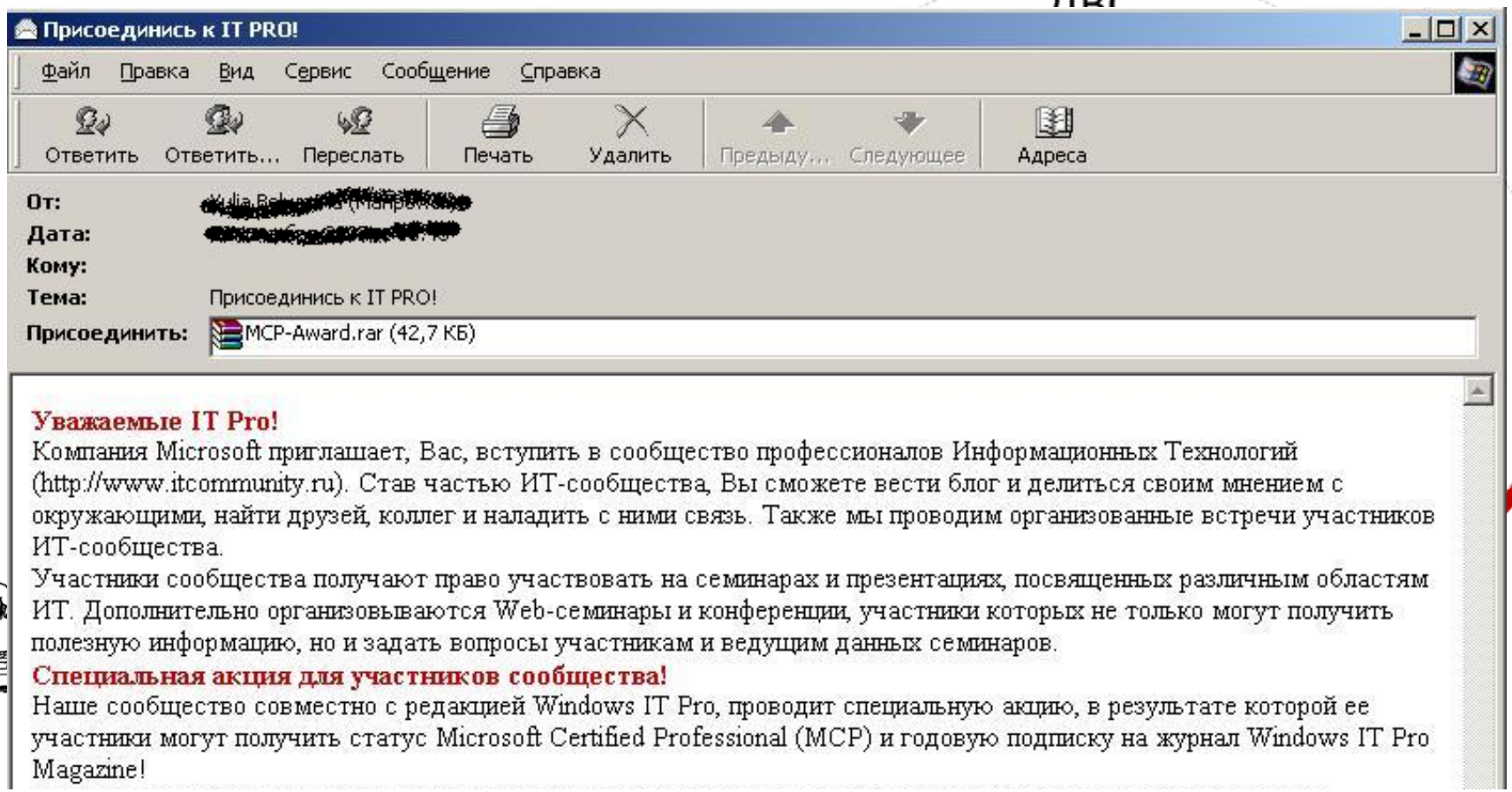
Шаг 2. Недостатки конфигурирования сетевого оборудования, недостатки сегментации

Шаг 3. Прослушивание трафика, слабые пароли

Шаг 4. Хранение критичных данных в открытом виде, недостатки антивирусной защиты, избыточные привилегии

Шаг 5. А с привилегиями, которые уже получили, дальше всё просто

Или ещё проще



Наш опыт работ показывает, что…

1-2 дня = «пройти» периметр

4 часа = максимальные привилегии доступа

10 минут = min 1 критическая уязвимость

Сколь угодно долго… можно оставаться незамеченными в системе

1 из 5 пользователей использует «слабый» пароль

Наличие 1Г, ISO…. в основном не влияет на перечисленные наблюдения выше (!)

http://devteev.blogspot.com

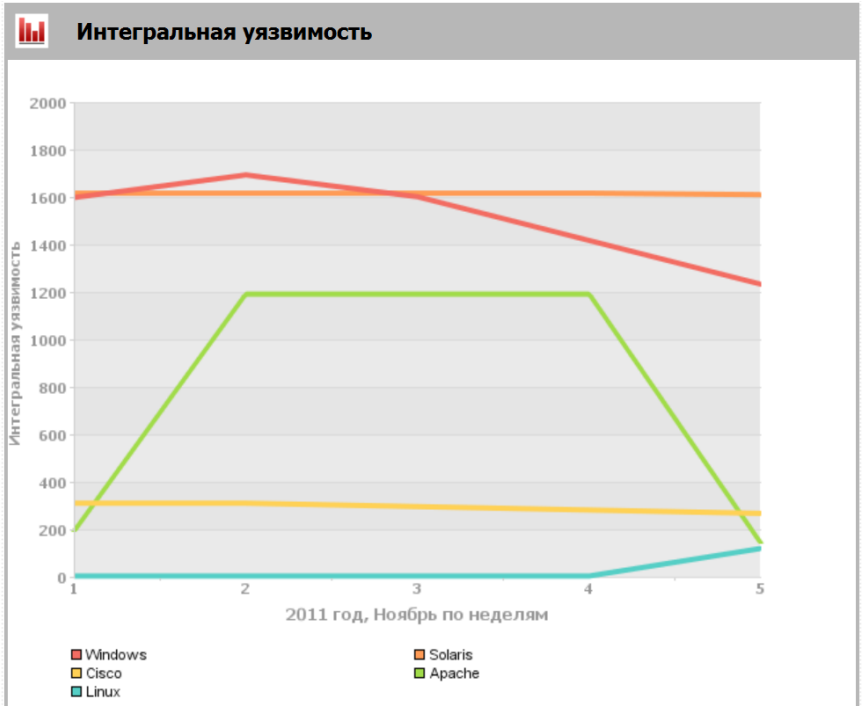
Как этого избежать

- **Реализовать процессы ИБ на практике, а не только на бумаге, в том числе:**
  - **Использовать защитные механизмы, соответствующие реальным угрозам**
  - **Регулярно проводить оценку защищенности ИС**
  - **Своевременно обновлять ПО**
  - **Обучать пользователей**
- **Обеспечить контроль реализации этих процессов:**
  - **Организационные меры**
  - **Автоматизированные средства контроля**

Например

MaxPatrol позволит обнаружить:

- **Уязвимости ПО, в том числе веб-приложений**
- **Избыточные привилегии пользователей**
- **Протоколы управления, доступные извне на сетевом оборудовании, и другие недостатки конфигурации**
- **Слабые пароли пользователей, стандартные значения SNMP community string и др.**
- **Использование незащищенных протоколов для передачи данных**
- **Отключенный или не обновленный антивирус на рабочих станциях и серверах**



Резюме

- **Как правило средства для контроля защищенности ИС у нас уже есть, нужно только правильно их использовать**

Спасибо за внимание!

Евгения Поцелуевская, CISA, CISSP
Ведущий консультант
epotseluevskaya@ptsecurity.ru