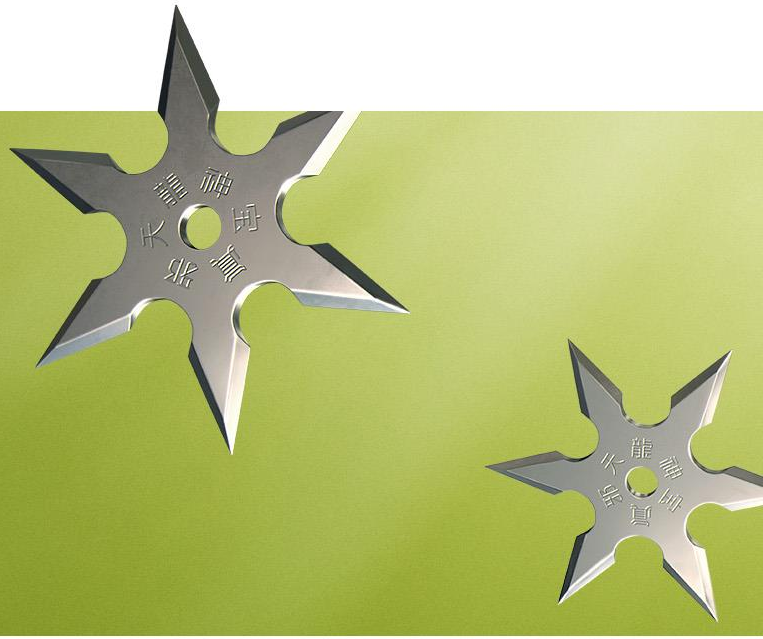
КРОК

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННЫХ МУЗЕЕВ



Евгений Дружинин
Эксперт по информационной безопасности

Москва, 14 декабря 2016

СОДЕРЖАНИЕ

- Общая проблематика музеев в области ИБ
- Особенности комплексного подхода к обеспечению ИБ в музеях
- Ключевые направления развития музеев в области ИБ

СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ИНФОРМАТИЗАЦИИ МУЗЕЕВ

КРОК

- Внедрение и развитие музейных информационных систем
- Развитие мультимедийных систем для посетителей
- Предоставление общедоступных информационных WEB-ресурсов
- Внедрение «бизнес-систем» для автоматизации финансово-экономической деятельности музеев (бухгалтерия, электронная почта и пр.)

ПРОБЛЕМЫ МУЗЕЕВ В ОБЛАСТИ ИБ

КРОК

- Угрозы информационной безопасности

  Деструктивные воздействия из сети Интернет (искажение хранимой информации, нарушение доступа, кража конфиденциальных данных, проникновение вирусов и пр.)

  Угрозы со стороны посетителей (несанкционированный доступ к внутренним информационным системам, нарушение работы wi-fi и пр.)

  Угрозы со стороны внутренних пользователей (утечка данных, посещение зараженных сайтов, активизация вредоносного ПО через сменные носители и электронную почту и пр.)

- Необходимость обеспечения соответствия государственным нормативно-правовым требованиям в области ИБ

  Необходимость соответствия ФЗ «О персональных данных»

ВОЗМОЖНЫЕ НЕГАТИВНЫЕ ПОСЛЕДСТВИЯ

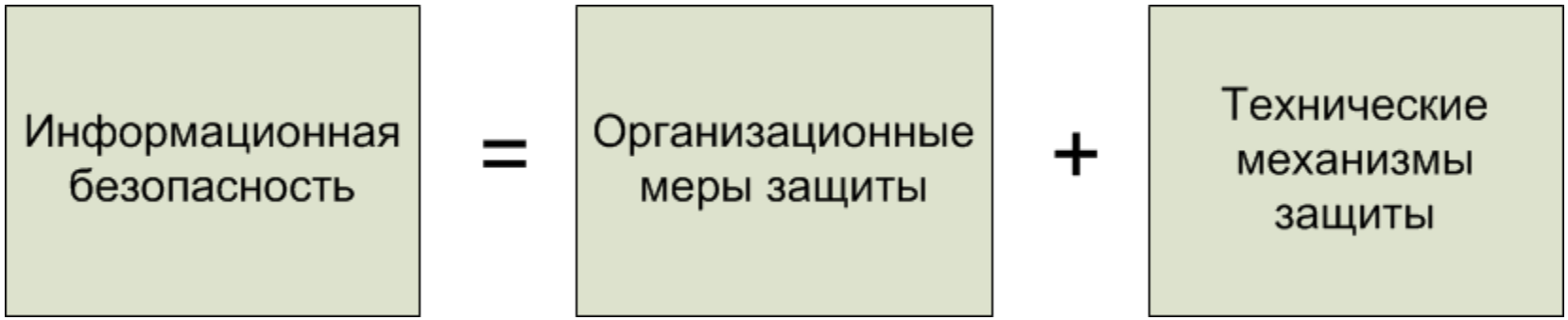
КРОК

- Технические последствия
  - Недоступность мультимедийных ресурсов для посетителей
  - Искажение или недоступность общедоступных информационных материалов , предоставляемых через сеть интернет
  - Искажение информации в музейной информационной системе
  - Нарушение работы электронной почты, бухгалтерии и пр. внутренних информационных систем музея
- Организационно-правовые последствия
  - Административная ответственность (штрафы) со стороны регулирующих органов за нарушение требований федерального законодательства в области защиты персональных данных
  - Снижение репутации музея

КОНЦЕПТУАЛЬНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИБ

КРОК

- Построение комплексной системы защиты информации музея, включающей технические и организационные меры защит



В основе проектирования системы защиты –

моделирование угроз!

ПОТЕНЦИАЛЬНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ МУЗЕЕВ В ОБЛАСТИ ИБ

КРОК

- Организация эффективной защиты ИТ-инфраструктуры музея от угроз ИБ (создание защищенной среды функционирования ИС)

  Проектирование защищенной ИТ-инфраструктуры (сегментирование и пр.)

  Реализация базовых инфраструктурных СЗИ(антивирус, защита от НСД, МЭ и пр.)

- Обеспечение безопасного функционирования информационных систем музея

  Размещение компонент ИС по сегментам

  Внедрение специализированных СЗИ (WAF, защита БД, защита от DDoS-атак и пр.)

- Обеспечение соответствия требованиям 152-ФЗ «О персональных данных»

  Реализация мер защиты в отношении автоматизированной и неавтоматизированной обработки ПДн

  Реализация организационных и технических мер защиты в отношении ИСПДн

ТИПЫ ПОТЕНЦИАЛЬНО НЕОБХОДИМЫХ ТЕХНОЛОГИЙ ЗАЩИТЫ ИТ-ИНФРАСТРУКТУРЫ

КРОК

- Межсетевое экранирование
- Защита от несанкционированного доступа
- Защита от вредоносного ПО и спама
- Защита от утечек конфиденциальной информации
- Мониторинг событий ИБ
- Анализ защищенности
- Защита виртуальной среды
- Защищенный терминальный доступ в Интернет
- Защищенный удаленный мобильный доступ
- Контроль действий администраторов и подрядчиков

ФОРМЫ ИСПОЛЬЗОВАНИЯ ТЕХНОЛОГИЙ ИБ

- Внедрение средств защиты информации внутри ИТ-инфраструктуры музея
- Использование внешних «облачных» сервисов и услуг

ВАРИАНТЫ ОБЛАЧНЫХ СЕРВИСОВ ИБ НА БАЗЕ КРОК

- Размещение общедоступных ИС
  - Web-сайты, Web-порталы
- Размещение инфраструктурных систем
  - Электронная почта, бухгалтерское ПО, документооборот и пр.
- Размещение музейных систем
  - Надежная сохранность баз данных
- Использование сервисов ИБ
  - Защита от НСД
  - Антивирусная защита
  - Межсетевое экранирование
  - Средства криптографической защиты сетевого трафика
  - Средства обнаружения сетевых атак
  - WAF (Web Application Firewall) – углубленная фильтрация web-трафика
  - Мониторинг событий ИБ
  - Защита от DDoS
  - Резервное копирование данных

ПОДХОД К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИС

КРОК

1. Анализ существующих угроз в отношении ИС
2. Формирование требований ИБ к внутренним механизмам защиты ИС с учетом особенностей защиты ИТ-инфраструктуры
3. Формирование требований ИБ к дополнительным механизмам защиты ИТ-инфраструктуры
4. Проектирование и разработка внутренних механизмов защиты ИС
5. Проектирование дополнительных внешних механизмов защиты ИТ-инфраструктуры
6. Внедрение и настройка внутренних и внешних механизмов защиты ИС

ДОПОЛНИТЕЛЬНЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ ИС

КРОК

- **Углубленная фильтрация веб-трафика (Web Application Firewall)** - выявление и блокирование атак на веб-ресурсы
- **Защита баз данных** – наблюдение и анализ действий пользователей, выявление аномальной активности и неавторизованных действий
- **Защита от DDoS-атак** – обеспечение доступности сетевых ресурсов для внешних пользователей в условиях целевой кибератаки
- **Тестирования на проникновение** – поиск уязвимостей

ОБЕСПЕЧЕНИЕ СООТВЕТСТВИЯ ТРЕБОВАНИЯМ 152-ФЗ

КРОК

- Классификация персональных данных
- Определение границ информационных систем ПДн
- Разработка модели угроз и требований к системе защиты
- Проектирование решения
- Разработка эксплуатационной и организационно-распорядительной документации
- Внедрение и эксплуатация системы защиты

ПЕРВООЧЕРЕДНЫЕ ОРГАНИЗАЦИОННЫЕ МЕРЫ ЗАЩИТЫ

- Выделение специальных лиц (подразделений), отвечающих за вопросы ИБ
- Разработка правил по регламентации действий пользователей
- Повышение осведомленности пользователей в вопросах ИБ

КРОК

СПАСИБО ЗА ВНИМАНИЕ!

Евгений Дружинин

Эксперт по информационной безопасности

111033, Москва, ул. Волочаевская, д.5, к.1
Т: (495) 974 2274 | Ф: (495) 974 2277
E-mail: edruzhinin@croc.ru

croc.ru