ДиалогНаука

Практические аспекты проведения аудита с целью оценки соответствия требованиям ФЗ «О персональных данных»

Виктор Сердюк, к.т.н., CISSP

Генеральный директор

ЗАО «ДиалогНаука»

ДиалогНаука

Стадии создания системы защиты персональных данных

- предпроектная стадия, включающая предпроектное обследование ИСПДн (аудит), а также разработку технического задания на ее создание
- стадия проектирования и реализации ИСПДн, включающая разработку СЗПДн в составе ИСПДн
- стадия ввода в действие СЗПДн, включающая опытную эксплуатацию
- приемо-сдаточные испытания средств защиты информации, а также оценку соответствия ИСПДн требованиям безопасности информации

ДиалогНаука

Обследование ИСПДн

- Анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн
- Определение используемых средств защиты ПДн, и оценка их соответствия требованиям нормативных документов РФ
- Определение перечня ПДн, подлежащих защите
- Определение перечня ИСПДн, обрабатывающих ПДн
- Определение степени участия персонала в обработке ПДн, характера взаимодействия персонала между собой

ДиалОгНаука

Анализ внутренних нормативных документов

- сбор существующей нормативной документации Заказчика регулирующей порядок обработки и обеспечения защиты ПДн
- сбор существующей нормативной документации Заказчика описывающей состав, структуру и функциональные возможности, технические характеристики и организацию использования ИСПДн и средств защиты ИСПДн, а так же регламентирующие порядок их взаимодействия
- анализ существующей нормативной документации Заказчика в области обработки и защиты ПДн на предмет соответствия требованием нормативных документов РФ

ДиалогНаука

Определение перечня ИСПДн

На данном этапе определяется перечень ИСПДн и их основные свойства, такие как:

- Структура ИС
- Подключение к сетям общего доступа
- Режим обработки ПДн
- Режим разграничения прав доступа пользователей ИС
- Местонахождение технических средств информационной системы
- Заданные оператором характеристики безопасности персональных данных, обрабатываемых в ИС

ДиалОгНаука

Определение перечня ПДн

Перечень ПДн, обрабатываемых в ИСПДн Заказчика, подлежащих защите включает в себя:

- цели обработки ПДн
- категории ПДн
- категории субъектов, ПДн которых обрабатываются
- правового основания обработки ПДн
- перечня действий с ПДн, общего описания используемых Заказчиком способов обработки ПДн
- сведений о лицах, которые имеют доступ к ПДн или которым может быть предоставлен такой доступ
- источника получения ПДн

ДиалогНаука

Определение используемых средств защиты

- Сбор данных о:
  - Составе и функциональных возможностях используемых СЗПДн
  - Технических характеристиках и организации использования СЗПДн
  - Условиях эксплуатации СЗПДн в составе ИСПДн
- Оценка соответствия используемых средств и методов защиты ПДн нормативным требованиям РФ

ДиалОгНаука

Основные этапы работ

- Заключение соглашения о неразглашении (NDA)
- Разработка регламента, устанавливающего порядок и рамки проведения работ
- Сбор исходной информации об автоматизированной системе компании
- Анализ полученной информации
- Проведение инструментальной части аудита
- Подготовка отчётных материалов
- Презентация и защита результатов проекта

ДиалогНаука

Структура регламента

- Состав рабочих групп от Исполнителя и Заказчика, участвующих в процессе проведения аудита
- Перечень информации, которая будет предоставлена Исполнителю для проведения аудита
- Список объектов информатизации Заказчика, аудит которых должен провести Исполнитель
- Перечень информационных систем, которые рассматриваются Исполнителем в качестве объектов защиты
- Порядок и время проведения инструментального обследования
- Порядок проведения совещаний по проекту

ДиалогНаука

Состав исходных данных

- Информация об организационной структуре компании
- Организационно-распорядительная и нормативно-методическая документация по вопросам информационной безопасности
- Информация об ИС, обрабатывающих персональные данные
- Информация об аппаратном, общесистемном и прикладном обеспечении ИСПДн
- Информация о средствах защиты, установленных в ИСПДн
- Информация о топологии ИСПДн

ДиалОгНаука

Методы сбора исходных данных

- Предоставление опросных листов по определённой тематике, самостоятельно заполняемых сотрудниками Заказчика
- Интервьюирование сотрудников Заказчика, обладающих необходимой информацией
- Анализ существующей организационно-технической документации, используемой Заказчиком
- Использование специализированных программных средств

Инструментальный анализ защищенности

Для чего предназначен:

- Инвентаризация сетевых сервисов ИСПДн (устройства, ОС, службы, ПО)
- Идентификация и анализ технологических уязвимостей ИСПДн

Типы используемых для анализа средств:

- Сетевые сканеры безопасности
- Хостовые сканеры безопасности (проверка ОС и приложений)
- Утилиты удаленного администрирования
- Утилиты для верификации найденных уязвимостей
- Утилиты для инвентаризации ресурсов

ДиалогНаука

Инструментальный анализ защищенности

- Анализ средств защиты информации
  - Анализ VPN-шлюзов
  - Анализ антивирусных средств защиты
  - Анализ систем обнаружения атак IDS/IPS
  - Анализ межсетевых экранов
  - Анализ систем защиты от утечки конфиденциальной информации
- Анализ безопасности сетевой инфраструктуры
  - Анализ безопасности коммутаторов
  - Анализ безопасности маршрутизаторов
  - Анализ безопасности SAN-сетей
  - Анализ безопасности сетей WLAN

ДиалогНаука

Инструментальный анализ защищенности

- Анализ безопасности общесистемного программного обеспечения
  - Анализ ОС Windows
  - Анализ ОС UNIX
  - Анализ ОС Novell Netware
- Анализ безопасности прикладного программного обеспечения
  - Анализ безопасности баз данных
  - Анализ безопасности почтовых серверов
  - Анализ безопасности Web-серверов
  - Анализ безопасности Web-приложений

Особенности использования инструментальных средств для сбора информации

- Заранее оговариваются рамки проведения инструментального аудита
- Результаты анализируются и интерпретируются экспертами
- Производится фильтрация полученных данных
- Используется несколько средств анализа защищённости
- Проверка критически важных систем проводится во внерабочие часы, в присутствии администратора с обязательным резервным копированием информации

ДиалогНаука

Пример элемента методики

Средства защиты от вредоносного кода

- **Описание**: Должны быть внедрены средства определения, предотвращения и восстановления для защиты против вредоносного кода и соответствующие процедуры предупреждения пользователей.
- **Документальная проверка**: документы, отражающие положения по антивирусной защиты информационных систем; должностные инструкции; документы, фиксирующие приобретение антивирусных средств защиты информации.
- **Инструментальный контроль**: методика инструментальной проверки средств защиты от вредоносного и мобильного кода.
- **Результат**: отчет; отчет об инструментальном анализе (детальная информация об эффективности применяемых средств защиты)

Критерии оценки

		Документальные подтверждения требований		
Дополнительные инструментальные подтверждения требований		Не установлены	Установлены частично	Установлены в полном объеме
	Не выполняются	0	0.25	0.5
	Выполняются частично	0.25	0.25	0.75
	Выполняются в полном объеме	0.5	0.75	1

Тест на проникновение (Penetration testing)

Тест на проникновение позволяет получить независимую оценку безопасности ИСПДн по отношению к внешнему нарушителю

Исходные данные

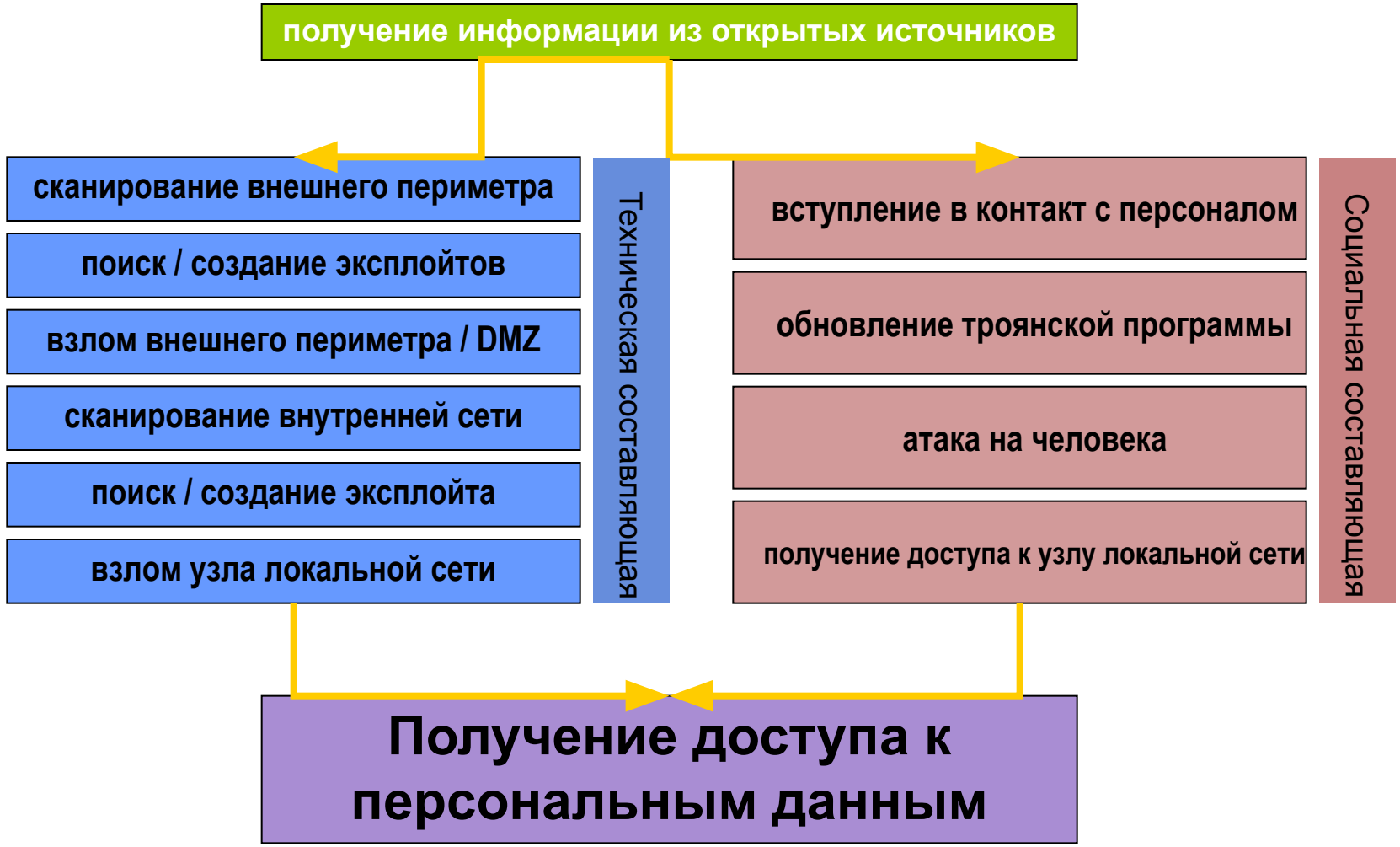
- IP-адреса внешних серверов
- Анализ проводится с внешнего периметра

Собираемая информация

- Топология сети
- Используемые ОС и версии ПО
- Запущенные сервисы
- Открытые порты, конфигурация и т.д.

ДиалогНаука

Обобщенный план теста на проникновение



ДиалогНаука

Структура итогового отчёта

- Границы проведения аудита безопасности
- Описание ИСПДн Заказчика
- Методы и средства проведения аудита
- Результаты классификации ИСПДн
- Частная модель угроз безопасности ПДн
- Требования по защите персональных данных
- Рекомендации по совершенствованию системы защиты персональных данных
- План мероприятий по созданию системы защиты персональных данных

ДиалОгНаука

Продолжительность этапов

Этап	Занимаемое время, %
Подготовительные работы (подписание NDA, подготовка регламента работ и т.д.)	10
Сбор необходимой информации (анкетирование, интервьюирование)	15
Анализ действующей нормативной документации	10
Инструментальное обследование	20
Анализ полученных данных	20
Подготовка отчетных материалов	20
Презентация и защита отчета	5

ДиалогНаука

Дальнейшие действия по результатам

Результаты аудита являются **основой** для проведения дальнейших работ по повышению информационной безопасности:

- ★ Совершенствование организационно-правового обеспечения Заказчика (разработка Политики безопасности, должностных инструкций, регламентов и т.д.)
- ★ Проектирование, разработка, внедрение и сопровождение систем защиты, устраняющих уязвимости, выявленные в процессе проведения аудита безопасности
- ★ Обучение персонала Заказчика

ДиалогНаука

Наши контакты

117105, г. Москва, ул. Нагатинская, д. 1

Телефон: +7 (495) 980-67-76
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: vas@DialogNauka.ru