ДиалогНаука

# Практические аспекты аудита информационной безопасности

*Виктор Сердюк, к.т.н.,*

*Генеральный директор*
*ЗАО «ДиалогНаука»*

ДиалогНаука

# О компании «ДиалогНаука»

- Создано в 1992 году  СП «Диалог» и Вычислительным центром РАН
- Первыми и самыми известными отечественными продуктами, поставляемыми компанией, были ревизор ADinf, Doctor Web и Aidstest
- В настоящее время ДиалогНаука является системным интегратором в области информационной безопасности

ДиалОгНаука

# План презентации

- Что такое аудит информационной безопасности?
- Виды аудита информационной безопасности
- Состав работ по проведению аудита безопасности
- Методы сбора исходной информации при проведении аудита
- Методика проведения аудита информационной безопасности
- Результаты проведения аудита
- Сертификация и оценка соответствия требованиям информационной безопасности

ДиалОгНаука

# Услуги по проведению аудита информационной безопасности

**ЦЕЛЬ:** Получить независимую и объективную оценку текущего уровня информационной безопасности

- Перед внедрением комплексной системы безопасности для подготовки ТЗ на её разработку и создание
- После внедрения комплексной системы безопасности для оценки уровня её эффективности
- Для приведения системы информационной безопасности в соответствие установленным требованиям (международные стандарты или требования российского законодательства)
- Для систематизации и упорядочивания существующих мер защиты информации
- Для проверки эффективности работы подразделений компании, ответственных за обеспечение ИБ
- Для обоснования инвестиций в направление информационной безопасности

ДиалогНаука

# Внешний и внутренний аудит безопасности

Внутренний аудит:

- Проводится внутренними подразделениями компании (отделом ИБ, отделом ИТ или службой внутреннего контроля)
- Рекомендуется проводить не реже 1 раза в квартал

Внешний аудит:

- Проводится с привлечением внешней организации
- Рекомендуется проводить не реже 1 раза в год

ДиалОгНаука

# Конечные потребители результатов аудита

Внутренние пользователи:

- Руководство компании
- Подразделение информационной безопасности
- Служба безопасности
- Подразделение автоматизации предприятия
- Служба внутреннего контроля/аудита

Внешние пользователи:

- Акционеры компании
- Регулирующие органы
- Клиенты компании

ДиалогНаука

# Варианты проведения аудита

- Тест на проникновение (penetration testing)
- Инструментальный анализ защищённости автоматизированной системы
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта ISO 27001 (ISO 27002)
- Оценка соответствия стандарту Банка России СТО БР ИББС
- Сертификационный аудит соответствия PCI DSS
- Оценка соответствия требованиям Федерального закона «О персональных данных»
- Аудит наличия конфиденциальной информации в сети Интернет
- Оценка и анализ рисков информационной безопасности
- Комплексный аудит информационной безопасности

ДиалогНаука

# Тест на проникновение (Penetration testing)

**Тест на проникновение позволяет получить независимую оценку безопасности компании глазами потенциального злоумышленника**

## Исходные данные

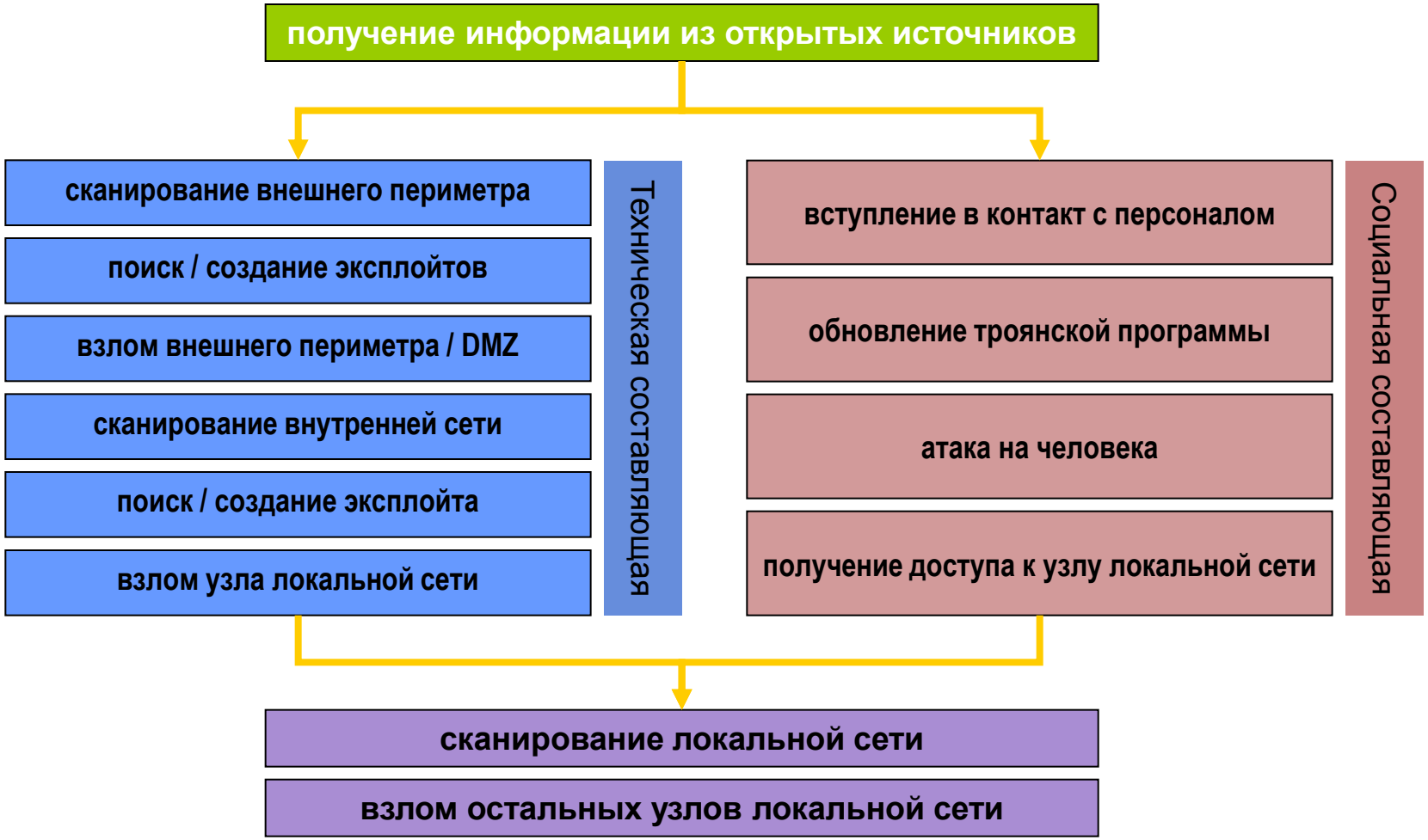
- IP-адреса внешних серверов
- Анализ проводится с внешнего периметра

## Собираемая информация

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

ДиалогНаука

# Обобщенный план удаленного аудита



ДиалогНаука

# Инструментальный анализ защищенности

## Для чего предназначен:

- Инвентаризация ресурсов сети (устройства, ОС, службы, ПО)
- Идентификация и анализ технологических уязвимостей
- Подготовка отчетов, описание проблем и методов устранения

## Типы используемых для анализа инструментальных 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

ДиалОгНаука

# Примеры выявляемых уязвимостей

- Наличие неустановленных обновлений ПО (patch’ей, hotfix’ов и др.)
- Наличие учетных записей и паролей доступа «по умолчанию»
- Неправильная конфигурация средств защиты информации
- Наличие в сети потенциально-опасных сервисов (telnet, неиспользуемые службы)

ДиалогНаука

# Разновидности инструментального аудита

- Оценка защищенности Web-приложений
- Оценка защищенности систем ДБО
- Оценка защищенности прикладного ПО
- Оценка защищенности беспроводных сетей связи
- Оценка устойчивости компании к атакам класса «отказ в облуживании»

ДиалОгНаука

# Аудит СУИБ по стандарту ISO 17799 (ISO 27002)

1. Политика безопасности
2. Организационные меры безопасности
3. Учет и категорирование информационных ресурсов
4. Кадровые аспекты ИБ
5. Физическая защита информационных ресурсов
6. Управление технологическим процессом
7. Управление доступом
8. Закупка, разработка и сопровождение компонент ИС
9. Управление инцидентами в области информационной безопасности
10. Обеспечение непрерывности работы и восстановления
11. Соответствие нормативным и руководящим документам

ДиалогНаука

# Пример элемента методики

Средства защиты от вредоносного кода (10.4.1)

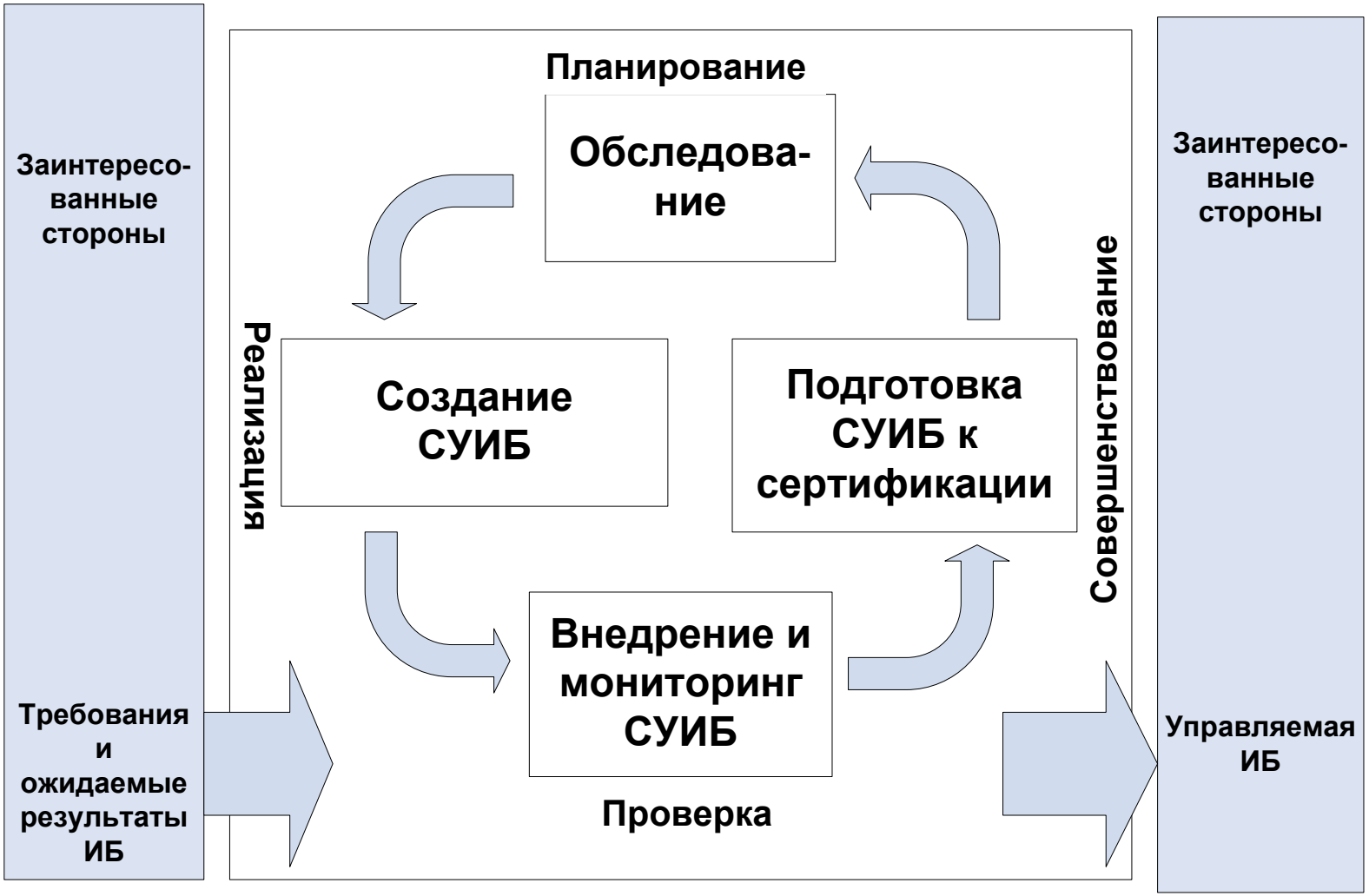
- **Описание**: Должны быть внедрены средства определения, предотвращения и восстановления для защиты против вредоносного кода и соответствующие процедуры предупреждения пользователей.
- **Документальная проверка**: документы, отражающие положения по антивирусной защиты информационных систем; должностные 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 |

ДиалогНаука

# Оценка соответствия ISO 27001



ДиалогНаука

# Определение уровня зрелости

| Уровень зрелости | Описание |
|---|---|
| 0 | Полное отсутствие процесса в рамках деятельности организации. |
| 1 | **«Начальный»**. Используемый процесс нестандартизован, применяется эпизодически и бессистемно. |
| 2 | **«Повторяемый»**. Процесс проработан до уровня, когда его выполнение обеспечивается различными людьми, решающими одну и ту же задачу. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а ответственность возложена на исполнителя. |
| 3 | **«Определенный»**. Характеризует то, что процессы стандартизованы, документированы и доведены до персонала посредством обучения. Однако порядок использования данных процессов оставлен на усмотрение самого персонала. Это определяет вероятность отклонений от стандартных процедур, которые могут быть не выявлены. Применяемые процедуры не оптимальны и недостаточно современны, но являются отражением практики, используемой в организации. |
| 4 | **«Управляемый»**. Характеризует то, что обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов менеджмента ИБ обеспечивается их оптимизация. Процессы менеджмента ИБ находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации менеджмента ИБ используются частично и в ограниченном объеме. |
| 5 | **«Оптимизированный»**. Характеризует проработанность процессов менеджмента ИБ до уровня лучшей практики, основанной на результатах непрерывного совершенствования и сравнения уровня зрелости относительно других организаций. |

ДиалОгНаука

# Аудит наличия конфиденциальной информации

- Аудит наличия конфиденциальной информации представляет собой независимый и документированный процесс поиска и анализа конфиденциальных сведений в сети Интернет при помощи средств конкурентной разведки
- Поиск информации осуществляется: на форумах, в блогах, в электронных СМИ, в гостевых книгах, на досках объявлений, в дневниках, конференциях и т.д.
- По результатам проведённого поиска проводится выдача «оценочной» информации в виде отчёта. Отчёт содержит следующую информацию:
  1. область поиска (где осуществлялся поиск);
  2. найденная конфиденциальная информация;
  3. где найдена конфиденциальная информация;
  4. рекомендации по устранению (удалению) найденной конфиденциальной информации в Интернете

ДиалОгНаука

# Услуги в области мониторинга Интернет-ресурсов

**Вариант 1 – ежедневный мониторинг**

- Объекты мониторинга: Интернет-сайты, поисковые системы, RSS-потоки, блоги, форумы, чаты, социальные сети.
- Направленность мониторинга: оперативное выявление угроз бизнесу, репутации и развитию. Мониторинг проводится по компании и ее руководству.
- Обновление новостной ленты – ежедневно.
- Оповещение о серьезных событиях и угрозах – ежедневно.
- Сводная справка по основным событиям – ежемесячно.
- Аналитическая поддержка: 8x5

ДиалогНаука

# Услуги в области мониторинга Интернет-ресурсов

**Вариант 2 – оперативный мониторинг в реальном времени**

- Объекты мониторинга: Интернет-сайты, поисковые системы, RSS-потоки, блоги, форумы, чаты, социальные сети.
- Направленность мониторинга: оперативное выявление утечек и угроз бизнесу, репутации и развитию. Мониторинг проводится по компании и ее руководству.
- Раннее выявление уязвимостей и утечек на порталах компании, партнеров и конкурентов.
- Обновление новостной ленты – в реальном времени.
- Оповещение о серьезных событиях и угрозах – в течение двух часов.
- Сводная справка по основным событиям – еженедельно.
- Аналитическая поддержка: 8x5

ДиалогНаука

# Услуги в области мониторинга Интернет-ресурсов

**Вариант 3 – расширенный оперативный мониторинг**

- Объекты мониторинга: Интернет-сайты, поисковые системы, RSS-потоки, блоги, форумы, чаты, социальные сети.
- Направленность мониторинга: оперативное выявление утечек и угроз бизнесу, репутации и развитию. Мониторинг проводится по компании, руководству, конкурентам и другим объектам интереса.
- Раннее выявление уязвимостей и утечек на порталах компании, партнеров и конкурентов.
- Обновление новостной ленты – в реальном времени.
- Оповещение о серьезных событиях и угрозах – в течение часа.
- Сводная справка по основным событиям – еженедельно.
- Автоматическое пополнение досье по всем объектам интереса (компаниям и персонам).
- Аналитическая поддержка: 24x7

ДиалогНаука

# Оценка соответствия стандарту Банка России

**Услуги по внедрению СТО БР ИББС:**

- Проведение оценки соответствия СТО БР ИББС
- Внедрение СТО БР ИББС в части защиты ПДн
- Внедрение СТО БР ИББС в части реализации системы менеджмента информационной безопасности

**Стандарт пока носит необязательный характер**

**Для подключения к НПС потребуется соответствие стандарту СТОБ Р ИББС**

**ЗАО «ДиалогНаука» - организация-консультант и организация-аудитор НП «АБИСС»**

**Детальная информация о стандартах ЦБ РФ –** www.abiss.ru

ДиалогНаука

# Оценка и анализ рисков безопасности

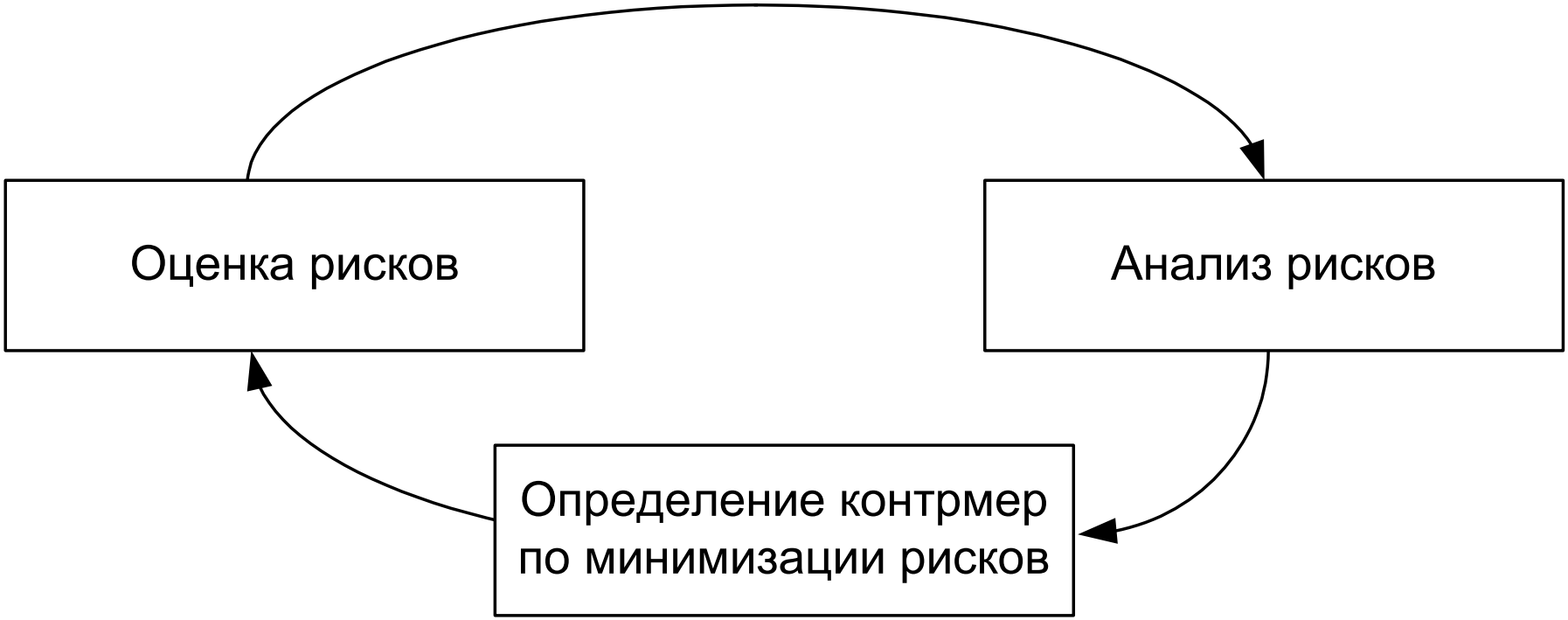
**Риск** - вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда (Закон о техническом регулировании)

**Риск нарушения информационной безопасности** - неопределенность, предполагающая возможность ущерба состояния защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз в информационной сфере (СТО БР ИББС 1.0)

**Риск** – комбинация вероятности возникновения последствия и его возможных последствий (ISO 17799:2005)

ДиалогНаука

# Оценка, анализ и управление рисками безопасности



ДиалогНаука

# Оценка и анализ рисков безопасности

- Идентификация информационных активов
- Формирование каталога возможных угроз безопасности
- Оценка уровня вероятности реализации угроз безопасности
- Оценка уровня ущерба, который может быть нанесен в случае реализации угрозы
- Определение интегрального значения риска безопасности
- Анализ рисков безопасности

ДиалогНаука

# Идентификация активов

- Информационные ресурсы, которые обеспечивают выполнение бизнес-процессов, заданных рамками проекта
- Прикладное и общесистемное программное обеспечение
- Аппаратное обеспечение
- Телекоммуникационное обеспечение
- Электронные носители
- Бумажные носители
- Помещения, где хранится и обрабатывается защищаемая информация

# Оценка рисков безопасности

- Оценка может осуществляться на основе количественных и качественных шкал
- Примерами методик оценки рисков являются NIST-800, OCTAVE, CRAMM, Методика оценки РС БР ИББС – 2.3 (проект) и т.д.
- Методика предполагает разработку модели угроз для информационных активов, определенных в рамках проекта

## Качественная шкала оценки уровня ущерба

1. **Малый ущерб**
   Приводит к незначительным потерям материальных активов, которые быстро восстанавливаются, или к незначительному влиянию на репутацию компании

2. **Умеренный ущерб**
   Вызывает заметные потери материальных активов или к умеренному влиянию на репутацию компании

3. **Ущерб средней тяжести**
   Приводит к существенным потерям материальных активов или значительному урону репутации компании

4. **Большой ущерб**
   Вызывает большие потери материальных активов или наносит большой урон репутации компании

5. **Критический ущерб**
   Приводит к критическим потерям материальных активов или к полной потере репутации компании на рынке

# Качественная оценка рисков

## Качественная шкала оценки вероятности проведения атаки

1. **Очень низкая**
   Атака практически никогда не будет проведена.
   Уровень соответствует числовому интервалу вероятности **[0, 0.25)**

2. **Низкая**
   Вероятность проведения атаки достаточно низкая.
   Уровень соответствует числовому интервалу вероятности **[0.25, 0.5)**

3. **Средняя**
   Вероятность проведения атаки приблизительно равна **0,5**

4. **Высокая**
   Атака, скорее всего, будет проведена.
   Уровень соответствует числовому интервалу вероятности **(0.5, 0.75]**

5. **Очень высокая**
   Атака почти наверняка будет проведена.
   Уровень соответствует числовому интервалу вероятности **(0.75, 1]**

# Качественная оценка рисков

## Пример таблицы определения уровня риска ИБ

| Вероятность атаки / Ущерб | Очень низкая | Низкая | Средняя | Высокая | Очень высокая |
|---|---|---|---|---|---|
| **Малый ущерб** | Низкий риск | Низкий риск | Низкий риск | Средний риск | Средний риск |
| **Умеренный ущерб** | Низкий риск | Низкий риск | Средний риск | Средний риск | Высокий риск |
| **Средний ущерб** | Низкий риск | Средний риск | Средний риск | Высокий риск | Высокий риск |
| **Большой ущерб** | Средний риск | Средний риск | Высокий риск | Высокий риск | Высокий риск |
| **Критический ущерб** | Средний риск | Высокий риск | Высокий риск | Высокий риск | Высокий риск |

# Качественная оценка рисков

## Определение допустимого уровня риска

| Вероятность атаки / Ущерб | Очень низкая | Низкая | Средняя | Высокая | Очень высокая |
|---|---|---|---|---|---|
| **Малый ущерб** | Допусти-мый риск | Допусти-мый риск | Допусти-мый риск | Допусти-мый риск | Допусти-мый риск |
| **Умеренный ущерб** | Допусти-мый риск | Допусти-мый риск | Допусти-мый риск | Допусти-мый риск | Недопусти-мый риск |
| **Средний ущерб** | Допусти-мый риск | Допусти-мый риск | Допусти-мый риск | Недопусти-мый риск | Недопусти-мый риск |
| **Большой ущерб** | Допусти-мый риск | Допусти-мый риск | Недопусти-мый риск | Недопусти-мый риск | Недопусти-мый риск |
| **Критический ущерб** | Средний риск | Недопусти-мый риск | Недопусти-мый риск | Недопусти-мый риск | Недопусти-мый риск |

# Количественная оценка рисков

## Количественная шкала оценки вероятности проведения атаки

Вероятность проведения атаки измеряется от 0 до 1

## Количественная шкала оценки уровня ущерба

Ущерб измеряется в финансовом эквиваленте (в денежном выражении)

**РИСК = Вероятность угрозы X Ущерб**

ДиалогНаука

# Анализ рисков

- Определение приемлемого уровня риска
- Выбор защитных мер, позволяющих минимизировать риски до приемлемого уровня
- Варианты управления рисками безопасности
  - уменьшение риска за счёт использования дополнительных организационных и технических средств защиты;
  - уклонение от риска путём изменения архитектуры или схемы информационных потоков АС;
  - изменение характера риска, например, в результате принятия мер по страхованию;
  - принятие риска в том случае, если он уменьшен до того уровня, на котором он не представляет опасности для АС

ДиалОгНаука

# Пример расчета риска

- **Информационный ресурс** – база данных с бухгалтерской информацией
- **Угроза** – утечка конфиденциальной информации посредством её копирования на внешние носители или передача за пределы контролируемой зоны
- **Ущерб** – Большой
- **Вероятность реализации угрозы** – Большая
- **Результирующий риск** – *Высокий* (*недопустимый*)

ДиалОгНаука

# ФЗ «О персональных данных» № 152

- Федеральный закон «О персональных данных» № 152-ФЗ был принят Государственной думой 08.07.2006 и одобрен Советом Федерации 14.07.2006
- Федеральный закон полностью вступил в силу с 01.07.2011
- Федеральным законом регулируются отношения, связанные с обработкой персональных данных
- **Персональные данные** - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

ДиалОгНаука

# ФЗ «О персональных данных» № 152

- **Оператор** - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данным
- **Обработка персональных данных** - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных

ДиалОгНаука

# Требования ФЗ «О персональных данных»

- Оператор обязан принимать организационные и технические меры, для защиты ПДн от НСД, уничтожения, изменения, блокирования, копирования, распространения и иных неправомерных действий
- Правительство РФ устанавливает требования к обеспечению безопасности ПДн при их обработке
- Федеральные органы в области обеспечения безопасности (ФСБ России, ФСТЭК России) осуществляют контроль и надзор
- Лица, виновные в нарушении требований несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность

ДиалОгНаука

# Ответственность

- Меры по приостановлению или прекращению обработки ПДн
- Приостановка действия или лишение лицензий, без которых деятельность по обработке персональных данных становится незаконной.
- Изъятие несертифицированных средств защиты информации
- Привлечение к административной или уголовной ответственности лиц, виновных в нарушении соответствующих статей уголовного или административного кодекса

ДиалОгНаука

# Требования ФЗ «О персональных данных»

Статья 21. Пункт 3. В случае выявления неправомерной обработки персональных данных, …, оператор в срок, не превышающий трех рабочих дней с даты этого выявления, обязан ***прекратить неправомерную обработку персональных данных или обеспечить прекращение неправомерной обработки персональных данных лицом, действующим по поручению оператора***. В случае ***если обеспечить правомерность обработки персональных данных невозможно***, оператор в срок, не превышающий ***десяти*** рабочих дней с даты выявления ***неправомерной обработки*** персональных данных, обязан уничтожить такие персональные данные ***или обеспечить их уничтожение***.

# ФЗ «О персональных данных»

Информационные системы персональных данных, созданные до 1 января 2011 года, должны быть приведены в соответствие с требованиями настоящего Федерального закона **не позднее 1 июля 2011 года**

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
- перечень 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
- источник 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

# Предпроектная стадия

**Результаты этапа**:

- Отчет о проведенном обследовании, содержащий оценку текущего уровня соответствия требованиям законодательства и детальные рекомендации по устранению выявленных недостатков
- Модель угроз безопасности
- Модель нарушителя

ДиалогНаука

# Комплексный аудит информационной безопасности

- Подмножество из различных видов аудита информационной безопасности
- Может включать в себя:
  - тест на проникновение;
  - инструментальный аудит;
  - оценку соответствия СТО БР ИББС;
  - оценку соответствия ISO 27001;
  - оценку соответствия требованиям ФЗ-152;
  - оценку рисков информационной безопасности

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 собранной информации с целью выявления технологических, эксплуатационных уязвимостей, а также недостатков организационно-правового обеспечения
- 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
- Роли участников проекта
- Порядок обмена информацией по проекту
- Порядок и время проведения инструментального обследования
- Порядок проведения совещаний по проекту

# Определение рамок проекта

- Область действия (scope) может охватывать наиболее критические бизнес-процессы компании
- На этапе определения границ проекта необходимо учитывать взаимодействие различных бизнес-процессов
- Область действия может определяться на основе следующих критериев:
  - Ключевые бизнес-задачи компании
  - Наиболее критическая информация
  - Ключевые информационные системы компании

ДиалогНаука

# Состав исходных данных

- Информация об организационной структуре компании
- Организационно-распорядительная и нормативно-методическая документация по вопросам информационной безопасности
- Информация об ИТ-активах, влияющих на бизнес-процессы компании
- Информация об аппаратном, общесистемном и прикладном обеспечении хостов
- Информация о средствах защиты, установленных в компании
- Информация о топологии автоматизированной системы компании

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

ДиалогНаука

# Критерии оценки безопасности

- Нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности
- Требования действующего российского законодательства (РД ФСТЭК, СТР-К, ГОСТы)
- Требования отраслевых стандартов (СТО БР ИББС 1.0, 382-П, PCI DSS)
- Рекомендации международных стандартов (ISO 17799, OCTAVE)
- Рекомендации компаний-производителей программного и аппаратного обеспечения (Microsoft, Oracle, Cisco и т.д.)

ДиалогНаука

# Структура итогового отчёта

- Границы проведения аудита безопасности
- Описание АС Заказчика
- Методы и средства проведения аудита
- Результаты инструментального анализа защищенности
- Результаты оценки соответствия требованиям международного стандарта ISO27001
- Результаты оценки рисков безопасности
- Результаты внешнего обследования (penetration testing)
- Рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности
- План мероприятий по реализации рекомендаций в области информационной безопасности

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

# Подготовка к сертификации по 27001

- Проводится аудит АС и осуществляется подготовка к сертификации на соответствие требованиям Международного стандарта 27001
- Саму сертификацию проводит BSI
- Компания «ДиалогНаука» - партнер BSI
- Выгодно с точки зрения экономии затрат на подготовку к сертификации

ДиалОгНаука

# Аттестация АС на требования ФСТЭК

«Аттестат соответствия» подтверждает, что объект соответствует требованиям стандартов, утвержденных ФСТЭК России. Дает право обработки информации с уровнем конфиденциальности и на период времени, установленными в «Аттестате соответствия»

- При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от НСД, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации.
- Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации.

ДиалогНаука

# Преимущества аудита безопасности

- Лучшее понимание руководством и сотрудниками целей, задач, проблем организации в области ИБ
- Осознание ценности информационных ресурсов
- Надлежащее документирование процедур и моделей ИС с позиции ИБ
- Принятие ответственности за остаточные риски

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: consulting@DialogNauka.ru