ДиалогНаука

Практические аспекты проведения аудита информационной безопасности компании

Романов Илья, CISA, CISM
Заместитель руководителя
Отдела консалтинга
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

Членство в ассоциациях

- Межрегиональная общественная организация «Ассоциация защиты информации» (АЗИ),
- Ассоциация документальной электросвязи (АДЭ),
- Сообщество ABISS (Association of Banking Information Security Standards)
- Ассоциация предприятий компьютерных и информационных технологий (АП КИТ)
- Консорциум «Инфорус»
- Британский Институт Стандартов (British Standards Institution Management Systems)

ДиалогНаука

Основные направления деятельности

- проведение аудита информационной безопасности
- разработка системы управления безопасностью в соответствии с ISO 27001
- разработка Политик информационной безопасности и других нормативных документов, регламентирующих вопросы защиты информации
- проектирование, разработка и внедрение комплексных систем обеспечения информационной безопасности
- поставка программного и аппаратного обеспечения в области защиты информации
- техническое сопровождение поставляемых решений и продуктов

ДиалогНаука

Лицензии компании «ДиалогНаука»

- Лицензия ФСТЭК на деятельность по разработке и (или) производству средств защиты конфиденциальной информации. КИ 0105 005225. № 0904 от 22 августа 2011 г.
- Лицензия ФСТЭК на деятельность по технической защите конфиденциальной информации. КИ 0105 005224, № 1565 от 22 августа 2011 г.
- Лицензия ФСБ на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем. № 10824 П от 21 июня 2011 г.
- Лицензия ФСБ на осуществление технического обслуживания шифровальных (криптографических) средств. № 10825 Х от 21 июня 2011 г.
- Лицензия ФСБ на распространение шифровальных (криптографических) средств. № 10826 Р от 21 июня 2011 г.
- Лицензия ФСБ на предоставления услуг в области шифрования информации. № 10827 У от 21 июня 2011 г.
- Свидетельство об аккредитации Роскомнадзор в области персональных данных № 54 от 1 ноября 2012 г.

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

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

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

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

Варианты проведения аудита

- Тест на проникновение (penetration testing)
- Инструментальный анализ защищённости автоматизированной системы
- Аудит безопасности, направленный на оценку соответствия требованиям стандарта ISO 27001 (ISO17799)
- Оценка соответствия стандарту Банка России
- Оценка соответствия требованиям 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

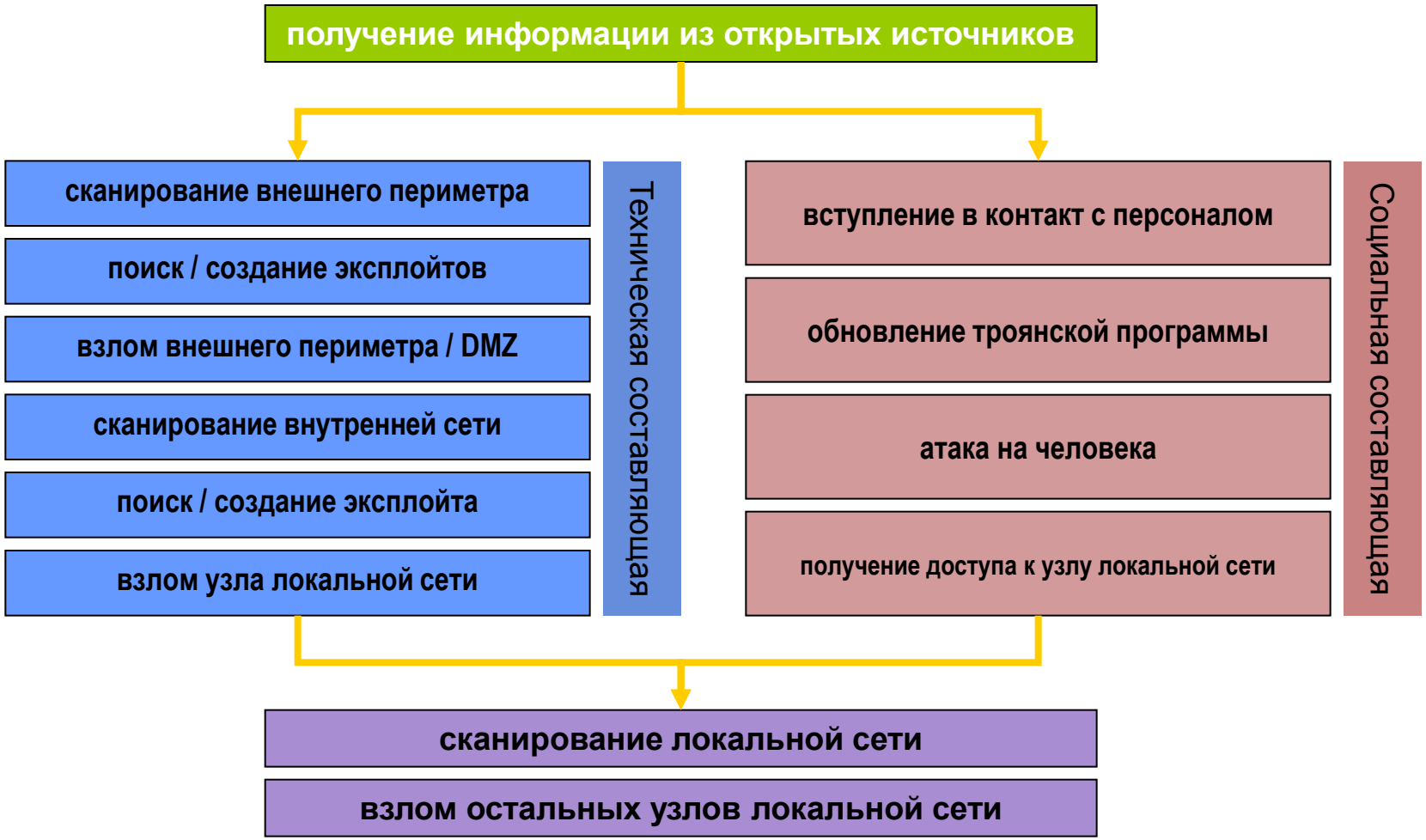
- IP-адреса внешних серверов
- Анализ проводится с внешнего периметра

Собираемая информация

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

ДиалогНаука

Обобщенный план удаленного аудита



ДиалогНаука

Инструментальный аудит

Цель: Идентификация и анализ технологических и эксплуатационных уязвимостей

Варианты реализации:

- Инструментальный аудит внутренней локальной вычислительной сети компании
- Инструментальный аудит Web-приложений (Интернет-порталов)
- Инструментальный аудит внешнего периметра безопасности компании

Типы средств используемых для анализа безопасности:

- Сетевой сканер безопасности Max Patrol, WebInspect, Nessus
- Экспертный анализ конфигурационных файлов

ДиалогНаука

Инструментальный анализ защищенности

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

ДиалогНаука

Инструментальный анализ защищенности

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

Инструментальный аудит

Инструментальный аудит ≠ Сетевое сканирование

ДиалогНаука

Особенности использования инструментальных средств для сбора информации

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

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

Пример элемента методики

Средства защиты от вредоносного кода (10.4.1)

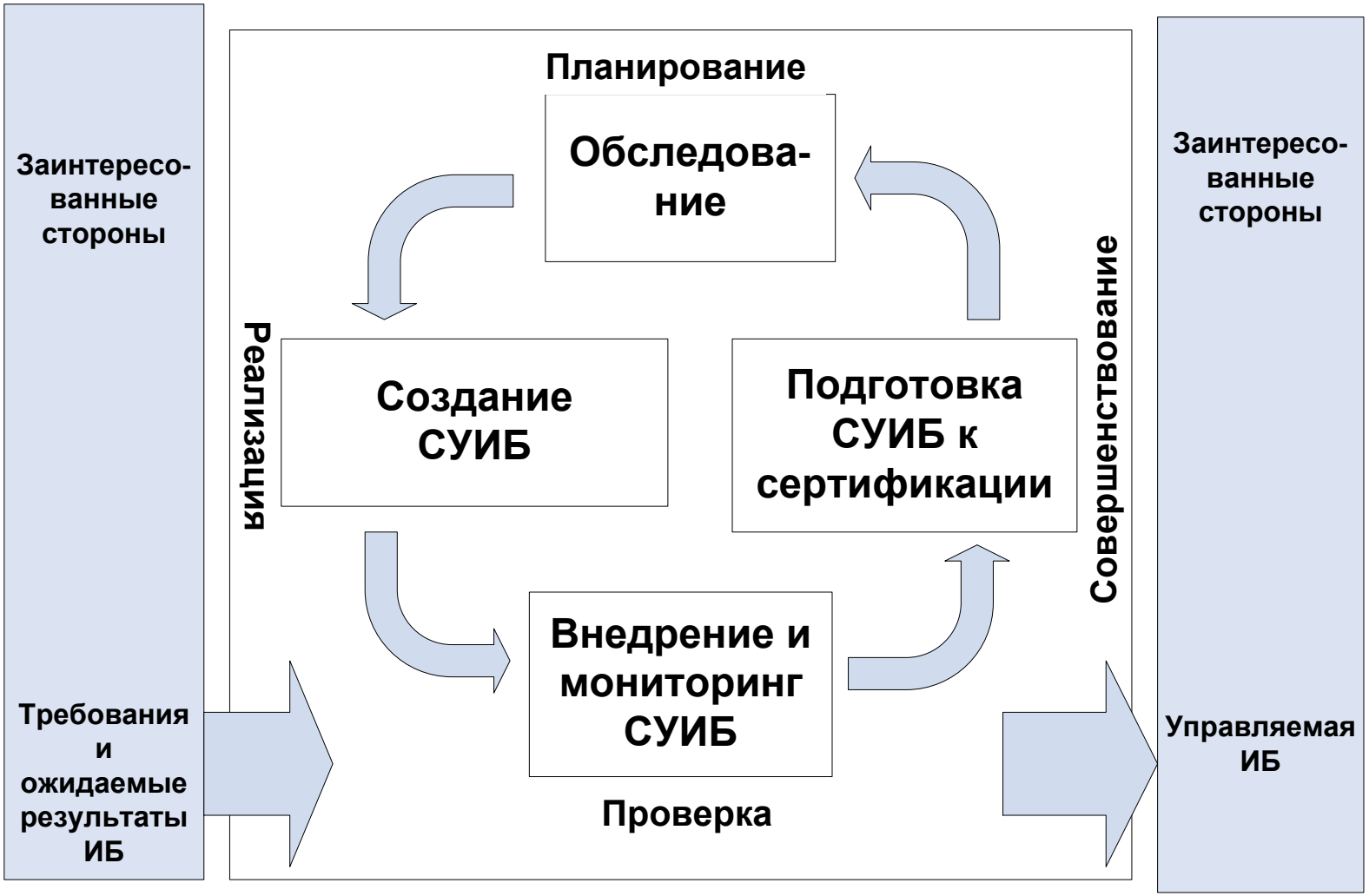
- **Описание**: Должны быть внедрены средства определения, предотвращения и восстановления для защиты против вредоносного кода и соответствующие процедуры предупреждения пользователей.
- **Документальная проверка**: документы, отражающие положения по антивирусной защиты информационных систем; должностные 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		
		Не установлены	Установлены частично	Установлены в полном объеме
Дополнительные инструментальные подтверждения требований	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

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 СТО БР ИББС

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

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

ДиалогНаука

Оценка соответствия PCI DSS

- Анализ рисков ИБ
- Ежеквартальные сканирования уязвимостей из сети Интернет (делает только внешняя компания)
- Ежеквартальные сканирования уязвимостей из ЛВС
- Тестирование на проникновение из сети Интернет и ЛВС
- Сертификационный аудит (делает только внешняя компания)

ДиалогНаука

Оценка и анализ рисков безопасности

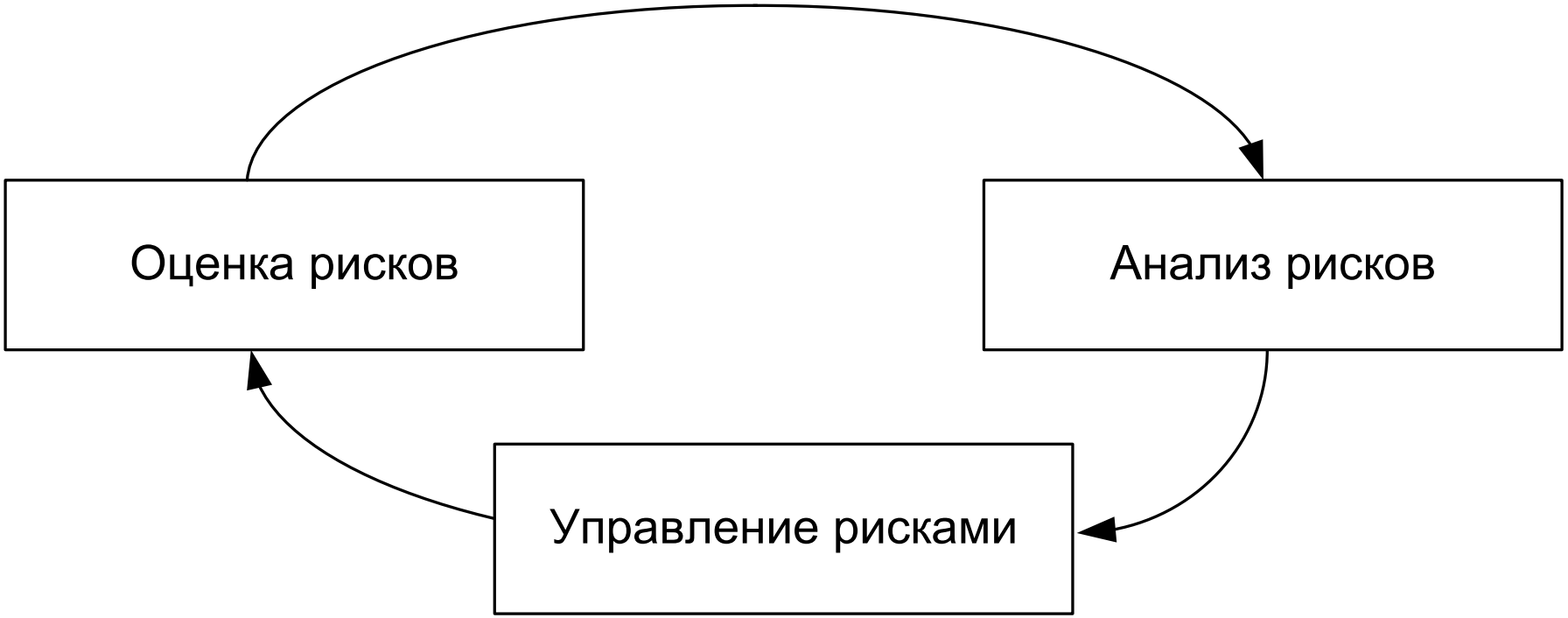
Риск - вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда (Закон о техническом регулировании)

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 события 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

ДиалогНаука

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 – 2.2 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 информационной безопасности

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	Допусти-мый 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

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*)
- **Управление риском** – уменьшение риска за счет внедрения системы DLP

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
- Вышло 13 законов, вносящих изменения в 152-ФЗ, в том числе 2 раза 152-ФЗ был существенно переработан, что свидетельствует о сложности реализации закона.
- Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

ДиалОгНаука

Ответственность

- Меры по приостановлению или прекращению обработки ПДн, вплоть до удаления ПДн (ст. 21, п. 3).
- Приостановка действия или лишение лицензий, без которых деятельность по обработке персональных данных становится незаконной.
- Привлечение к административной или уголовной ответственности лиц, виновных в нарушении соответствующих статей уголовного или административного кодекса
- В планах: Реестр нарушителей правил обработки ПДн

ДиалогНаука

Новые штрафы

Нарушение	Штраф	
	Должностное лицо	Юридическое лицо
Непредставление общедоступной Политики	6 000	30 000
Непредставление ответа субъекту	6 000	40 000
Нарушение требований к содержанию согласия	8 000	50 000
Инцидент с материальными носителями ПДн	10 000	50 000
Обработка ПДн без согласия	15 000	50 000
Инцидент в ИСПДн	15 000	200 000
Незаконная обработка специальных ПДн	25 000	300 000
Инцидент в государственных ИСПДн	50 000	–

ДиалогНаука

Регуляторы

- Роскомнадзор (аудит ОРД)
- ФСБ (аудит СКЗИ)
- ФСТЭК (аудит технических средств защиты информации)
- Центробанк (в части кредитно-финансовых организаций, принявших СТО БР ИББС)

ДиалОгНаука

Примеры информационных систем, обрабатывающие персональные данные

- Бухгалтерские программы
- Программы кадрового учета
- CRM-системы с информацией о действующих и потенциальных клиентах
- Системы биллинга
- ERP-системы, обрабатывающие персональные данные
- и др.

ДиалогНаука

Как построить систему защиты ПДн?

Обследование

Процессы обработки | ИТ, ИБ

Проектирование и создание СЗПДн

ОРД | Проектная документация СЗПДн

Ввод в действие СЗПДн

Внедрение процессов | Внедрение СЗИ

Оценка соответствия СЗПДн

ДиалогНаука

Обследование

- Анализ внутренних нормативных документов, регламентирующих порядок обработки и защиты ПДн;
- Определение перечня ПДн, подлежащих защите;
- Определение перечня ИСПДн, обрабатывающих ПДн;
- Определение используемых средств защиты ПДн, и оценка их соответствия требованиям нормативных документов РФ;
- Разработка частной модели нарушителя и угроз информационной безопасности ПДн;
- Выбор уровней защищенности ПДн

ДиалогНаука

Оценка эффективности реализованных мер по защите

Оценка эффективности реализованных мер должна проводиться не реже 1 раза в 3 года.

Возможные варианты оценки эффективности:

- Декларирование соответствия
- Аттестация информационной системы персональных данных

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 PCI DSS;
  - 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 взаимодействия Заказчика и Исполнителя

- Уточнение задач проведения аудита безопасности
- Состав рабочих групп от Исполнителя и Заказчика, участвующих в процессе проведения аудита
- Роли участников проекта
- Перечень информации, которая будет предоставлена Исполнителю для проведения аудита
- Порядок обмена информацией между Исполнителем и Заказчиком
- 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

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

ДиалогНаука

Анализ исходных данных

- Нормативно-правовые документы предприятия, касающиеся вопросов информационной безопасности
- Требования действующего российских нормативно-правовых документов (РД ФСТЭК, СТР-К, ГОСТы, ФЗ 152)
- Требования отраслевых стандартов (СТО БР ИББС, базовый уровень информационной безопасности операторов связи)
- Рекомендации международных стандартов (ISO 27002 (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 автоматизированной системы Заказчика
- Методы и средства проведения аудита
- Результаты проведенного аудита:
  - Результаты инструментального анализа защищенности
  - Результаты оценки соответствия требованиям международного стандарта ISO27001
  - Результаты оценки соответствия СТО БР ИББС
  - Результаты оценки ФЗ-152
  - Результаты оценки рисков безопасности
  - Результаты теста на проникновение
- Рекомендации по совершенствованию комплексной системы обеспечения информационной безопасности
- План мероприятий по реализации рекомендаций в области информационной безопасности

ДиалОгНаука

Продолжительность этапов

Этап	Занимаемое время, %
Анализ действующей нормативной документации	10
Подготовительные работы (подписание NDA, подготовка регламента работ и т.д.)	10
Сбор необходимой информации (анкетирование, интервьюирование)	15
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 уровня защищенности:

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

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

ВНИМАНИЕ!
16 сентября 2014 года с 11.00 до 12.00 состоится вебинар
«Обзор современных технологий и продуктов для защиты от инсайдеров»
Регистрация на сайте www.dialognauka.ru