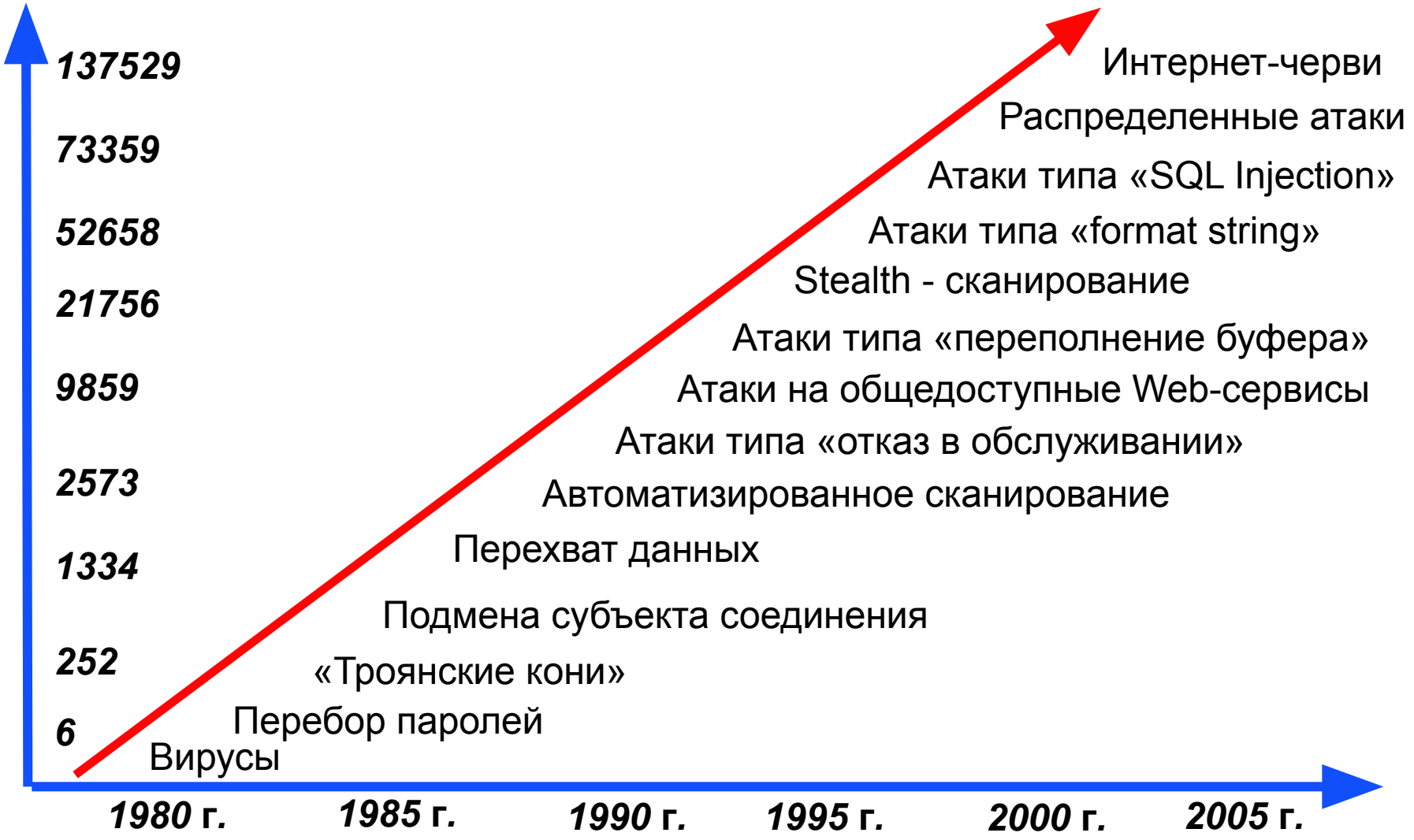
Система управления информационной безопасности

Виктор Сердюк, к.т.н.
Генеральный директор ЗАО «ДиалогНаука»

01 февраля 2008 года

ДиалогНаука

Рост количества атак



Причина неэффективности применяемых мер защиты

- В ряде случаев в организациях отсутствуют нормативно-методические документы, формализующие процесс обеспечения информационной безопасности
- Персонал компании зачастую не осведомлён о возможных угрозах, вследствие чего допускаются непреднамеренные ошибки, приводящие вирусным атакам
- В компаниях отсутствует полноценная система защиты информации
- **Информационная безопасность воспринимается как проект, подразумевающий разовое выполнение задач по защите данных**

Система Управления Информационной Безопасностью

СУИБ – это документированная системы управления, определённая в рамках компании, которая включает в себя

- Утвержденную руководством политику информационной безопасности
  - Определяет понятие информационной безопасности, цели и задачи СУИБ, приверженность руководства и т.д.
- План по оценке рисков безопасности
  - Описывает порядок оценки и анализа рисков безопасности
- Перечень информационных активов, подпадающие в области действия СУИБ
- Положение о применимости контролей (Statement of Applicability)
  - определяет набор контрмер, направленных на минимизацию рисков информационной безопасности
- Исчерпывающий набор взаимоувязанных процедур, подполитик, регламентов и инструкций, направленных на формализацию процессов защиты информации

СУИБ предназначена для:

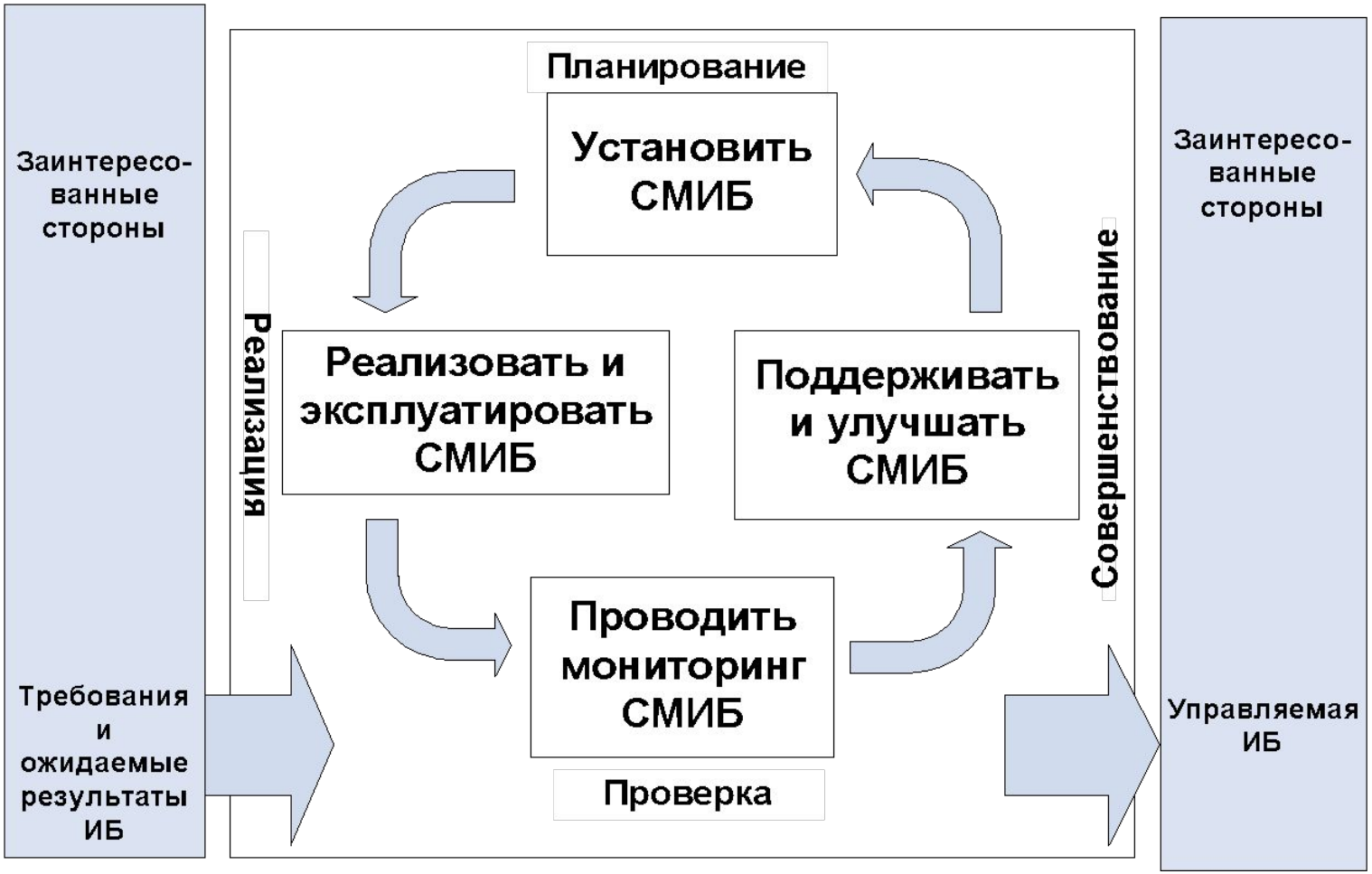
- Успешного руководства обеспечением ИБ, организуя её функционирование систематически и прозрачным способом
- Постоянного улучшения деятельности в области обеспечения ИБ с учётом потребностей всех заинтересованных сторон
- Получения уверенности в том, что заданные требования к ИБ будут выполнены
- Формирования единых подходов к оценке достигнутого уровня ИБ

Международный стандарт ISO/IEC 27001

История формирования стандарта

- BS 7799 Часть 1 опубликована – февраль 1995
- BS 7799 Часть 2 опубликована – февраль 1998
- BS 7799:1999 Часть 1 и Часть 2 опубликованы – апрель 1999
- ISO 17799 Часть 1 опубликована – декабрь 2000
- BS 7799:2002 Часть 2 опубликована – сентябрь 2002
- ISO 17799:2005 опубликован – июнь 2005
- ISO 27001:2005 опубликован – октябрь 2005

Процесс реализации СУИБ



ДиалогНаука

Планирование

- Определение области действия проекта (scope)
- Идентификация информационных активов
- Оценка и анализ рисков информационной безопасности
- Принятие высшим руководством остаточных рисков
- Разработка Политики информационной безопасности организации
- Определение защитных мер контроля и их обоснование для минимизации рисков

Реализация

- Реализация плана обработки рисков ИБ и внедрение защитных мер
- Определение ключевых показателей эффективности для выбранных защитных мер
- Управление работами и ресурсами, связанными с реализацией СМИБ
- Реализация программ по обучению и осведомленности ИБ

Проверка

- Мониторинг и контроль защитных мер, включая регистрацию действий и событий, связанных с СУИБ
- Анализ эффективности СУИБ, включая анализ уровней остаточного риска ИБ и приемлемого риска при изменениях
- Внутренний аудит СУИБ
- Анализ СУИБ со стороны высшего руководства
- Внешний аудит СУИБ

Действие

- Реализация тактических улучшений СУИБ
- Реализация стратегических улучшений СУИБ
- Информирование об изменениях и их согласование с заинтересованными сторонами
- Оценка достижения поставленных целей и потребностей в развитии СУИБ

Определение рамок проекта

- Область действия (scope) должна 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

Идентификация активов

- Информационные ресурсы, которые обеспечивают выполнение бизнес-процессов, заданных рамками проекта
- Прикладное и общесистемное программное обеспечение
- Аппаратное обеспечение
- Телекоммуникационное обеспечение
- Персонал

Классификация информационных ресурсов

- открытая информация
- открытая информация ограниченного распространения (для внутреннего использования)
- конфиденциальная информация
- строго конфиденциальная информация

Оценка рисков безопасности

- Методика базируется на лучших мировых практиках NIST-800, OCTAVE и др.
- Выполняется адаптация методики исходя из специфики организации Заказчика
- Методика предполагает разработку модели угроз для информационных активов, определенных в рамках проекта
- Может осуществляться на основе количественных и качественных шкал оценки рисков

Качественная оценка рисков

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

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

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)
- Рекомендации международных стандартов (ISO 13335, OCTAVE)
- Рекомендации компаний-производителей программного и аппаратного обеспечения (Microsoft, Oracle, Cisco и т. д.)

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

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 средств:

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

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

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 инструменталь-ных средств для сбора информации

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

Состав исходных данных

- Информация об организации Заказчика
- Организационно-распорядительная документация по вопросам информационной безопасности
- Информация об аппаратном, общесистемном и прикладном обеспечении хостов
- Информация о топологии автоматизированной системы Заказчика
- Схема информационных потоков внутри компании

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

Что такое контроли (Control)?

1. Меры контроля (Control) – это мера по минимизации риска
2. Меры контроля позволяют снизить риск, но не устранить его полностью
3. Стоимость внедрения меры контроля должна быть меньше величины ущерба
4. Каждый актив может быть подвержен различным рискам
5. Каждому риску должна быть сопоставлена мера контроля
6. Некоторые меры контроля влияют на несколько различных рисков
7. Меры контроля должны быть комплексными

Разработка Положения о применимости контролей

Положение о применимости контролей (Statement of Applicability) описывает совокупность контролей, которая должна быть внедрена в компании для обеспечения минимизации рисков до приемлемого остаточного уровня

Положение базируется на контролях, описанных в ISO 17799, но может включать в себя дополнительные меры, необходимые для повышения уровня информационной безопасности

Нормативно-правовое обеспечение информационной безопасности

Основные разделы Политики

- Цели и задачи Политики безопасности
- Законодательная и нормативная основа обеспечения информационной безопасности
- Модель угроз информационной безопасности
- Требования к комплексной системе защиты организации
- Организационные меры защиты информации
- Технологические меры защиты информации
- План краткосрочных и долгосрочных мер по реализации Политики безопасности

Особенности создания Политики

- учитывается **текущее состояние** и **ближайшие перспективы** развития АС
- учитываются цели, задачи и правовые основы создания и эксплуатации АС
- учитываются режимы функционирования данной системы
- производится **анализ рисков информационной безопасности** для ресурсов АС Компании

Частные политики ИБ

- Политика предоставления доступа к информационным ресурсам
- Политика обеспечения безопасности коммуникаций
- Политика обеспечения безопасности приложений
- Политика выбора технических средств
- Политика антивирусной защиты
- Политика обеспечения физической безопасности средств информатизации и защиты информации
- Политика взаимодействия с организациями-подрядчиками

Регламенты в области ИБ

- Регламент резервного копирования информации
- Регламент расследования инцидентов в области информационной безопасности
- Регламент проведения аудита информационной безопасности
- Регламент управления документами в области ИБ

Инструкции по безопасности

- Инструкция администратору безопасности
- Инструкция пользователю по обеспечению информационной безопасности

Система контроля версий

- правила оформления титульного листа
- систему нумерации документов и их версий в рамках единого классификатора
- специальные поля для учета изменений, внесенных в текст документа
- правила авторизации изменений, вносимых в нормативные документы

Внедрение разработанных документов

- Обучение администраторов безопасности, ответственных за установку и обслуживание средств защиты
- Обучение пользователей, работающих со средствами защиты
- Аттестация специалистов по результатам программы обучения
- Укомплектование подразделений предприятия сотрудниками, ответственными за выполнение работ по защите от угроз безопасности

Разработка и внедрение СУИБ

1.	**Обследование компании**
1.1.	Выбор области действия системы управления информационной безопасностью
1.2.	Идентификация информационных активов в рамках области действия СУИБ
1.3.	Сбор и анализ информации о применяемых в компании средствах и методах защиты
2.	**Оценка и анализ рисков информационной безопасности компании**
2.1.	Разработка и согласование методики анализа рисков безопасности
2.2.	Проведение оценки рисков безопасности
2.3.	Разработка рекомендаций по совершенствованию нормативно-методического и технологического обеспечения, направленного на минимизацию рисков информационной безопасности

Разработка и внедрение СУИБ

3.	**Разработка проекта по внедрению системы управления информационной безопасностью**
3.1.	Разработка/корректировка политики информационной безопасности компании
3.2.	Разработка/корректировка политик и процедур СУИБ
3.3.	Разработка технического проекта по реализации комплексной системы защиты информации компании
4.	**Внедрение системы управления информационной безопасностью**
4.1.	Обучение сотрудников компании в соответствии с разработанными документами (пп. 3.1, 3.2)
4.2.	Установка/настройка средств защиты информации в соответствии с техническим проектом (п. 3.3)

Разработка и внедрение СУИБ

5.	**Общий аудит по окончанию работ**
5.1.	Контрольный аудит
5.2.	Корректировка и устранение недостатков
6.	**Подготовительные работы к проведению сертификации на соответствие ISO 27001**
6.1.	Оформление необходимых документов
6.2.	Подача заявки в представительство BSI

Спасибо за внимание!

ЗАО «ДиалогНаука»
Тел.: (495) 980-67-76
Факс: (495) 980-67-75

vas@DialogNauka.ru
www.DialogNauka.ru

ДиалогНаука