«Безопасность информационных систем и средств коммуникаций»

Принципы построения системы информационной безопасности

Борисов Алексей Викторович

2011

Краткое содержание

- Понятия информационной безопасности: что, зачем, от чего и как защищать?
- Система ИБ: основные функции, этапы и принципы потроения
- Комплексное обследование ИС
- Определение требований к защите
- Моделирование угроз
- Что такое «аудит ИБ»?
- Оценка информационных рисков
- Что такое «политика ИБ»?

Понятия информационной безопасности

ЧТО ТАКОЕ БЕЗОПАСНОСТЬ?

Безопасность – состояние защищенности активов от потенциально или реально существующих угроз, или отсутствие таких угроз

Активы - все, что имеет ценность для владельца

Угроза – возможная опасность совершения какого-либо деяния, наносящего ущерб

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ ИНФОРМАЦИЯ?

«Информация - сведения (сообщения, данные), независимо от формы их представления.»

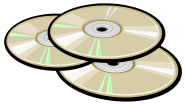
Федеральный закон от 27 июля 2006 г. № 149-ФЗ
«Об информации, информационных технологиях
и защите информации»

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ ИНФОРМАЦИЯ?

- Информация идеальна, т.к. ее значение не зависит от формы представления
- Представленная в конкретной форме информация является материальной ценностью, которую можно купить, продать, подарить, уничтожить, украсть и т.д.

Понятия информационной безопасности: что защищать?



ИНФОРМАЦИЯ

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ ОБЪЕКТ ИНФОРМАТИЗАЦИИ?

«Объект информатизации - совокупность

- *информационных ресурсов,*
- *средств и систем обработки информации, используемых в соответствии с заданной информационной технологией,*
- *средств обеспечения объекта информатизации,*
- *помещений или объектов (зданий, сооружений, технических средств), в которых они установлены,*

или помещения и объекты, предназначенные для ведения конфиденциальных переговоров»

ГОСТ Р 51275-99

Понятия информационной безопасности: что защищать?

ЧТО ТАКОЕ АВТОМАТИЗАИРОВАННАЯ СИСТЕМА?

«Автоматизированная система – система, состоящая из

- *персонала*
- *комплекса средств автоматизации его деятельности,*

реализующая информационную технологию выполнения установленных функций»

ГОСТ 34.003-90

Понятия информационной безопасности: что защищать?

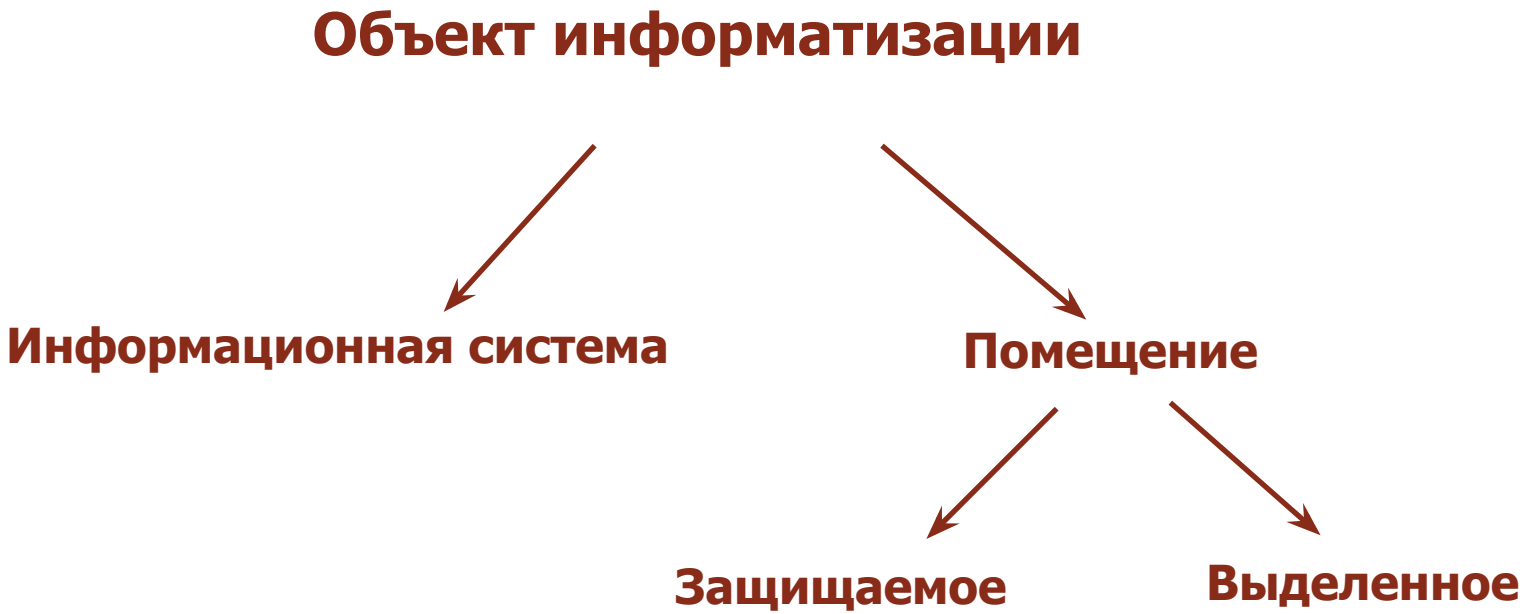
ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ СИСТЕМА?

«Информационная система – совокупность

- *содержащейся в базах данных информации*
- *обеспечивающих ее обработку информационных технологий и технических средств»*

Федеральный закон от 27 июля 2006 г. № 149-ФЗ
«Об информации, информационных технологиях
и защите информации»

Понятия информационной безопасности: что защищать?



Понятия информационной безопасности: что защищать?

ТАК ЧТО ЖЕ ЗАЩИЩАТЬ?

Объект информатизации (ИС, помещения)?

Информацию?

Владельца информации?

Понятия информационной безопасности: что защищать?

«Информация - это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищён надлежащим образом»

ГОСТ Р ИСО/МЭК 17799-2005

Понятия информационной безопасности: что защищать?

- Защищать следует то, что представляет собой ценность!
- Объектом защиты является информация, но только та, которая представлена в конкретной форме, циркулирует в конкретной среде – на объекте информатизации!

Понятия информационной безопасности: что защищать?

Основная цель защиты: исключение нанесения ущерба

Что такое ущерб?

- невыгодные последствия

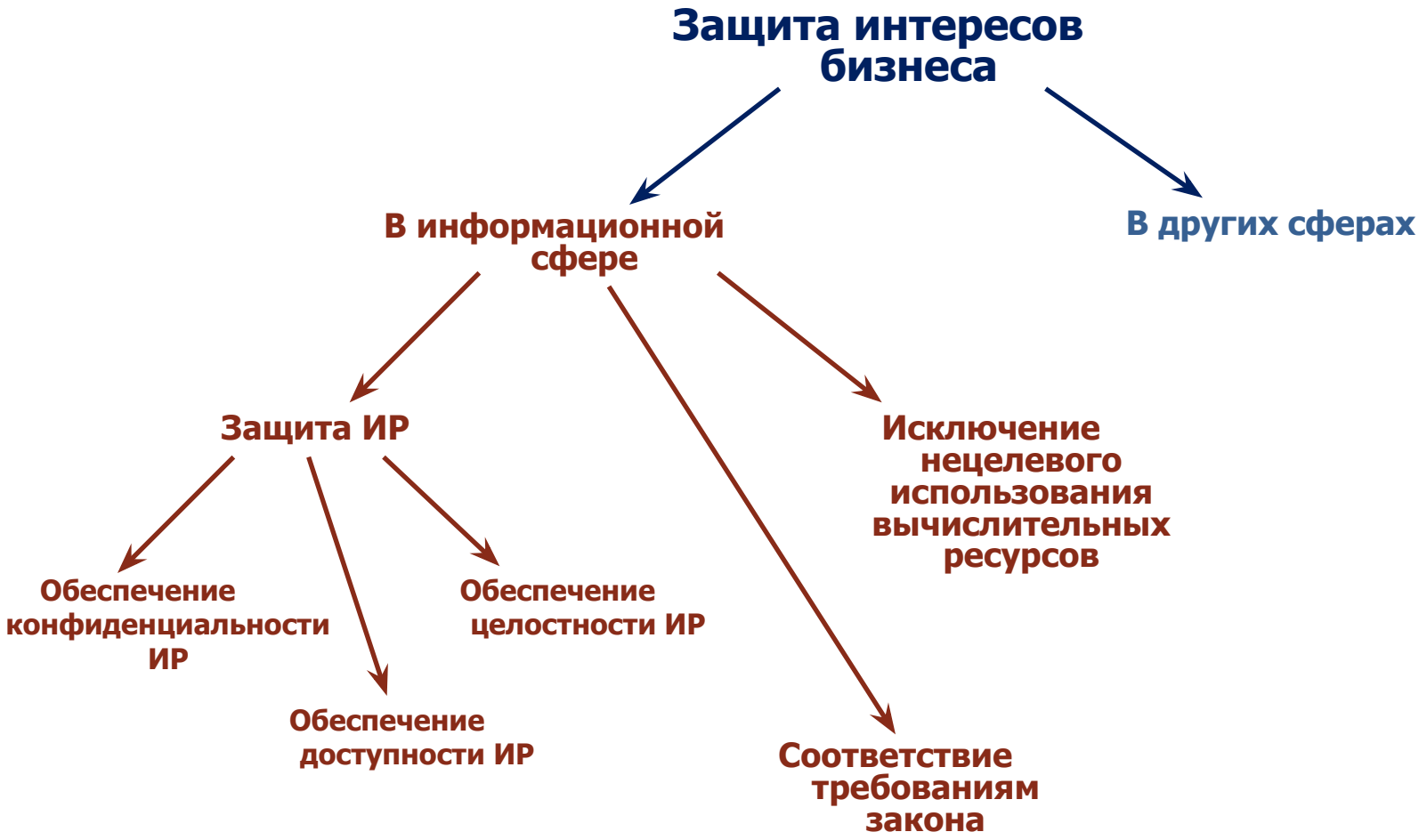
Каким может быть ущерб?

- простои производства
- повторный ввод информации
- судебные издержки
- отзыв лицензии, приостановление деятельности
- отток клиентов
- обгон конкурентами
- потеря репутации
- ухудшение психологического климата в коллективе
- нецелевое использование вычислительных ресурсов

Понятия информационной безопасности: что защищать?

Задачи информационной безопасности являются подмножеством задач защиты бизнеса (экономической безопасности)

Понятия информационной безопасности: что защищать?



Понятия информационной безопасности: от чего защищать?

КАКИЕ УГРОЗЫ МОГУТ БЫТЬ АКТУАЛЬНЫ ДЛЯ ИНФОРМАЦИИ

для информации актуальны те угрозы, которые могут нарушить ее свойства безопасности

Понятия информационной безопасности: от чего защищать?

СВОЙСТВА (АСПЕКТЫ) БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- ✔ **Конфиденциальность**
- ✔ **Целостность**
- ✔ **Доступность**

Понятия информационной безопасности: от чего защищать?

ЧТО ТАКОЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ?

свойство информации быть доступной только ограниченному кругу пользователей ИС, в которой циркулирует данная информация

Понятия информационной безопасности: от чего защищать?

ЧТО ТАКОЕ ЦЕЛОСТНОСТЬ ИНФОРМАЦИИ?

свойство информации сохранять свою структуру

и содержание

Понятия информационной безопасности: от чего защищать?

ЧТО ТАКОЕ ДОСТУПНОСТЬ ИНФОРМАЦИИ?

свойство информации быть доступной для пользователей ИС

Понятия информационной безопасности: от чего защищать?

Нарушение конфиденциальности:

- **хищение**
- **ознакомление**
- **копирование**

Нарушение целостности:

- **модификация**

Нарушение доступности:

- **блокирование**
- **уничтожение**

Понятия информационной безопасности

ЧТО ТАКОЕ БЕЗОПАСНОСТЬ ИНФОРМАЦИИ?

«Безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз»

РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Термины и определения»

Понятия информационной безопасности

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ?

«Информационная безопасность - свойство информации сохранять конфиденциальность, целостность, доступность»

ГОСТ Р ИСО/МЭК 27001-2006

Понятия информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства

- *соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны*
- *информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации...*
- *развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи...*
- *защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем...*

Доктрина информационной безопасности Российской Федерации

Понятия информационной безопасности

ЧТО ТАКОЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ?

состояние защищенности интересов организации в информационной сфере

Понятия информационной безопасности

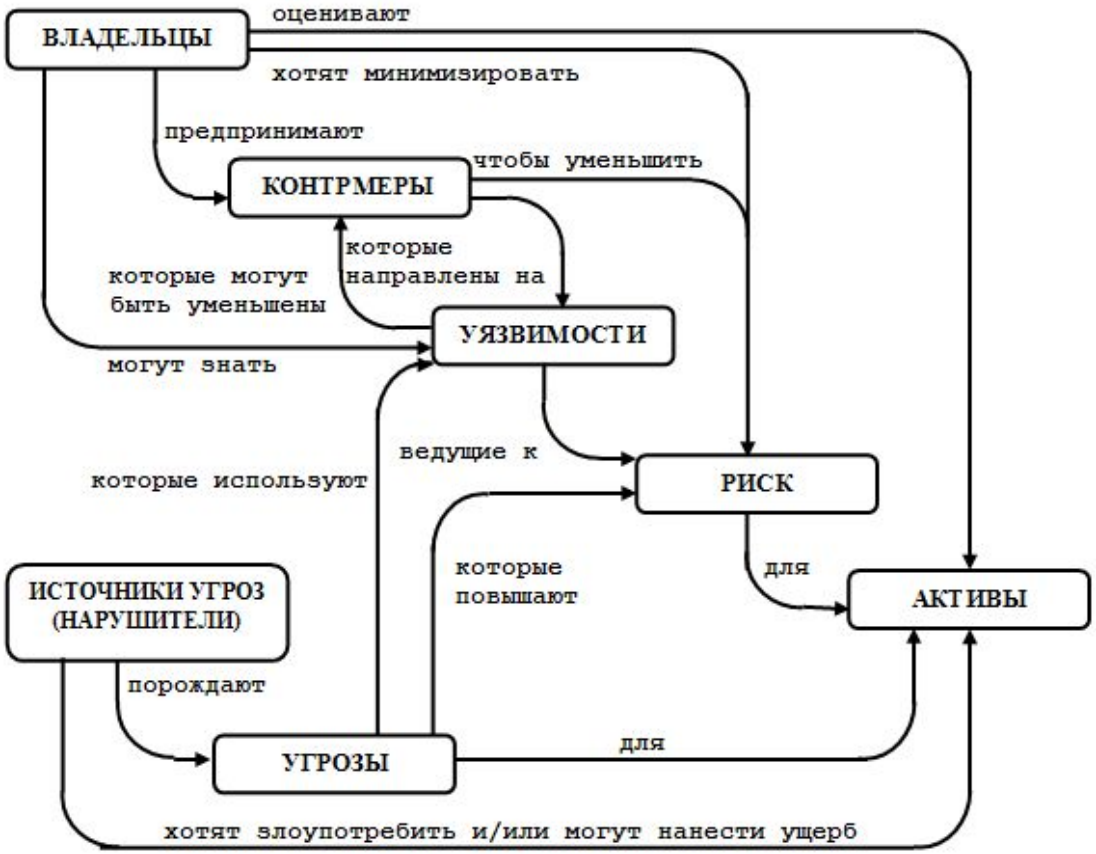
ЧТО ТАКОЕ ЗАЩИТА ИНФОРМАЦИИ?

«Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) *обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;*
2) *соблюдение конфиденциальности информации ограниченного доступа,*
3) *реализацию права на доступ к информации.»*

Федеральный закон от 27 июля 2006 г. № 149-ФЗ
«Об информации, информационных технологиях
и защите информации»

Понятия информационной безопасности



ГОСТ Р ИСО/МЭК 15408-1-2002

Понятия информационной безопасности: как защищать?

МЕРЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

- ✔ Технические
- ✔ Правовые
- ✔ Организационные
- ✔ Физические
- ✔ Морально-этические

Понятия информационной безопасности: как защищать?

ТЕХНИЧЕСКИЕ МЕРЫ

основаны на использовании различных программных и/или аппаратных средств, входящих в состав ИС и предназначенных самостоятельно или в комплексе с другими средствами выполнять функции защиты

Понятия информационной безопасности: как защищать?

ПРАВОВЫЕ МЕРЫ

действующие в государстве нормативные правовые акты (законы, указы, постановления и др.), регламентирующие правила обращения с информацией, а также устанавливающие ответственность за нарушения этих правил

Понятия информационной безопасности: как защищать?

ОРГАНИЗАЦИОННЫЕ МЕРЫ

меры административного и процедурного характера, регламентирующие процессы функционирования ИС, использования ИР, затрудняющие реализацию угроз безопасности информации

Понятия информационной безопасности: как защищать?

ФИЗИЧЕСКИЕ МЕРЫ

основаны на применении устройств и сооружений, предназначенных для создания физических препятствий для доступа к ИС

Понятия информационной безопасности: как защищать?

МОРАЛЬНО-ЭТИЧЕСКИЕ МЕРЫ

нормы поведения, традиционно сложившиеся или складывающиеся по мере распространения информационных технологий в обществе. Данные нормы не являются обязательными, однако их несоблюдение приводит к падению авторитета человека или организации (работы по укреплению морального климата в организации)

Понятия информационной безопасности: как защищать?

ПОДХОДЫ К ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ

Фрагментарный – направлен на противодействие четко определенным угрозам в заданных условиях.

Комплексный – ориентирован на создание защищенной среды обработки информации, объединяющий в единый комплекс разнородные меры противодействия всем угрозам. Основан на построении системы обеспечения безопасности информации.

Понятия информационной безопасности: как защищать?

ФРАГМЕНТАРНЫЙ ПОДХОД

Достоинства

- высокая избирательность к конкретным угрозам
- относительно низкая стоимость реализации

Недостатки

- отсутствие полного анализа всех угроз
- отсутствие единой защищенной среды обработки информации

Понятия информационной безопасности: как защищать?

КОМПЛЕКСНЫЙ ПОДХОД

Достоинства

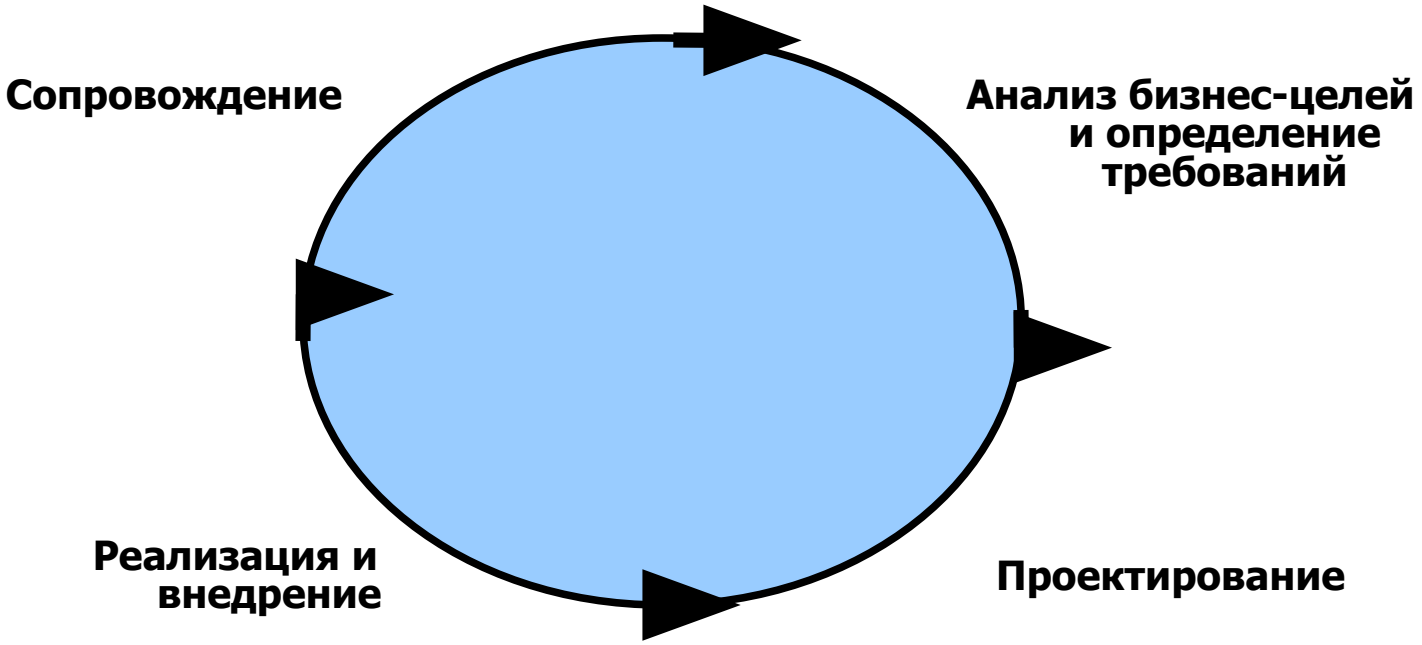
- позволяет гарантировать определенный уровень защиты

Недостатки

- сложность управления
- высокая стоимость реализации

Система информационной безопасности

ЦИКЛИЧНОСТЬ ПРОЦЕССА ОБЕСПЕЧЕИЯ БЕЗОПАСНОСТИ



Система информационной безопасности

МОДЕЛЬ ЗАЩИЩЕННОЙ СРЕДЫ ОБРАБОТКИ ИНФОРМАЦИИ

- ✔ Доверенные окружение и субъекты
- ✔ Доверенная аппаратная платформа
- ✔ Доверенная программная платформа
- ✔ Доверенные каналы передачи информации
- ✔ Доверенные правила

Система информационной безопасности

ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- ✔ Счетность всех субъектов и объектов
- ✔ Доверенная конфигурация и настройки
- ✔ Целостность всех элементов
- ✔ Подконтрольность всех действий
- ✔ Документированность всех событий

Система информационной безопасности

Основные задачи СИБ

- ✔ Защита ИР от НСД и утечек
- ✔ Контроль подлинности и целостности информации
- ✔ Обеспечение юридической значимости информации
- ✔ Аудит и мониторинг безопасности системы
- ✔ Построение доверенных каналов
- ✔ Безопасное подключение ИС к открытым сетям
- ✔ Обнаружение вторжений и антивирусная защита
- ✔ Управление безопасностью

Система информационной безопасности

Основные принципы построения СИБ

- ✔ Системность
- ✔ Комплексность
- ✔ Многоуровневость
- ✔ Интегрируемость
- ✔ Разумная достаточность

Система информационной безопасности

СИСТЕМНОСТЬ

Реализуется полный комплекс этапов по созданию СИБ:

- анализ состояния и определение требований,
- проектирование,
- реализация,
- оценка эффективности

Система информационной безопасности

КОМПЛЕКСНОСТЬ

Для обеспечения безопасности используется комплекс мер, который включает в себя:

- технические меры
- правовые меры
- организационные меры
- физические меры

Система информационной безопасности

МНОГОУРОВНЕВОСТЬ

Безопасность информации обеспечивается с помощью нескольких последовательных рубежей защиты

Система информационной безопасности

ИНТЕГРИРУЕМОСТЬ

СОБИ строится на основе существующей IT-инфраструктуры с использованием встроенных средств защиты информации

Система информационной безопасности

РАЗУМНАЯ ДОСТАТОЧНОСТЬ

При определении перечня мероприятий по обеспечению безопасности информации необходимо учитывать возможный ущерб от реализации угроз и соотносить его с совокупной стоимостью защиты

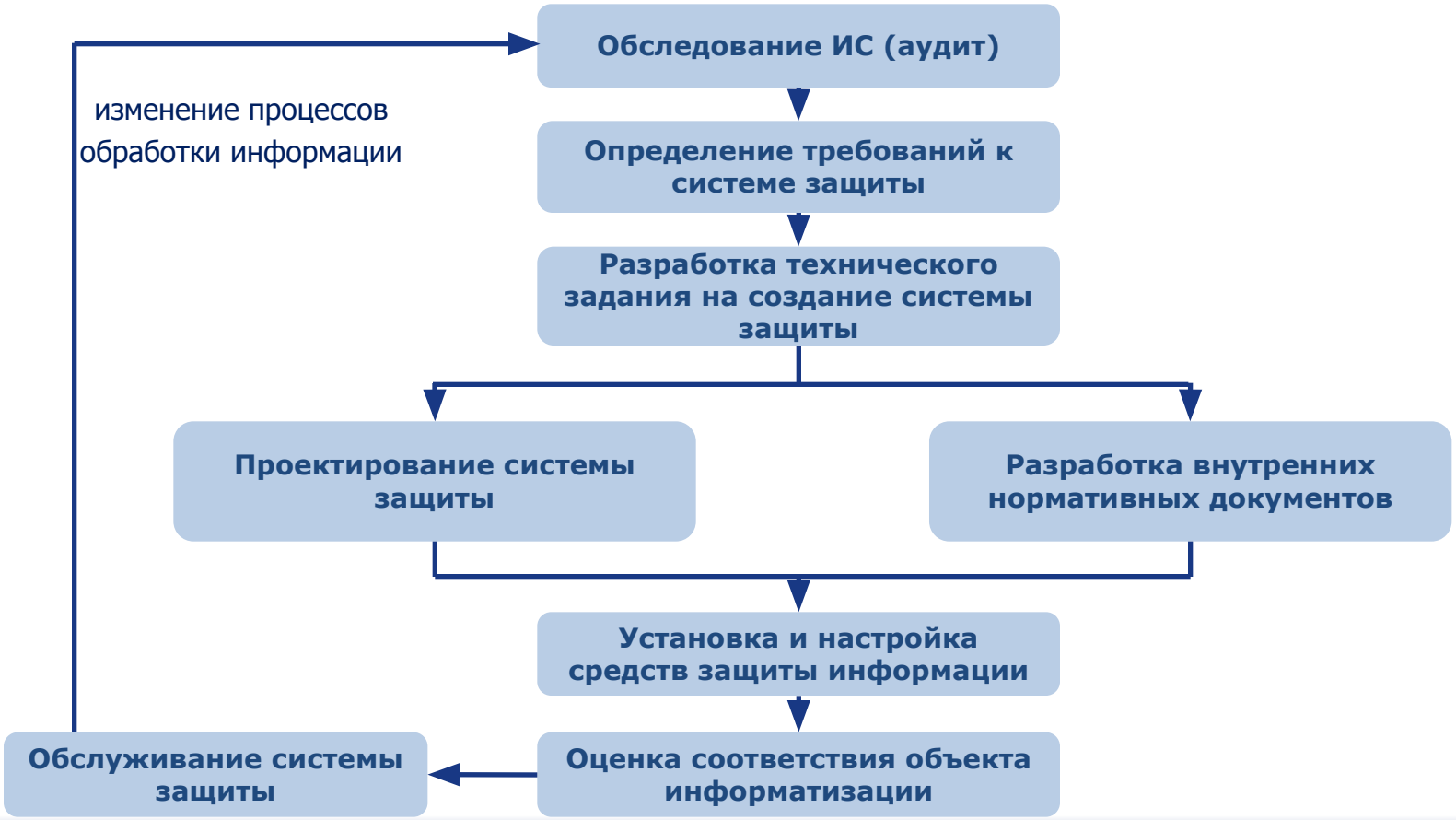
Система информационной безопасности

Этапы построения СИБ

- ✔ Комплексное обследование ИС
- ✔ Моделирование и анализ угроз безопасности информации
- ✔ Определение требований к защите
- ✔ Проектирование системы защиты информации
- ✔ Разработка организационно-распорядительной и эксплуатационной документации
- ✔ Внедрение системы защиты информации
- ✔ Оценка соответствия требованиям
- ✔ Сопровождение и корректировка

Система информационной безопасности

Этапы построения СИБ



Построение СИБ: комплексное обследование ИС

На этапе **комплексного обеследования** ИС собирают данные о всех значимых (с точки зрения безопасности информации) особенностях функционирования ИС для последующего анализа

Какие данные собирают?

- ✔ Данные о составе и принципах работы ИС
- ✔ Данные о ролях пользователей, работающих с ИС
- ✔ Данные о потоках и процессах обработки информации

Источники исходных данных:

- ✔ Интервьюирование пользователей ИС
- ✔ Организационно-распорядительные и эксплуатационные документы
- ✔ Сканирование ИС с использованием специализированного ПО

Построение СИБ: моделирование и анализ угроз

На этапе **моделирования и анализа угроз** моделируются возможные угрозы, а также определяется их актуальность для последующего формирование требований к защите

Для моделирования угроз используются исходные данные, полученные на этапе комплексного обследования

Построение СИБ: моделирование и анализ угроз

Как моделировать угрозы?

Угрозу можно представить как совокупность следующих элементов:

- источник угрозы,
- уязвимость ИС,
- способ реализации угрозы,
- объект воздействия (ИР),
- деструктивное действие.

Источник,
используя уязвимость системы
и применяя какой-либо способ реализации угрозы,
совершает деструктивное действие
над защищаемой информацией

Построение СИБ: определение требований к защите

На этапе **определения требований** формируются требования к защите, которым должна удовлетворять СОБИ

Источники формирования требований к защите:

- смоделированные угрозы безопасности информации
- требования нормативных правовых актов Российской Федерации
- требования методических документов ФСТЭК России и ФСБ России
- требования международных, государственных и отраслевых стандартов
- требования, включенные в договора с партнерами и контрагентами

Построение СИБ: определение требований к защите

Классификация защищаемых информационных ресурсов

<table>
<tr><td rowspan="6">Информационные ресурсы, подлежащие защите</td><td rowspan="5">с ограниченным доступом</td><td rowspan="3">содержащие сведения, составляющие государственную тайну</td><td colspan="2">секретные</td></tr>
<tr><td colspan="2">совершенно секретные</td></tr>
<tr><td colspan="2">особой важности</td></tr>
<tr><td rowspan="4">содержащие конфиденциальные сведения</td><td rowspan="2">защищаемые по закону</td><td>персональные данные</td></tr>
<tr><td>профессиональная тайна</td></tr>
<tr><td>служебная тайна</td><td rowspan="2">защищаемые по решению собственника</td></tr>
<tr><td>коммерческая тайна</td></tr>
<tr><td>общедоступные</td><td colspan="3">содержащие сведения, неправомерное обращение с которыми может нанести ущерб окружающей среде, гражданам и обществу</td></tr>
<tr><td colspan="4">представляющие коммерческую ценность</td></tr>
</table>

Построение СИБ: определение требований к защите

Классификация защищаемых информационных ресурсов

Государственная тайна

«защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации»

Закон Российской Федерации от 21 июля 1993 г. № 5485-1
«О государственной тайне»

Построение СИБ: определение требований к защите

Классификация защищаемых информационных ресурсов

Персональные данные

«любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация»

Федеральный закон от 27 июля 2006 г. № 152-ФЗ
«О персональных данных»

Построение СИБ: определение требований к защите

Классификация защищаемых информационных ресурсов

Профессиональная тайна

«сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.)»

Указ Президента РФ от 06 марта 1997 г. № 188
«Об утверждении перечня сведений конфиденциального характера»

Построение СИБ: определение требований к защите

Классификация защищаемых информационных ресурсов

Служебная тайна

«Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом и федеральными законами»

Указ Президента РФ от 06 марта 1997 г. № 188

«К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью»

Постановление Правительства РФ
от 03 ноября 1994 г. № 1233

Построение СИБ: определение требований к защите

Классификация защищаемых информационных ресурсов

Коммерческая тайна

«сведения любого характера, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны»

Федеральный закон от 29 июля 2004 г. № 98-ФЗ

«О коммерческой тайне»

Построение СИБ: проектирование системы защиты информации

На этапе **проектирования системы защиты информации** формируются технические решения и разрабатывается проектная документация с описанием таких решений

Технические решения должны удовлетворять сформулированным требованиям

Построение СИБ: разработка ОРД

На этапе **разработки организационно-распорядительной и эксплуатационной документации** фиксируются и документируются правила, которые должны соблюдаться при обработке информации и использовании вычислительных ресурсов

Правила должны быть утверждены руководством организации

Совокупность таких правил составляет **политику обеспечения безопасности информации**

Построение СИБ: оценка соответствия требованиям

Оценка соответствия требованиям обеспечения безопасности информации является комплексом контрольных мероприятий

Контрольные мероприятия могут проводиться в различной форме

В некоторых случаях форма контрольных мероприятий регламентируется требованиями нормативных правовых актов

Аудит безопасности информации

ЧТО ТАКОЕ АУДИТ БЕЗОПАСНОСТИ ИНФОРМАЦИИ?

процесс

сбора, анализа, оценки

данных о текущем состоянии обеспечения безопасности информации в обследуемой ИС

на соответствие определенным критериям

Аудит безопасности информации

ЧТО ДЕЛАЮТ ПРИ АУДИТЕ?

- ✔ Собрают, оценивают и анализируют информацию об ИС
- ✔ Оценивают возможные последствия нарушения безопасности
- ✔ Выбирают уровень (класс) защищенности
- ✔ Сравнивают реальное и требуемое
- ✔ Документально фиксируют результаты сравнения

Аудит безопасности информации

КОГДА МОЖЕТ ПРОВОДИТЬСЯ АУДИТ?

- ✔ При создании (проектировании) новой ИС
- ✔ При модернизации ИС
- ✔ При оценке соответствия (аттестация)
- ✔ При штатной эксплуатации ИС(контрольный аудит)

Аудит безопасности информации

ВНУТРЕННИЙ АУДИТ

Проводится штатными сотрудниками Организации

Достоинства:

- лучшая осведомленность об особенностях работы ИС и процессах Организации
- получение необходимой информации с минимальными затратами
- результаты остаются внутри Организации

Недостатки:

- отсутствие у проверяющих обширной базы знаний
- недостаток времени
- недостаток квалификации
- необходимость дополнительного обучения персонала организации

Аудит безопасности информации

ВНЕШНИЙ АУДИТ

Проводится сотрудниками сторонней специализированной организации

Достоинства:

- Независимость экспертов
- Наличие специалистов необходимой квалификации
- Наличие отработанных методик проведения аудита
- Наличие опыта и обширной базы знаний

Недостатки:

- Единовременные затраты

Оценка информационных рисков

ЧТО ТАКОЕ РИСК?

«Риск — комбинация вероятности события и его последствий»

ISO/IEC 17799-2005

Информационные риски рассчитывают

- для оценки эффективности защитных мер
- для обоснования расходов на защитные меры
- для определения значимости угроз
- для ранжирования угроз по значимости

Оценка информационных рисков

КАКИМ МОЖЕТ БЫТЬ УЩЕРБ?

- простои производства
- повторный ввод информации
- судебные издержки
- штраф
- отзыв лицензии
- приостановление деятельности
- отток клиентов
- обгон конкурентами
- снижение (потеря) репутации
- ухудшение психологического климата

Оценка информационных рисков

КОЛИЧЕСТВЕННЫЙ АНАЛИЗ

$$R = P \times I$$

P – вероятность реализации угрозы

I – величина возможного ущерба от реализации угрозы

Риск является экономическим показателем и измеряется в деньгах

Оценка информационных рисков

КОЛИЧЕСТВЕННЫЙ АНАЛИЗ

Для количественной оценки риска необходимо:

- оценить вероятность реализации угрозы
- оценить возможные потери в деньгах

Оценка информационных рисков

КОЛИЧЕСТВЕННЫЙ АНАЛИЗ

Почему сложно сделать количественную оценку риска?

Сложно посчитать вероятность реализации угрозы: отсутствует статистика

Сложно посчитать возможный ущерб:

- ИР может иметь разную ценность в разное время, при разных обстоятельствах, в разных бизнес-процессах
- потери могут принимать разные формы
- одно событие может быть причиной различных потерь
- объем потерь определяется множеством факторов

Оценка информационных рисков

КАЧЕСТВЕННЫЙ АНАЛИЗ

- Ущерб измеряют безразмерной величиной
- Возможную вероятность и возможный ущерб представляют в виде дискретных рядов возможных значений

При качественном анализе риск становится безразмерной величиной!

Оценка информационных рисков

КАЧЕСТВЕННЫЙ АНАЛИЗ

Пример

Threat Likelihood	Impact		
	Low (10)	***Medium*** (50)	***High*** (100)
High (1.0)	**Low** 10 X 1.0 = 10	**Medium** 50 X 1.0 = 50	**High** 100 X 1.0 = 100
Medium (0.5)	**Low** 10 X 0.5 = 5	**Medium** 50 X 0.5 = 25	**Medium** 100 X 0.5 = 50
Low (0.1)	**Low** 10 X 0.1 = 1	**Low** 50 X 0.1 = 5	**Low** 100 X 0.1 = 10

Risk Scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)[8]

NIST SP 800-30
Risk Management Guide
for Information Technology Systems

Политика информационной безопасности

ЧТО ТАКОЕ ПОЛИТИКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ?

Согласованный пакет внутренних документов, устанавливающих требования и порядок обеспечения безопасности информации, регламентирующих все вопросы организации, управления и контроля безопасности, а также эксплуатации средств защиты информации

Политика информационной безопасности

ЗАЧЕМ НУЖНА ПОЛИТИКА?

Создание единой, целостной и эффективной СОБИ требует усилий от каждого сотрудника

Руководству организации необходимо поставить перед собой и подчиненными цель, а также определить, как необходимо действовать каждому сотруднику для достижения этой цели

Для различных должностных обязанностей такие правила будут различными, но все они направлены на повышение уровня защищенности, и поэтому должны быть логически связаны

Спасибо за внимание!

Борисов Алексей Викторович

+7-904-391-66-07

borisov-aleksey@bk.ru