Тема 1. Основы обеспечения информационной безопасности хозяйствующего субъекта
Занятие 1. Основы и система обеспечения информационной безопасности хозяйствующего субъекта

УЧЕБНЫЕ ВОПРОСЫ:

1. Основы обеспечения информационной безопасности хозяйствующего субъекта
2. Система обеспечения информационной безопасности хозяйствующего субъекта

Литература:

1. А. Ю. Невский, О. Р. Баронов. Система обеспечения информационной безопасности хозяйствующего субъекта : учебное пособие.
2. Ю.А. Родчев. Нормативная база и стандарты в области информационной безопасности. Учебное пособие.
3. Бирюков А.А. Информационная безопасность: защита и наподение.
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
5. ГОСТ Р 51275-99 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
6. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

Современное состояние информационной безопасности

- - больше всего страдает от утечек конфиденциальной информации коммерческий сектор;
- - наблюдается рост масштабов инцидентов в области ИБ;
- - наибольшую опасность для организаций представляют собственные сотрудники компаний.

Что необходимо осознавать руководству ХС в области ИБ

- Во-первых, обеспечение информационной безопасности – это непрерывный процесс, взаимоувязывающий правовые, организационные и программно-аппаратные и прочие меры защиты;
- Во-вторых, в основе этого процесса лежит периодический анализ защищенности информационной системы в соответствии с анализом угроз и динамикой их развития;
- В-третьих, информационная система хозяйствующего субъекта, в своем развитии, должна подвергаться периодическим реорганизациям, отправной точкой каждой из которых служит анализ выявленных уязвимостей при проведении аудита информационной безопасности.

Понятие информационной безопасности ХС

- **Под *информационной безопасностью* хозяйствующего субъекта будем понимать защищенность его информационных ресурсов и поддерживающей их инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации**

- ***Комплексная безопасность*** хозяйствующего субъекта - система взглядов и практических действий, направленных на создание и поддержание таких условий, которые обеспечивают деятельность всего комплекса мер безопасности, направленных на достижение целей его функционирования.
- ***Система комплексной*** *безопасности* включает в себя следующие составляющие подсистемы:

- правовую безопасность;
- кадровую безопасность;
- финансовую безопасность;
- инженерно-техническую безопасность;
- экономическую безопасность;
- ***информационную безопасность***;
- и другие.

- Под ***системой обеспечения информационной безопасности*** (СОИБ) будем понимать функциональную подсистему системы комплексной безопасности хозяйствующего субъекта, объединяющую силы, средства и объекты защиты информации, организованные и функционирующие по правилам, установленным правовыми, организационно-распорядительными и нормативными документами по защите информации

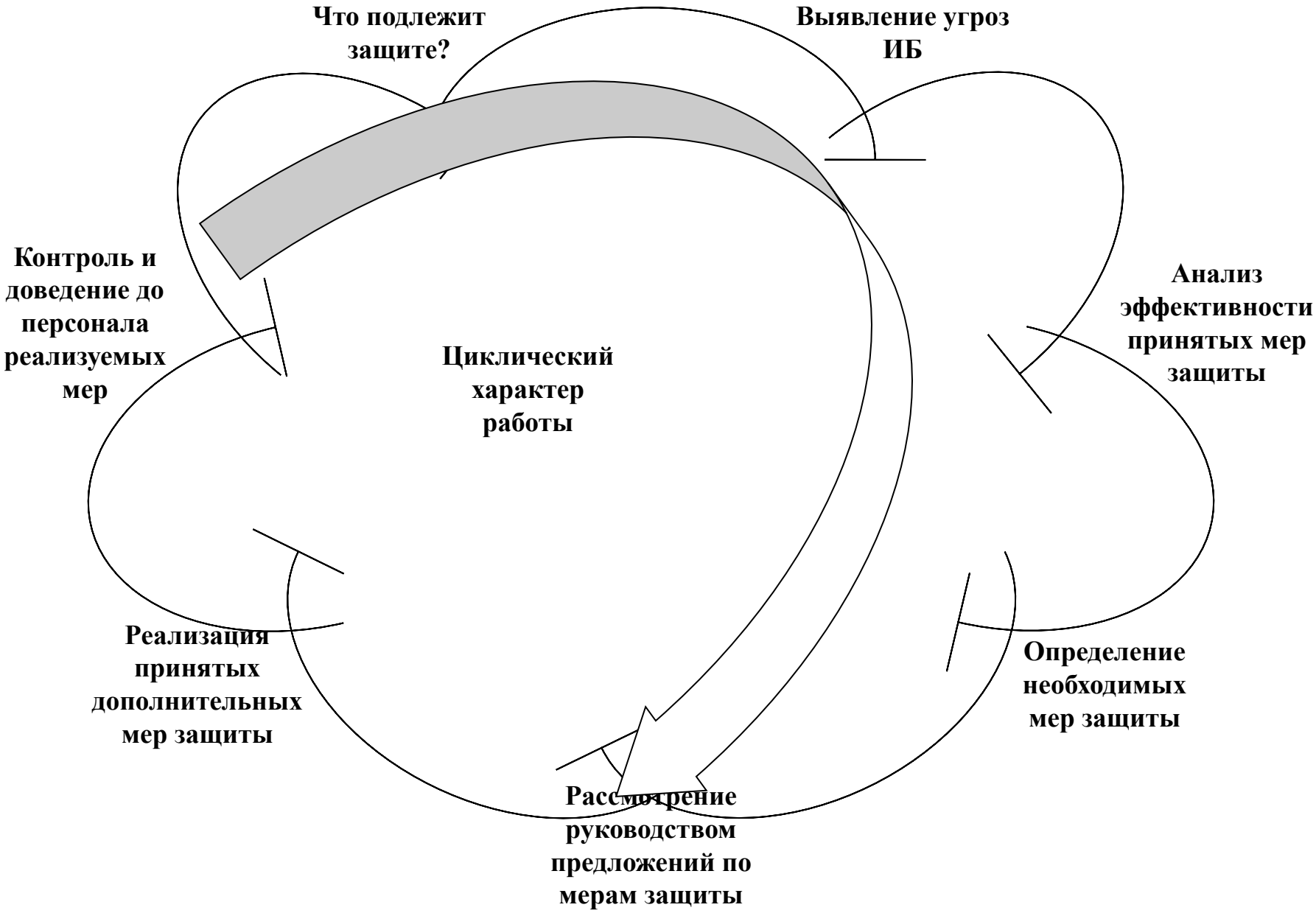
Укрупненная структура СОИБ

- ***Силы СОИБ*** - совокупность органов и (или) исполнителей работ, связанных с защитой информации в интересах данного хозяйствующего субъекта (структурное подразделение, выполняющее задачи управления функционированием данной системы.
- ***Средства защиты информации*** – это совокупность правовых, организационных, технических и других решений, предназначенных для защиты информационных ресурсов хозяйствующего субъекта от внутренних и внешних воздействий.
- ***Объекты защиты информации*** - информационные ресурсы, т.е. любые виды активов информационной системы хозяйствующего субъекта: структурированная и неструктурированная информация, документы, вычислительная техника, коммуникационное и сетевое оборудование, оргтехника и др.

Концепция системного подхода к обеспечению защиты конфиденциальной информации (OPSEC Operation Security)

- Первый этап - (анализ объекта защиты) состоит в определении того, что нужно защищать;
- Второй этап - выявление угроз;
- Третий этап - анализ эффективности принятых и постоянно действующих подсистем безопасности (физическая безопасность документации, надежность персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т.д.);
- Четвертый этап - определение необходимых мер защиты;
- Пятый этап - рассмотрение руководителями фирмы (организации) представленных предложений по всем необходимым мерам безопасности и расчет их стоимости и эффективности;
- Шестой этап - реализация принятых дополнительных мер безопасности с учетом установленных приоритетов;
- Седьмой этап - контроль и доведение до персонала фирмы (организации) реализуемых мер безопасности

Концепция (OPSEC Operation Security)



- ***Конфиденциальность*** информации – это субъективно определяемая для нее характеристика, указывающая на необходимость создания в информационной системе хозяйствующего субъекта условий, при которых вводятся ограничения на доступ к этой информации.
- ***Доступность*** информации – это свойство информационной системы хозяйствующего субъекта, характеризующееся способностью обеспечивать своевременный и беспрепятственный доступ к информации субъектов, имеющих на это полномочия.
- ***Целостность*** информации – это свойство информации, заключающееся в возможности ее существования в информационной системе хозяйствующего субъекта в неискаженном виде.

Цели и задачи СОИБ

- **Целью СОИБ** является создание таких условий функционирования информационной системы хозяйствующего субъекта (ХС), при которых обеспечивается выполнение требований по конфиденциальности, доступности и целостности информации, принадлежащей ему
- **Задачи СОИБ**:

1. Предупреждение появления угроз информационной безопасности
2. Обнаружение появившихся угроз и предупреждение их воздействия на информационную систему хозяйствующего субъекта
3. Обнаружение воздействия угроз на информационную систему хозяйствующего субъекта и локализация этого воздействия
4. Ликвидация последствий воздействия угроз на информационную систему хозяйствующего субъекта

Требования к СОИБ

1. Группа обусловлена **характером информации, циркулирующей в информационной системе ХС:**
- степени конфиденциальности информации;
- объемы информации, циркулирующей в информационной системе;
- интенсивность обработки информации.
2. Группа обусловлена **архитектурой ИС ХС:**
- пространственные размеры информационной системы;
- территориальная распределённость информационной системы;
- структурированность компонентов информационной системы.
3. Группа обусловлена **условиями функционирования ИС ХС:**
- расположение информационной инфраструктуры системы на территории объекта;
- степень обустроенности информационной инфраструктуры;
- развитость информационных коммуникаций.
4. Группа обусловлена **технологией обработки информации в системе:**
- масштабируемость системы;
- стабильность функционирования;
- доступность технологических решений;
- структурированность технологии обработки информации в системе.
5. Группа обусловлена **организацией функционирования ИС ХС:**
- общую организацию функционирования системы;
- степень и качество укомплектованности кадрами;
- уровень подготовки и мотивации кадров;
- уровень производственной (технологической) дисциплины.

Обеспечение функционирования СОИБ

- изучение правовых основ обеспечения ИБ;
- определения перечня источников конфиденциальной информации;
- организация кадровой работы ХС;
- введением в хозяйствующем субъекте комплекса ограничительных (режимных) мероприятий;
- применения комплекса инженерно-технических мер защиты.

Источники конфиденциальной информации

- люди (сотрудники, клиенты, посетители, обслуживающий персонал);
- документы самого различного характера и назначения;
- публикации: доклады, статьи, интервью, проспекты, книги;
- технические средства носителей информации и их обработки;
- выпускаемая ХС продукция;
- производственные и промышленные отходы ХС и другие.

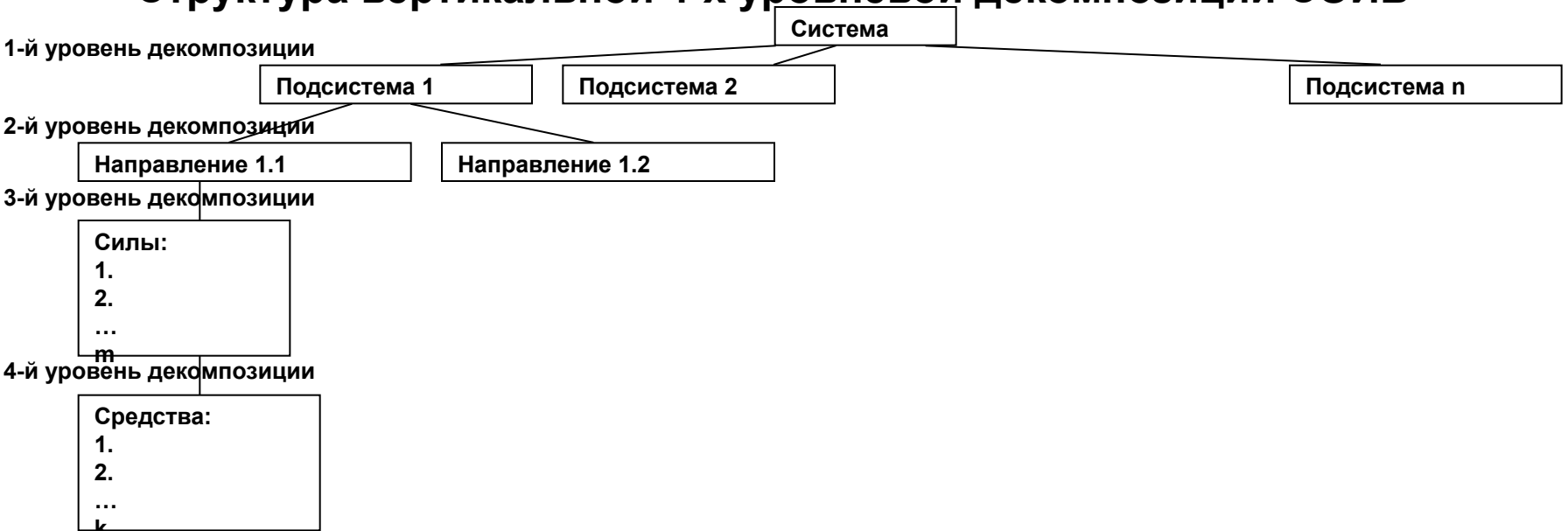
Универсальный перечень режимных мероприятий для обеспечения информационной безопасности бизнеса

- физическая защита сотрудников ХС, являющихся потенциальными носителями конфиденциальной информации;
- постоянный контроль и проверка персонала с целью устранения возможностей для совершения мошенничества, предотвращения возможного сговора между сотрудниками и, например, клиентами ХС;
- ограничение прав доступа сотрудников к информации, которое должно регламентироваться только характером выполняемых ими должностных обязанностей;
- налаженная и постоянно действующая система внутреннего контроля ХС, включающая проведение плановых, внезапных и скрытых контрольных проверок;
- проведение предупредительной активной политики аудита информационной безопасности ХС

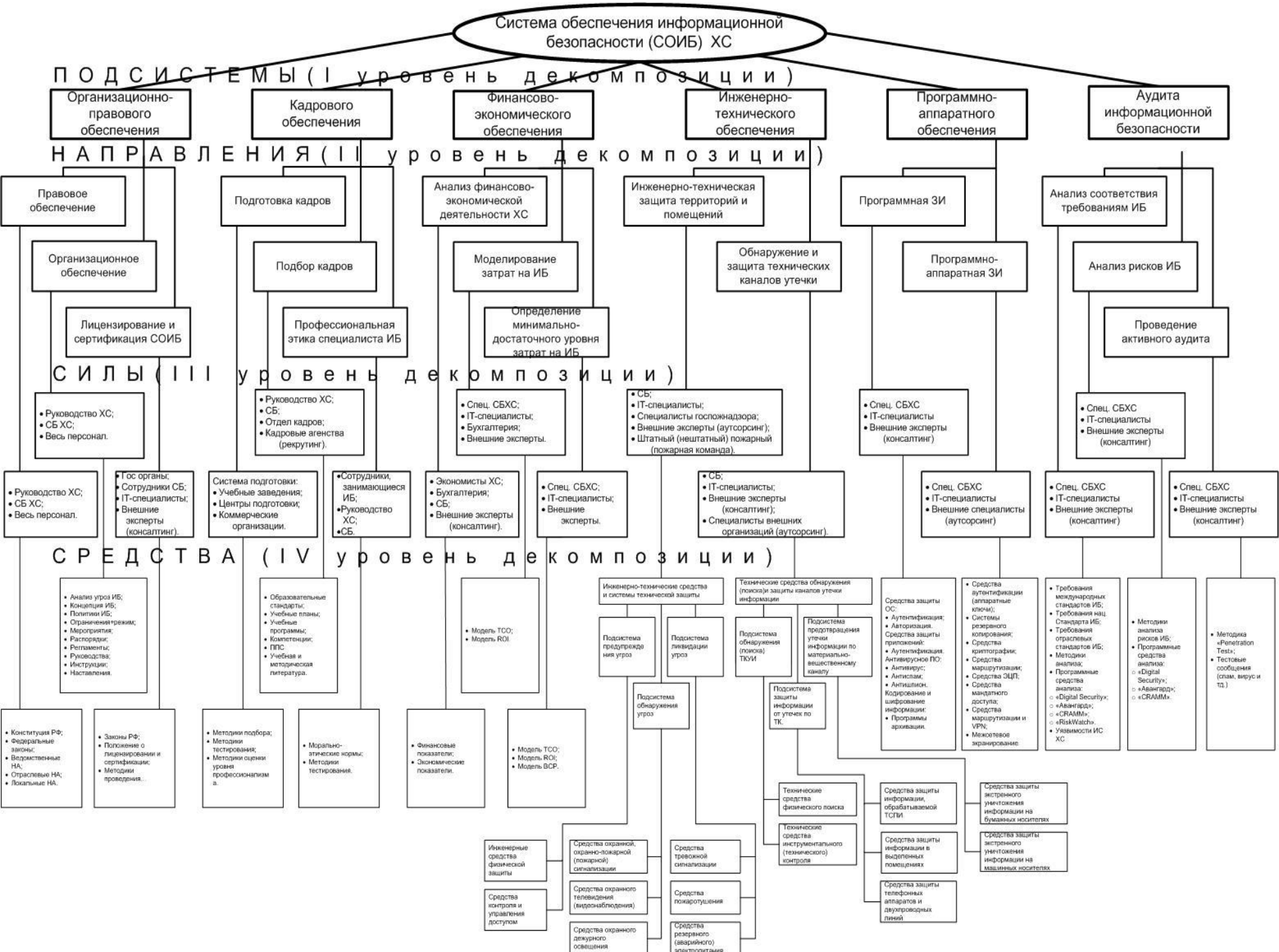
Декомпозиция СОИБ

- - под СОИБ рассматриваем *сложную организационно-иерархическую систему* с видами обеспечения;
- - каждый вид обеспечения является сложной системой и рассматривается в качестве *подсистемы* СОИБ;
- - в каждой подсистеме СОИБ выделяются *направления деятельности* по обеспечению информационной безопасности в интересах хозяйствующего субъекта;
- - каждое направление деятельности по обеспечению информационной безопасности реализуется определенными *силами* (организации, подразделения, должностные лица);
- - конкретные задачи обеспечения информационной безопасности в интересах хозяйствующего субъекта решаются применением конкретных *средств* (методики, документы, компьютерные программы и др.).

Структура вертикальной 4-х уровневой декомпозиции СОИБ




Система обеспечения информационной безопасности хозяйствующего субъекта
П о д с и с т е м ы
Организационно-правового обеспечения
Кадрового обеспечения
Финансово-экономического обеспечения
Инженерно-технического обеспечения
Программно-аппаратного обеспечения
Аудита
Организационное
- наставления;
- руководства;
- инструкции;
- регламенты;
- распорядки
Правовое
- Конституция РФ;
- федеральные законы;
- ведомственные нормативные акты;
- отраслевые нормативные акты;
- локальные нормативные акты;
Н а п р а в л е н и я
Анализ финансово-экономической деятельности
Моделирование экономических и финансовых процессов
Моделирование экономических и финансовых рисков
С р е д с т в а
- экономические показатели;
- финансовые показатели;
- модели TCO, ROI и др.;
- модели оценки экономических и финансовых рисков


Система обеспечения информационной безопасности (СОИБ) ХС
ПОДСИСТЕМЫ (I уровень декомпозиции)
Организационно-правового обеспечения
Кадрового обеспечения
Финансово-экономического обеспечения
Инженерно-технического обеспечения
Программно-аппаратного обеспечения
Аудита информационной безопасности
НАПРАВЛЕНИЯ (II уровень декомпозиции)
Правовое обеспечение
Организационное обеспечение
Лицензирование и сертификация СОИБ
Подготовка кадров
Подбор кадров
Профессиональная этика специалиста ИБ
Анализ финансово-экономической деятельности ХС
Моделирование затрат на ИБ
Определение минимально-достаточного уровня затрат на ИБ
Инженерно-техническая защита территорий и помещений
Обнаружение и защита технических каналов утечки
Программная ЗИ
Программно-аппаратная ЗИ
Анализ соответствия требованиям ИБ
Анализ рисков ИБ
Проведение активного аудита
СИЛЫ (III уровень декомпозиции)
• Руководство ХС;
• СБ ХС;
• Весь персонал.
• Руководство ХС;
• СБ ХС;
• Весь персонал.
• Гос органы;
• Сотрудники СБ;
• IT-специалисты;
• Внешние эксперты (консалтинг).
• Руководство ХС;
• СБ;
• Отдел кадров;
• Кадровые агенства (рекрутинг).
Система подготовки:
• Учебные заведения;
• Центры подготовки;
• Коммерческие организации.
•Сотрудники, занимающиеся ИБ;
•Руководство ХС;
•СБ.
• Спец. СБХС;
• IT-специалисты;
• Бухгалтерия;
• Внешние эксперты.
• Экономисты ХС;
• Бухгалтерия;
• СБ;
• Внешние эксперты (консалтинг).
• Спец. СБХС;
• IT-специалисты;
• Внешние эксперты.
• СБ;
• IT-специалисты;
• Специалисты госнадзора;
• Внешние эксперты (аутсорсинг);
• Штатный (нештатный) пожарный (пожарная команда).
• СБ;
• IT-специалисты;
• Внешние эксперты (консалтинг);
• Специалисты внешних организаций (аутсорсинг).
• Спец. СБХС
• IT-специалисты
• Внешние эксперты (консалтинг)
• Спец. СБХС
• IT-специалисты
• Внешние специалисты (аутсорсинг)
• Спец. СБХС
• IT-специалисты
• Внешние эксперты (консалтинг)
• Спец. СБХС
• IT-специалисты
• Внешние эксперты (консалтинг)
• Спец. СБХС
• IT-специалисты
• Внешние эксперты (консалтинг)
СРЕДСТВА (IV уровень декомпозиции)
• Анализ угроз ИБ;
• Концепция ИБ;
• Политики ИБ;
• Ограничения режим;
• Мероприятия;
• Распорядки;
• Регламенты;
• Руководства;
• Инструкции;
• Наставления.
• Образовательные стандарты;
• Учебные планы;
• Учебные программы;
• Компетенции;
• ППС
• Учебная и методическая литература.
• Модель ТСО;
• Модель ROI.
Инженерно-технические средства и системы технической защиты
Технические средства обнаружения (поиска)и защиты каналов утечки информации
Средства защиты ОС:
• Аутентификация;
• Авторизация.
Средства защиты приложений:
• Аутентификация.
Антивирусное ПО:
• Антивирус;
• Антишпион.
Кодирование и шифрование информации:
• Программы архивации.
Средства аутентификации (аппаратные ключи);
• Системы резервного копирования;
• Средства криптографии;
• Средства маршрутизации;
• Средства ЭЦП;
• Средства мандатного доступа;
• Средства маршрутизации и VPN;
• Межсетевое экранирование
• Требования международных стандартов ИБ;
• Требования нац. Стандарта ИБ;
• Требования отраслевых стандартов ИБ;
• Методики анализа;
• Программные средства анализа:
○ «Digital Security»;
○ «Авангард»;
○ «CRAMM»;
○ «RiskWatch».
• Уязвимости ИС ХС
• Методики анализа рисков ИБ;
• Программные средства анализа:
○ «Digital Security»;
○ «Авангард»;
○ «CRAMM».
• Методика «Penetration Test»;
• Тестовые сообщения (спам, вирус и тд.)
Подсистема предупреждения угроз
Подсистема ликвидации угроз
Подсистема обнаружения (поиска) ТКУИ
Подсистема предотвращения утечки информации по материально-вещественному каналу
Подсистема обнаружения угроз
Подсистема защиты информации от утечек по ТК
• Конституция РФ;
• Федеральные законы;
• Ведомственные НА;
• Отраслевые НА;
• Локальные НА.
• Законы РФ;
• Положение о лицензировании и сертификации;
• Методики проведения..
• Методики подбора;
• Методики тестирования;
• Методики оценки уровня профессионализма.
• Моально-этические нормы;
• Методики тестирования.
• Финансовые показатели;
• Экономические показатели.
• Модель ТСО;
• Модель ROI;
• Модель BCP.
Инженерные средства физической защиты
Средства контроля и управления доступом
Средства охранной, охранно-пожарной (пожарной) сигнализации
Средства охранного телевидения (видеонаблюдения)
Средства охранного дежурного освещения
Средства тревожной сигнализации
Средства пожаротушения
Средства резервного (аварийного) электропитания
Технические средства физического поиска
Технические средства инструментального (технического) контроля
Средства защиты информации, обрабатываемой ТСПИ
Средства защиты информации в выделенных помещениях
Средства защиты телефонных аппаратов и двухпроводных линий
Средства защиты экстренного уничтожения информации на бумажных носителях
Средства защиты экстренного уничтожения информации на машинных носителях

Подсистема организационно-правового обеспечения

Подсистема предназначена для формирования правового поля по выполнению мероприятий обеспечения информационной безопасности, а также обеспечения выполнения концептуальных разработок, практических ограничительных и режимных мероприятий по обеспечению информационной безопасности в интересах хозяйствующего субъекта. организационно-правовое

Обеспечение информационной безопасности хозяйствующего субъекта (ХС) представляет собою совокупность законов, нормативов и управленческих решений, регламентирующих как общую организацию работ по обеспечению информационной безопасности ХС, так и создание и функционирование систем защиты информации на его конкретных объектах.

Подсистема кадрового обеспечения

Подсистема базирующаяся на создаваемой системе подготовки специалистов в области информационной безопасности, а также имеющая в своем составе систему подбора специалистов и систему работы с сотрудниками.

Эти виды деятельности в организации и функционировании данной подсистемы можно представить как три отдельных направления подсистемы кадрового обеспечения:

- Подготовки кадров;
- Подбора персонала ХС для обеспечения ИБ;
- Формирования профессиональной этики специалиста в области ИБ.

Подсистема финансово-экономического обеспечения

Подсистема предназначенная для обеспечения выполнения функций использования результатов анализа финансово-экономической деятельности хозяйствующего субъекта с целью определения возможных масштабов финансирования деятельности по обеспечению информационной безопасности, а также выполнения работ по моделированию и оценке затрат на обеспечение ИБ и определения минимально достаточного уровня затрат, т.е. выполнения оптимизационных расчетов.

Подсистема инженерно-технического обеспечения

Подсистема инженерно-технического обеспечения охватывает совокупность работ по инженерно-техническому оборудованию элементов (объектов) информационной инфраструктуры хозяйствующего субъекта, а также обеспечению предупреждения, обнаружения и ликвидации угроз информационной безопасности на на объектах защиты, и защиты информации, в том числе и компьютерной, от ее утечек по различным техническим каналам.

Под инженерно-техническим обеспечением СОИБ будем понимать совокупность средств инженерно-технической защиты территорий и помещений хозяйствующего субъекта и средств обнаружения и защиты информации, организованная направленность применения которых состоит в создании системы охраны и защиты информации на объектах и элементах информационной системы хозяйствующего субъекта от угроз ее хищения, модификации или уничтожения.

Подсистема программно-аппаратного обеспечения

- Программно-аппаратная защита информации представляет собой совокупность возможностей аппаратных устройств современных информационных и автоматизированных систем ХС, а также установленного на них, или взаимодействующего с ними программного обеспечения по защите информации, хранящейся и обрабатывающейся в данных системах.

Подсистема аудита информационной безопасности

- Под *аудитом информационной безопасности* корпоративной системы будем понимать системный процесс получения объективных количественных и качественных оценок текущего состояния ИБ ХС в соответствии с принятыми критериями и показателями безопасности.
- Подсистема предназначена для обеспечения контроля и проверок качества функционирования всех подсистем и элементов СОИБ применением методик анализа рисков информационной безопасности, а также различных форм проведения проверок.