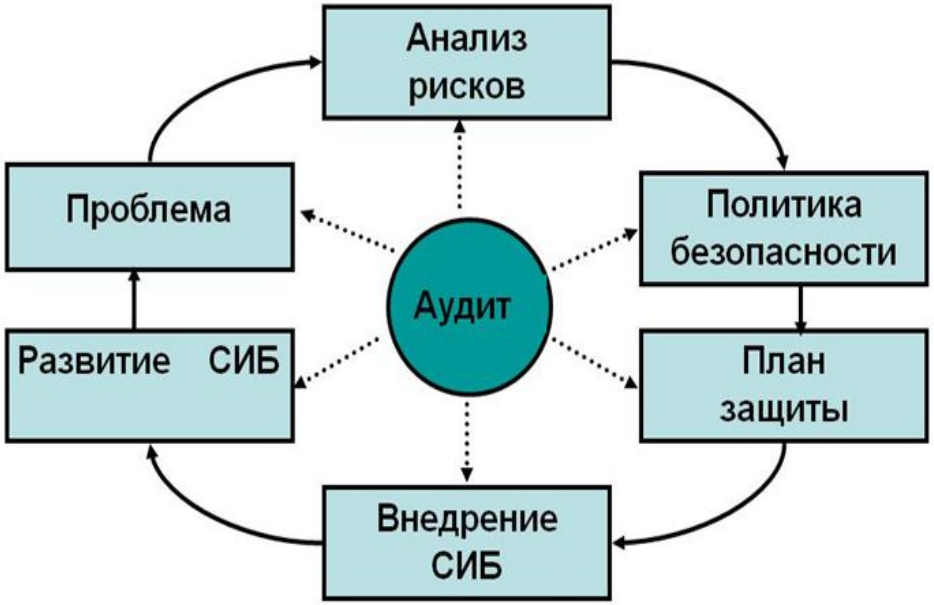
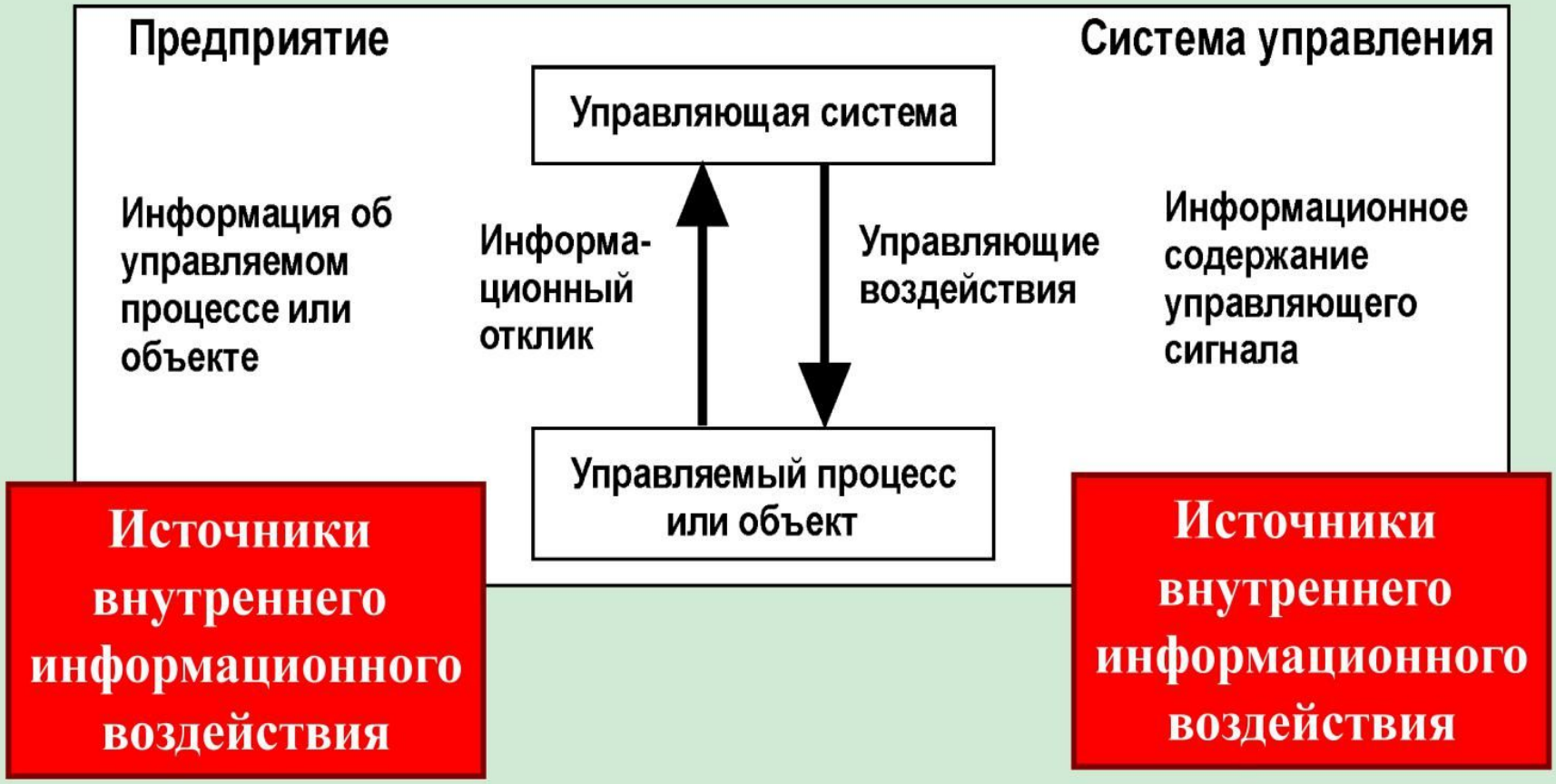
Лекция 4. Модель информационной безопасности предприятия

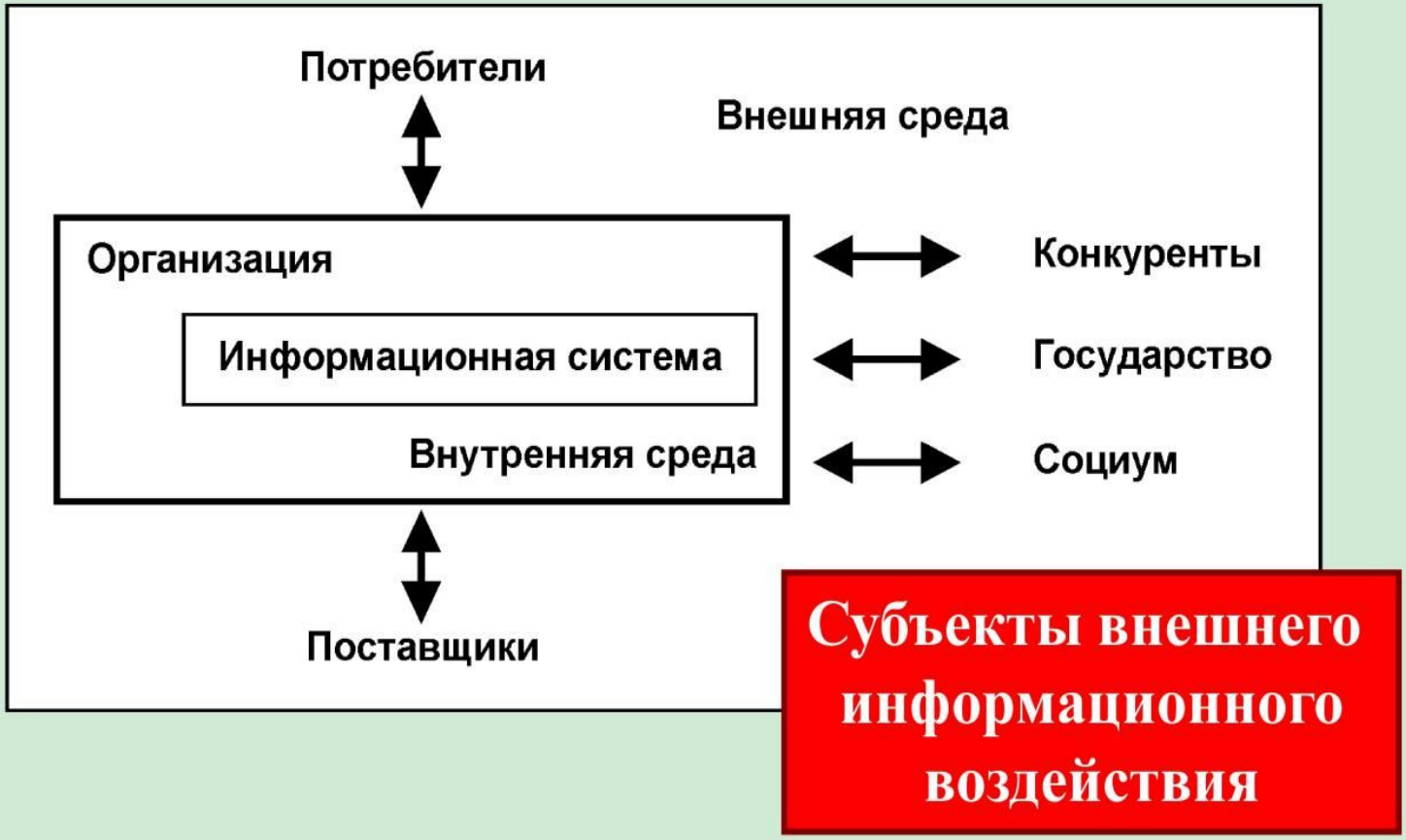
1. Системообразующие функции системы управления предприятием.
2. Реализация программы информационной безопасности на предприятии.



Локальный информационный контур



Внешняя и внутренняя среды предприятия



Ключевые вопросы ИБ

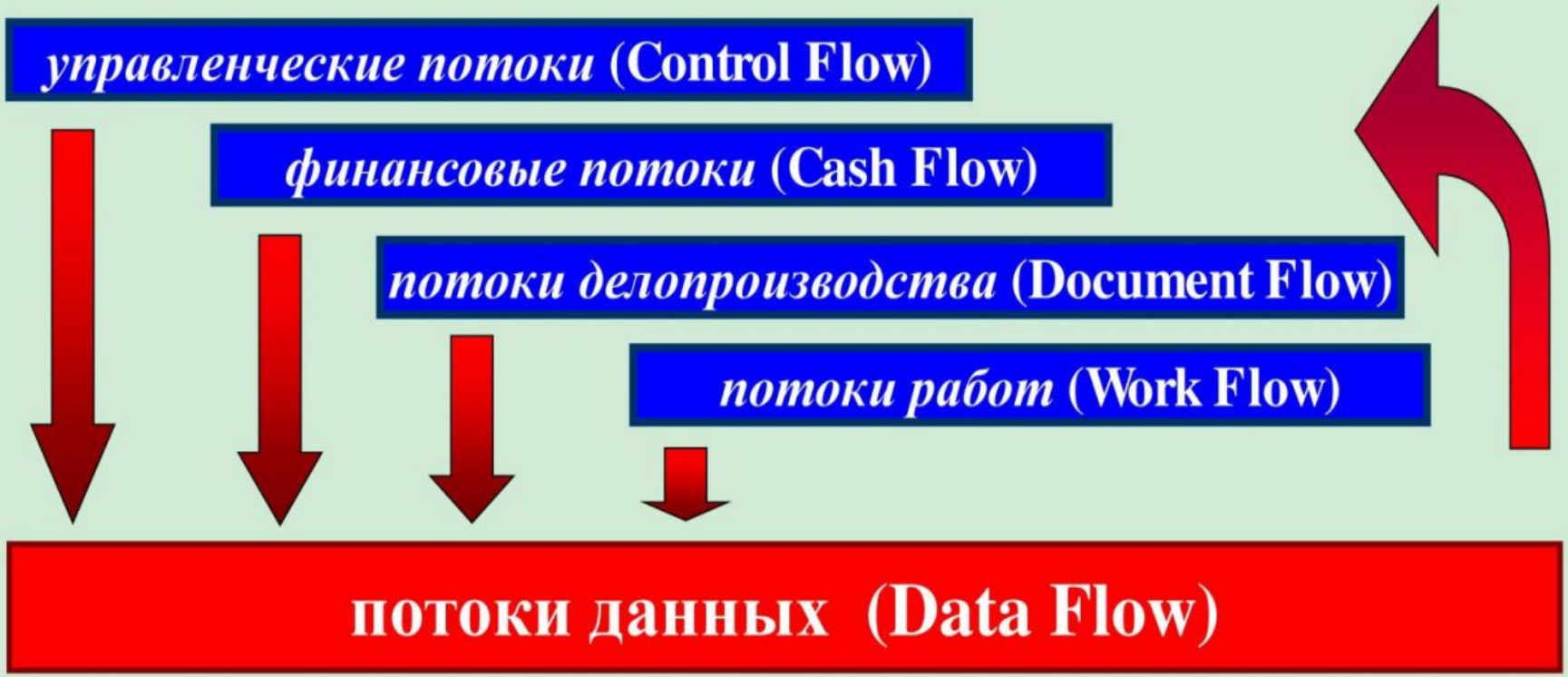
Субъекты нелегального доступа
Вредоносные программы

Что защищать?

От кого защищать?

Как и чем защищать?

Можно выделить *четыре основных вида потоков*, способствующих образованию и циркуляции данных, информации, управляющих сигналов, документов, которые формируют *информационное поле* компании:



Информационное поле и информационный контур компании

Контур информационной защиты

Внешняя среда: **экономические, политические, социальные субъекты и системы, действующие вне предприятия и образующие связи и отношения с ним**

Информация внешней среды —

как правило, неполна, противоречива, приблизительна, разнородна, неадекватно отражает состояние среды, требует постоянного анализа и может содержать дестабилизирующие факторы

Внутренняя среда: **административно-управленческие органы, юридический, планово-финансовый и бухгалтерский отделы, производственные подразделения, ИТ-службы, службы логистики, эксплуатации и т.д.**

Информация внутренней среды —

должна быть точной, актуальной и адекватно отражать текущее состояние предприятия, для того, чтобы обеспечивать его нормальное функционирование и принятие эффективных управленческих и деловых решений;

требует квалифицированной защиты

Общая классификация охраняемой информации

Бóльшая часть внутренней информации является свободно используемой в процессе реализации деятельности государственного или коммерческого предприятия.

В зависимости от особенностей внутренней деятельности и взаимодействия с внешней средой часть информации может быть «для служебного пользования», «строго конфиденциальной», «секретной» или «совершенно секретной».

Такая информация является, как правило, «закрытой» и требует соответствующих политических, организационных физических и технических мер защиты!

Модель информационной безопасности

Раздел классификации	Категория и вид информации
Общедоступная (Public)	Открытая информация, при работе с которой нет никаких ограничений
Для служебного пользования (Restricted Access)	Информация ограниченного доступа на разных уровнях управления предприятием
Конфиденциальная (Confidential)	Конфиденциальная информация, при работе с которой вводятся строгие ограничения в зависимости от уровней допуска пользователя
Персональная (Private)	Персональная информация (платежная ведомость, адресные и паспортные данные, медицинские карточки, ИНН, СПС сотрудников и пр.)

Модель информационной безопасности

Для обеспечения безопасности при работе с охраняемой информацией следует:

- **выстроить политику работы со служебной, конфиденциальной и секретной информацией;**
- **разработать и внедрить соответствующие руководства, правила, процедуры и инструкции;**
- **обеспечить необходимые программно-аппаратные ресурсы для реализации правил и процедур.**

Первый шаг — это введение *коммерческой тайны* в соответствии с Федеральным законом № 98-ФЗ «О коммерческой тайне».

Положение о коммерческой тайне разрабатывается департаментом (отделом) информационной безопасности предприятия и вводится приказом генерального директора.

Коммерческую тайну могут составлять научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, а также секреты производства (ноу-хау), которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа и в отношении которой обладатель такой информации ввел режим «коммерческой тайны».

Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»

Обладатель информации, составляющей коммерческую тайну, имеет право разрешать или запрещать доступ к ней, вводить ее в гражданский оборот на основании договоров, требовать от юридических и физических лиц, органов государственной власти и местного самоуправления, получивших доступ к коммерческой тайне (в том числе от лиц, получивших доступ к ней случайно или по ошибке), соблюдения обязанностей по охране ее конфиденциальности.

Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»

Процедура реализации процесса «Коммерческая тайна»

- Положение о коммерческой тайне
- Приказ высшего руководителя о введении коммерческой тайны в компании
- Приказ о назначении ответственных за соблюдение коммерческой тайны
- Перечень сведений, составляющих коммерческую тайну
- Учет носителей коммерческой тайны (базы данных, журналы, документы с грифом «ДСП» и «Секретно»)
- Приказ генерального директора об ответственности за разглашение или несанкционированную передачу коммерческой тайны.

Программно-аппаратные средства для работы с охраняемой информацией:

- **встраиваются в соответствующие модули корпоративной информационной системы (КИС),**
- **используются локально в системах, оговоренных в политике *информационной безопасности*.**

Средства противодействия угрозам ИБ и утечкам данных и информации являются программно-аппаратным «слоем», реализующим требования *информационной безопасности*, между ИТ-инфраструктурой предприятия и корпоративными ными приложениями, где обрабатываются конфиденциальные данные и с которыми работают сотрудники.

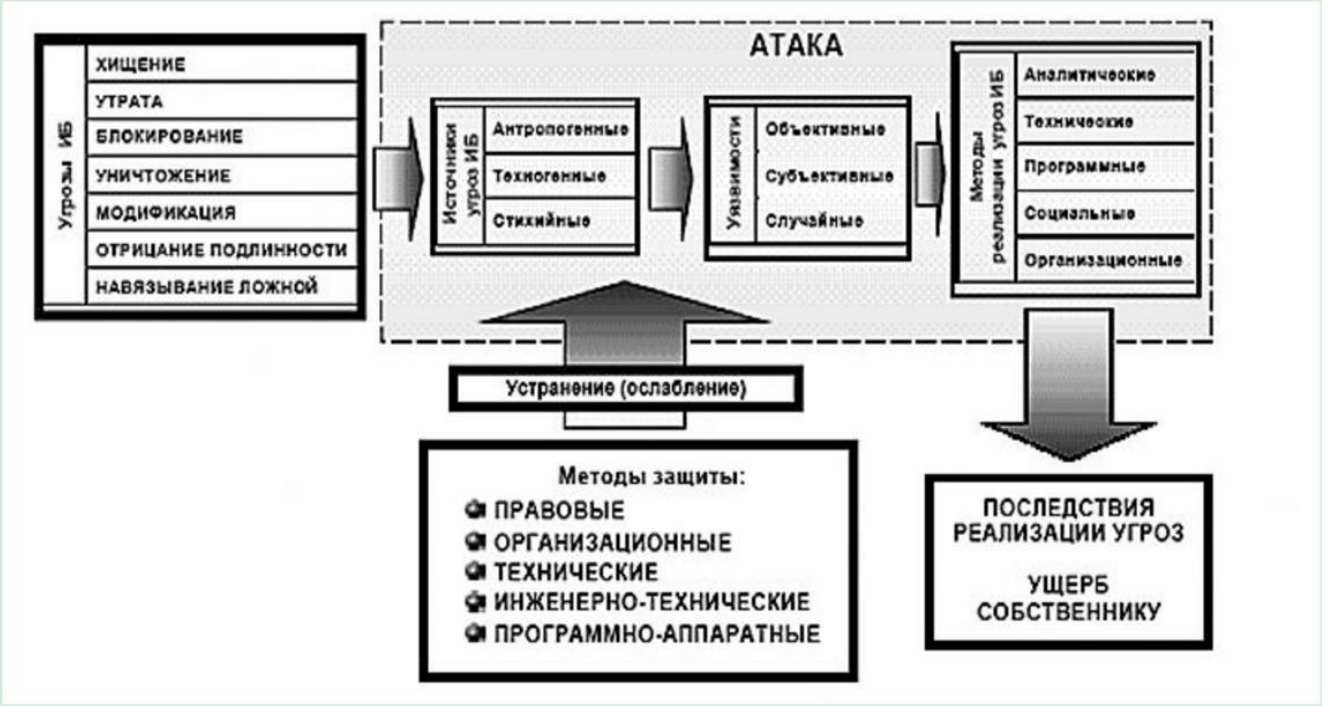
Информационная безопасность

Информационная безопасность **– защищенность данных, информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений – владельцам и пользователям информации и поддерживающей инфраструктуры.**

Информационная безопасность **обеспечивает, прежде всего, сохранность, целостность, конфиденциальность и доступность данных и информации, работоспособность информационной системы, её подсистем и сервисов, средств взаимодействия и связи.**

Содержание поля информационной безопасности

Модель возможных угроз и основные классы методов защиты



Аксиомы воздействия ИТ-угроз

Крупные предприятия имеют достаточно ресурсов (опыт, знания, технические средства), чтобы внедрить защиту от внешних ИТ-угроз, малые – не имеют таких ресурсов

Недооценка рисков внешнего и внутреннего финансового и информационного мошенничества может привести к невосполнимым потерям

Чем крупнее организация, тем более актуальна защита от внутренних угроз.

Утечки информации для крупного предприятия обходится гораздо дороже.

Алгоритм анализа и оценки угроз позволяет:

- установить приоритеты целей ИБ
- определить перечень актуальных источников угроз
- определить перечень актуальных уязвимостей
- оценить взаимосвязь уязвимостей, источников угроз, возможности их осуществления
- определить перечень возможных атак на объект
- разработать сценарии возможных атак
- описать возможные последствия реализации угроз
- разработать комплекс защитных мер и систему управления экономической и информационной безопасностью предприятия.

Пользователь, как источник угрозы

- Непреднамеренная (потеря или искажение данных и информации, порча текстов программ и пр.)
- Намеренная (встраивание логической бомбы, которая со временем разрушит программное ядро или приложения или «взлом» системы администрирования, кража данных и паролей, передача их посторонним лицам и т.д.
- Нежелание пользователя работать с программной или информационной системой и намеренный вывод из строя её программно-аппаратных устройств
- Невозможность правильно работать с системой в силу отсутствия соответствующей подготовки

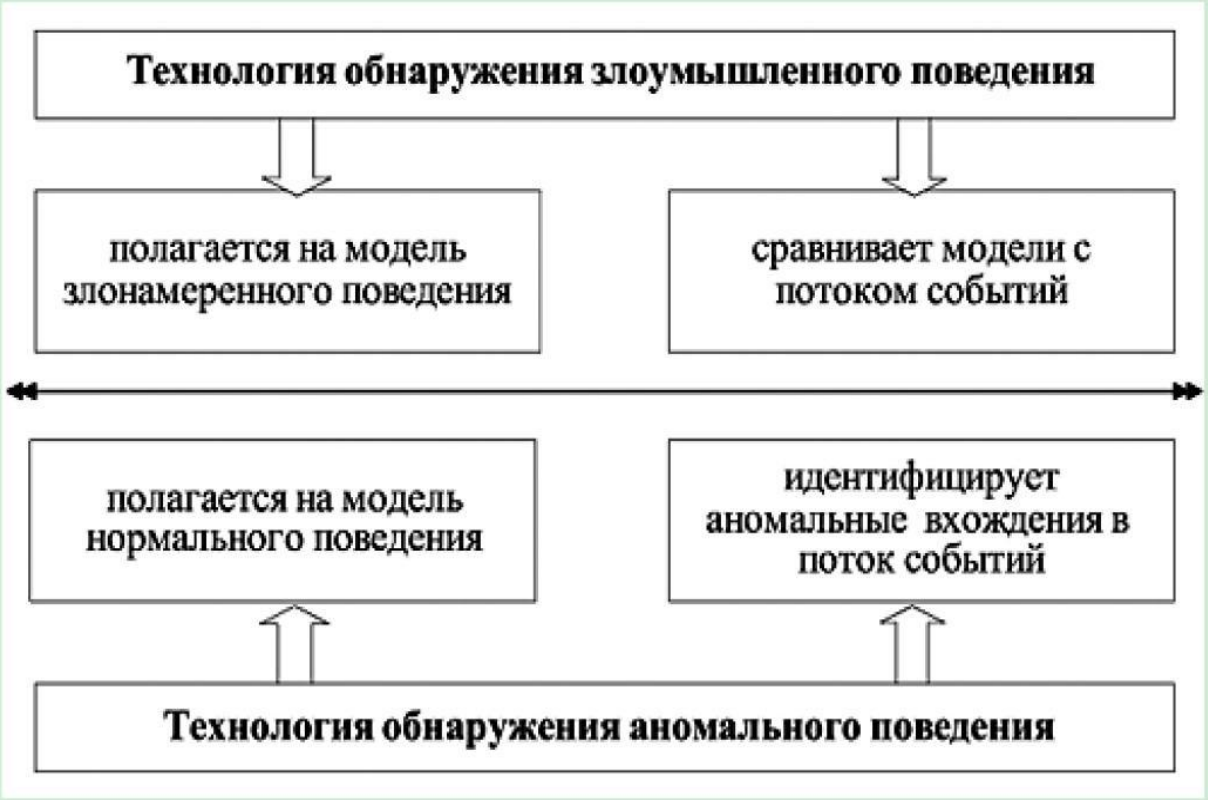
Внутренние системные угрозы

- Выход системы из штатного режима эксплуатации (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)
- Ошибки конфигурирования системы
- Отказы программного и аппаратного обеспечения
- Разрушение базы данных или потеря данных
- Повреждение или разрушение аппаратуры
- Отсутствие технической поддержки (неполнота или неадекватность документации, недостаток справочной информации и т.п.)
- Отступление (случайное или умышленное) от установленных правил эксплуатации.

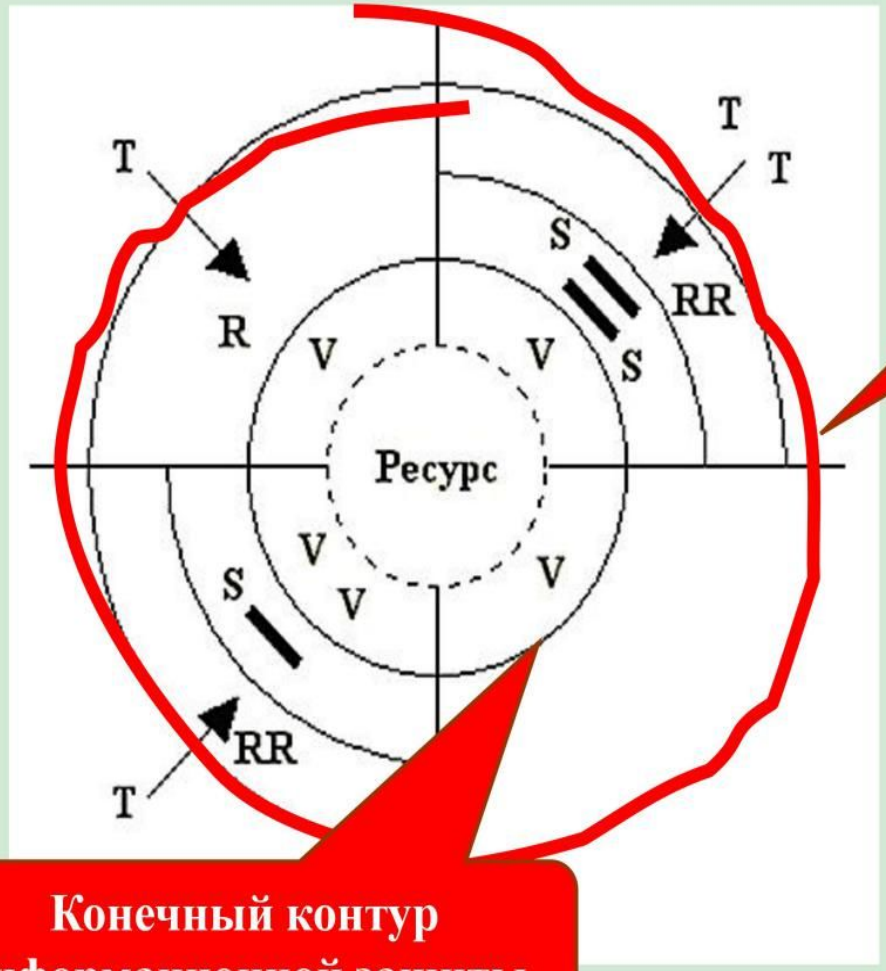
Инфраструктурные и внешние угрозы

- Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
- Разрушение или повреждение помещений
- Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).
- Непреднамеренные и намеренные техногенные катастрофы (пожары, взрывы, обрушения зданий и конструкций и т.д.)
- Стихийные бедствия (наводнения, землетрясения, ураганы, смерчи, снегопады)

Схема обнаружения угрозы на базе моделей



Концептуальная модель защиты от угроз



Начальный контур информационной защиты

Конечный контур информационной защиты

{T, R, RR, S,V}

T – **Threat** (*Угроза*)
R – **Risk** (*Риск*)
RR – **Residual Risk** (*Остаточный риск*)
S – **Safeguard** (*Средство защиты*)
V – **Vulnerability** (*Уязвимость*)

Содержание модели информационной безопасности

Используется в качестве:
- руководства по созданию системы ИБ
- методики формирования требований к системе ИБ
- инструмента оценки состояния системы ИБ
- основы для управления процессами реализации и функционирования системы ИБ

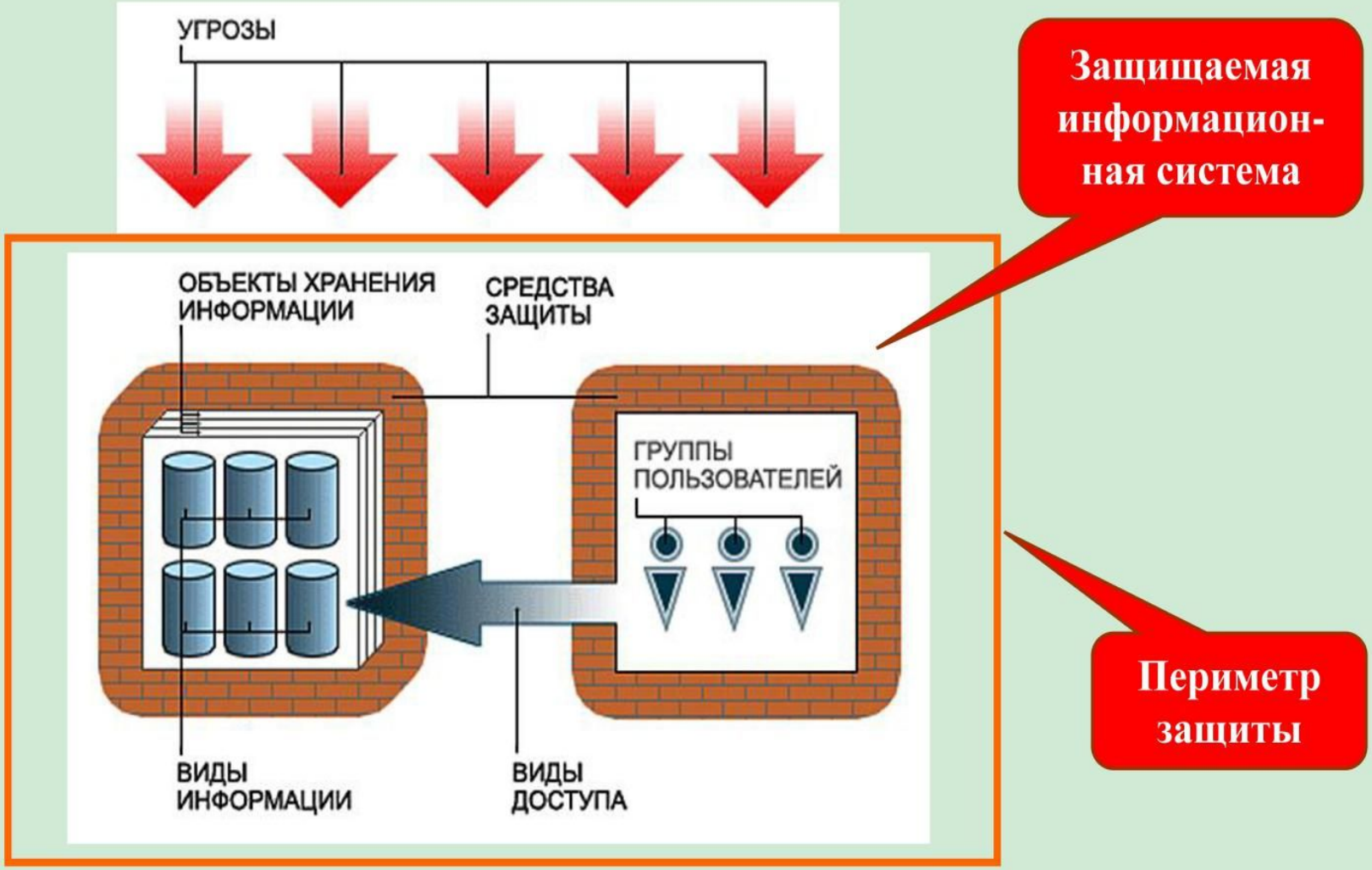
Обладает свойствами:
- комплексности
- универсальности
- наглядности
- практической направленности
- простоты использования

Модель системы информационной безопасности

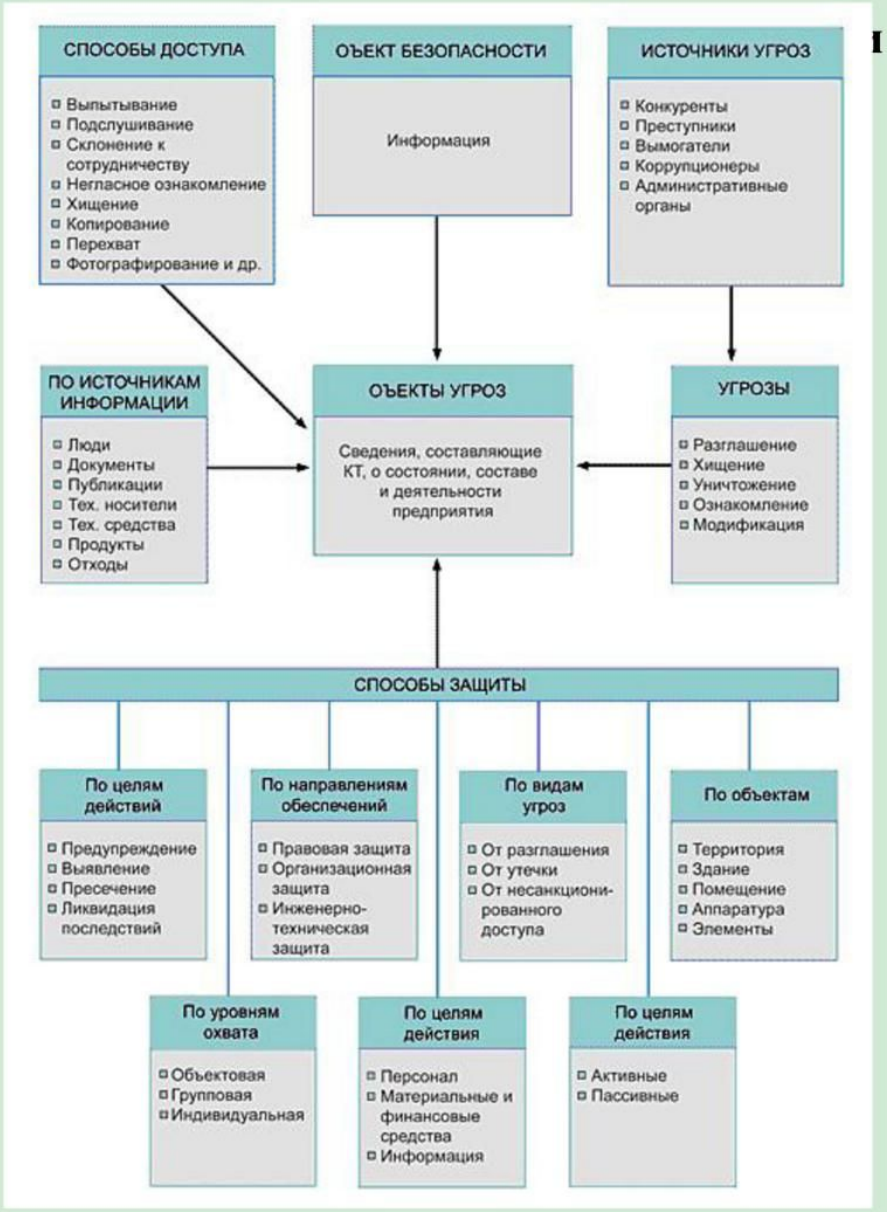
Комплекс методологий, процессов, документов, ресурсов для реализации информационной безопасности

Позволяет:
- применять системный подход к разрешению проблем формирования системы ИБ
- установить связь между требованиями к системе ИБ, относящимися к различным видам угроз
- разрабатывать метрики и получать количественные оценки уязвимостей и рисков
- ранжировать показатели оценки рисков и защищенности на всех уровнях защиты
- определять объекты, процессы и процедуры информационной защиты
- контролировать текущее состояние системы ИБ
- эффективно управлять функционированием системы ИБ
- оперативно реагировать на изменение внешних и внутренних условий функционирования

Общая схема информационной безопасности



Структура модели защиты информационных ресурсов



Оценка защищенности информационной среды

МЕТОДИКИ

1. Разработка регламента проведения аудита
2. Сбор исходных данных
3. Анализ полученных данных с целью оценки текущего уровня безопасности
4. Разработка рекомендаций по повышению уровня защиты АС предприятия

ТЕХНОЛОГИ

Политика информационной безопасности предприятия

Ответственность в информационной сфере

- формирование *единой концепции и программы работ* в области информационной безопасности
- разработка *многоуровневой политики ИБ* и системы структурной и персональной ответственности за её реализацию
- обеспечение выполнения положений политики и программы реализации ИБ
- планирование и выделение *необходимых ресурсов* для системной реализации ИБ
- формирование *структурных* подразделений и служб ИБ
- контроль и аудит *текущего состояния* системы ИБ.

Программу верхнего уровня формирует и возглавляет лицо, отвечающее за *информационную безопасность организации.*

Эти обязанности, как правило, входят в обязанности руководителя ИТ-подразделения (Chief Information Officer – CIO) или службы безопасности (Chief Security Officer – CSO)

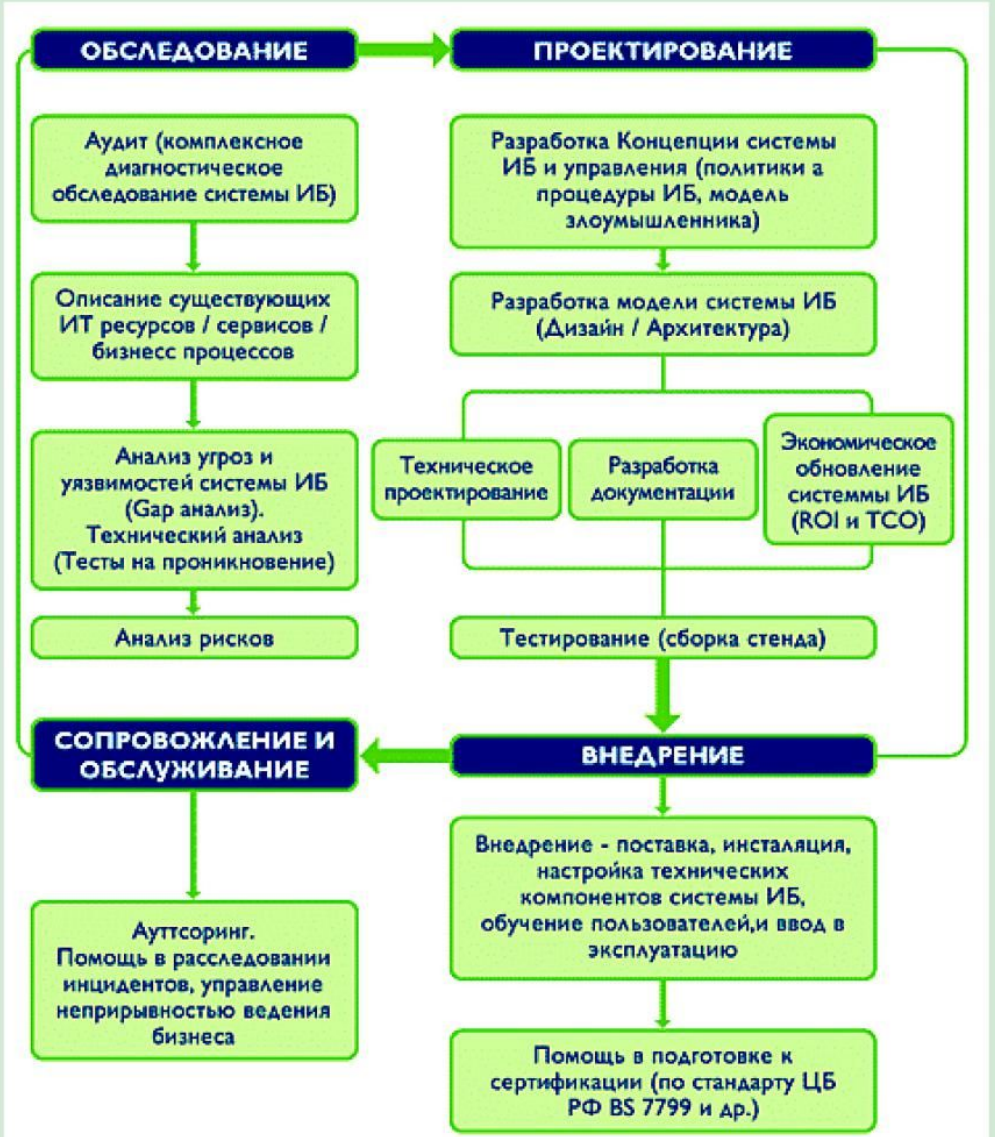
Программа должна содержать следующие главные цели:

- **стратегическое планирование в области развития информационной безопасности**

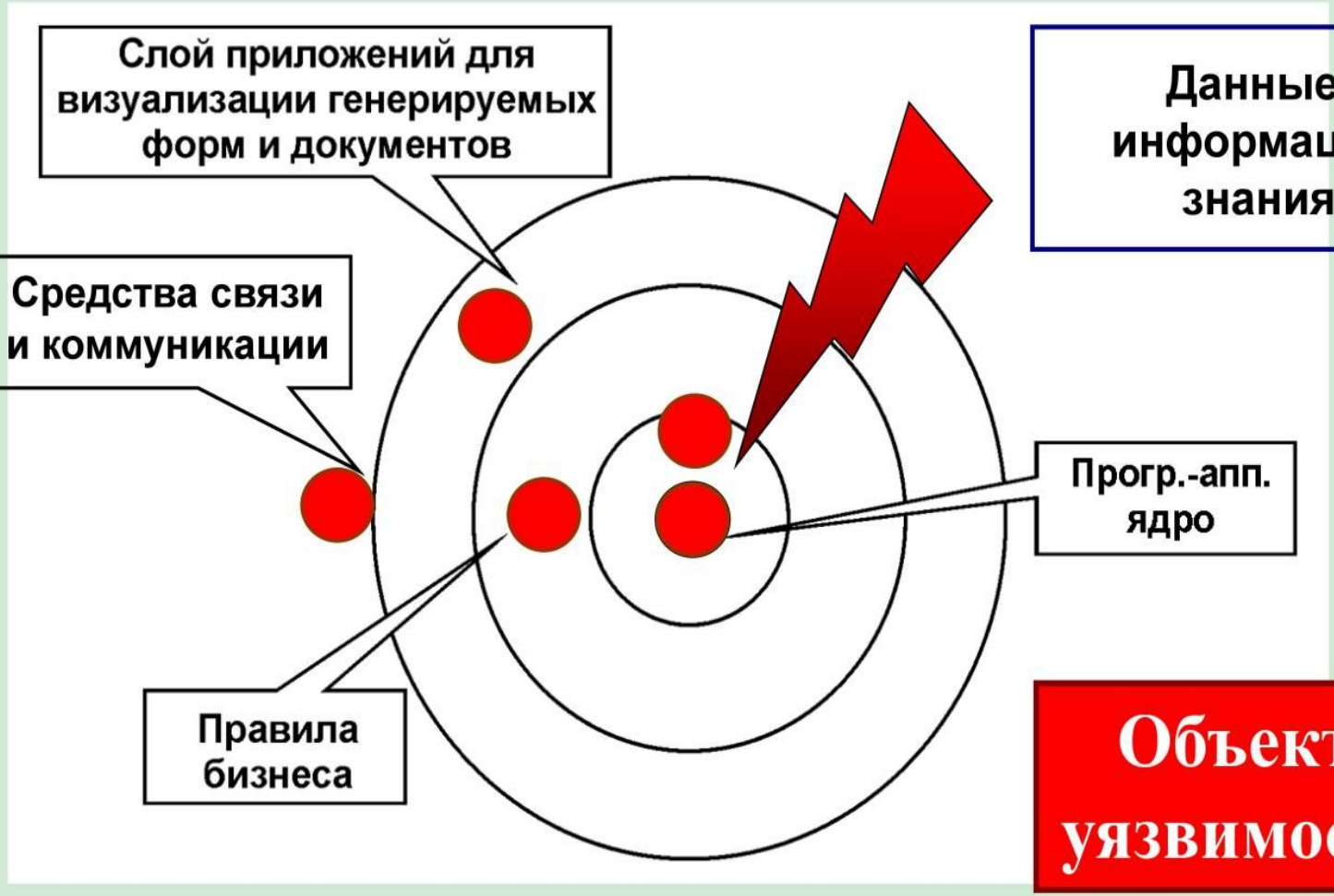
- разработку и исполнение политики в области ИБ
- оценка рисков и управление рисками
- координация деятельности в области информационной безопасности:
  - обследование предприятия и выбор эффективных средств защиты
  - их приобретение или разработка
  - распределение, внедрение, эксплуатация и развитие защитных ресурсов
  - обучение персонала пользованию средствами защиты
- контроль деятельности в области ИБ.

Защищенная ИС, программа ИБ

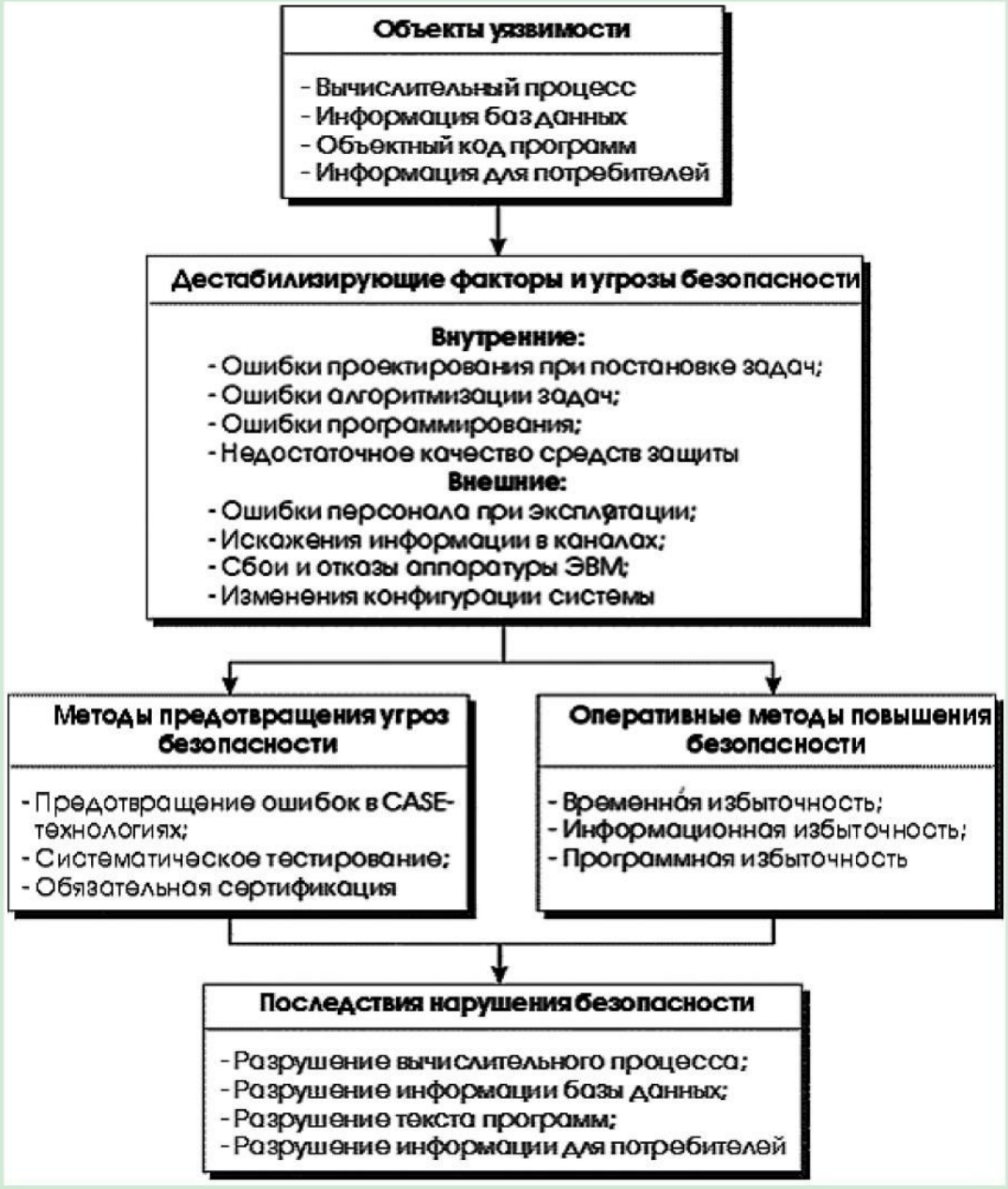
Порядок выполнения «Программы информационной безопасности»



Уровни представления ИС



Модель анализа безопасности информационной системы при отсутствии злоумышленных угроз



Необходимое и достаточное условие безопасности ИС

Надежная и защищённая **информационная система – это «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную достоверную обработку информации разной степени секретности различными пользователями или группами пользователей без нарушения прав доступа, целостности и конфиденциальности данных и информации, и поддерживающая свою работоспособность в условиях воздействия на неё совокупности внешних и внутренних угроз».**

«Оранжевая книга» **[Trusted Computer System Evaliation Criteria (TCSEC). – USA DoD 5200.28-STD, 1993]**

Концепция «Защищенные информационные системы» включает ряд законодательных инициатив, научных, технических и технологических решений, готовность государственных организаций и компаний использовать их для того, чтобы люди, используя устройства на базе компьютеров и программного обеспечения, чувствовали себя безопасно и комфортно.

В общем случае можно говорить о степени доверия, или надежности систем, оцениваемых по двум основным критериям: *наличие и полнота политики безопасности и гарантированность безопасности*.

Уровень базовых документов в иерархии

- Концепция информационной безопасности
- Программа информационной безопасности
- Политика информационной безопасности
- Корпоративные стандарты ИБ
- Конкретные распорядительные и оперативно-функциональные документы

Наличие и полнота политики безопасности **– набор внешних и корпоративных стандартов, правил и норм поведения, отвечающих законодательным актам страны и определяющих, как организация собирает, обрабатывает, распространяет и защищает информацию.**

В политике безопасности сформулированы *права и зоны ответственности* пользователей и персонала. На этом основании можно формировать конкретные механизмы, обеспечивающие безопасность информационной системы.

Чем больше информационная система и чем больше она имеет «входов» и «выходов» (распределённая система), тем «строже», детализированнее и многообразнее должна быть *политика безопасности*.

Гарантированность безопасности **— мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации информационной системы и методам управления её конфигурацией и целостностью.**

Гарантированность проистекает как из тестирования и верификации, так и из системной или эксплуатационной проверки проектирования и исполнения системы в целом и её компонентов.

Гарантированность показывает, насколько *корректны* механизмы, отвечающие за проведение в жизнь политики безопасности.

Гарантированность является *пассивным*, но очень важным параметром защиты и заложенных в информационную или программную систему принципов безопасности.

Концепция гарантированности **является центральной при оценке степени, с которой информационную систему можно считать надежной.**

Надежность определяется всей совокупностью защитных механизмов системы в целом и надежностью вычислительной базы (ядра системы), отвечающих за проведение в жизнь *политики безопасности*.

Надежность вычислительной базы определяется ее программно-аппаратной реализацией и корректностью исходных данных, вводимых административным и операционным персоналом.

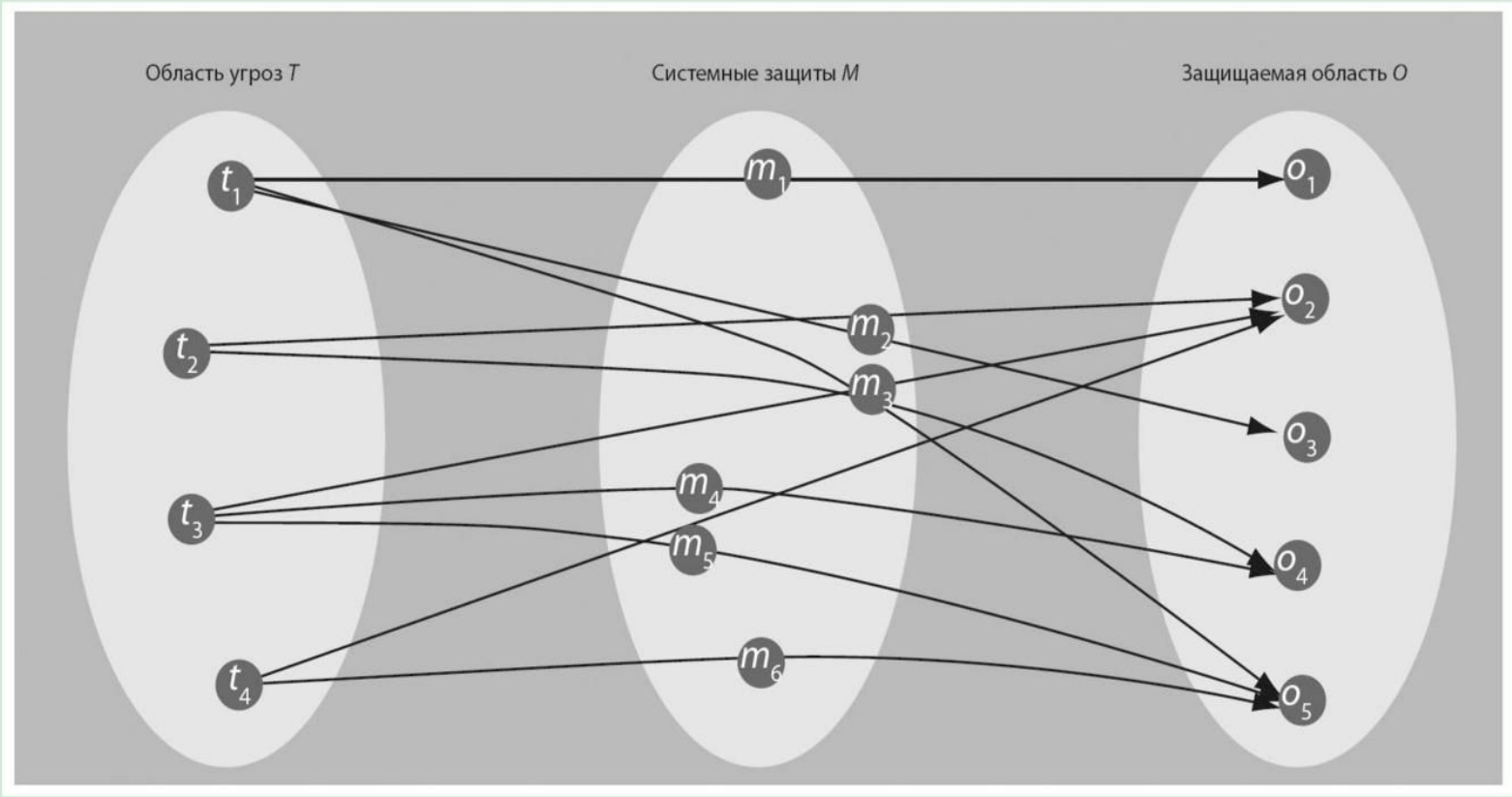
Оценка уровня защищенности ИТ/ИС обычно производится по *трём базовым группам* критериев.

Методология анализа защищенности информационной системы

Основой формального описания систем защиты считается *модель системы защиты с полным перекрытием*, в которой рассматривается взаимодействие «области угроз», «защищаемой области» и «системы защиты».

Таким образом, имеем три множества: $T = \{t_i\}$ – множество угроз безопасности, $O = \{o_j\}$ – множество объектов (ресурсов) защищенной системы, $M = \{m_k\}$ – множество системных механизмов безопасности АС.

Модель системы защиты с полным перекрытием



$T = \{t_i\}$ $M = \{m_k\}$ $O = \{o_j\}$

Развитие модели предполагает введение еще двух элементов {V} – набор уязвимых мест, определяемый подмножеством декартова произведения {T*O}: $v_r = <t_i , o_j>$.

Под уязвимостью системы защиты понимают вероятность осуществления угрозы T в отношении объекта O.

{B} – набор барьеров, определяемый декартовым произведением {V*M}: $b_l = <t_i , o_j , m_k>$, представляющих собой пути осуществления угроз, перекрытые средствами защиты.

В результате получаем систему, состоящую из пяти элементов: <T, M, B, V, O,>, описывающую систему защиты с учетом наличия уязвимостей.

Надёжность барьера $B = \langle t_i, o_j, m_k \rangle$ характеризуется величиной остаточного риска $Risk_k$, связанного с возможностью осуществления угрозы t_i в отношении объекта информационной системы o_j при использовании механизма защиты m_k:

$$Risk_k = P_k * L_k * (1 - R_k).$$

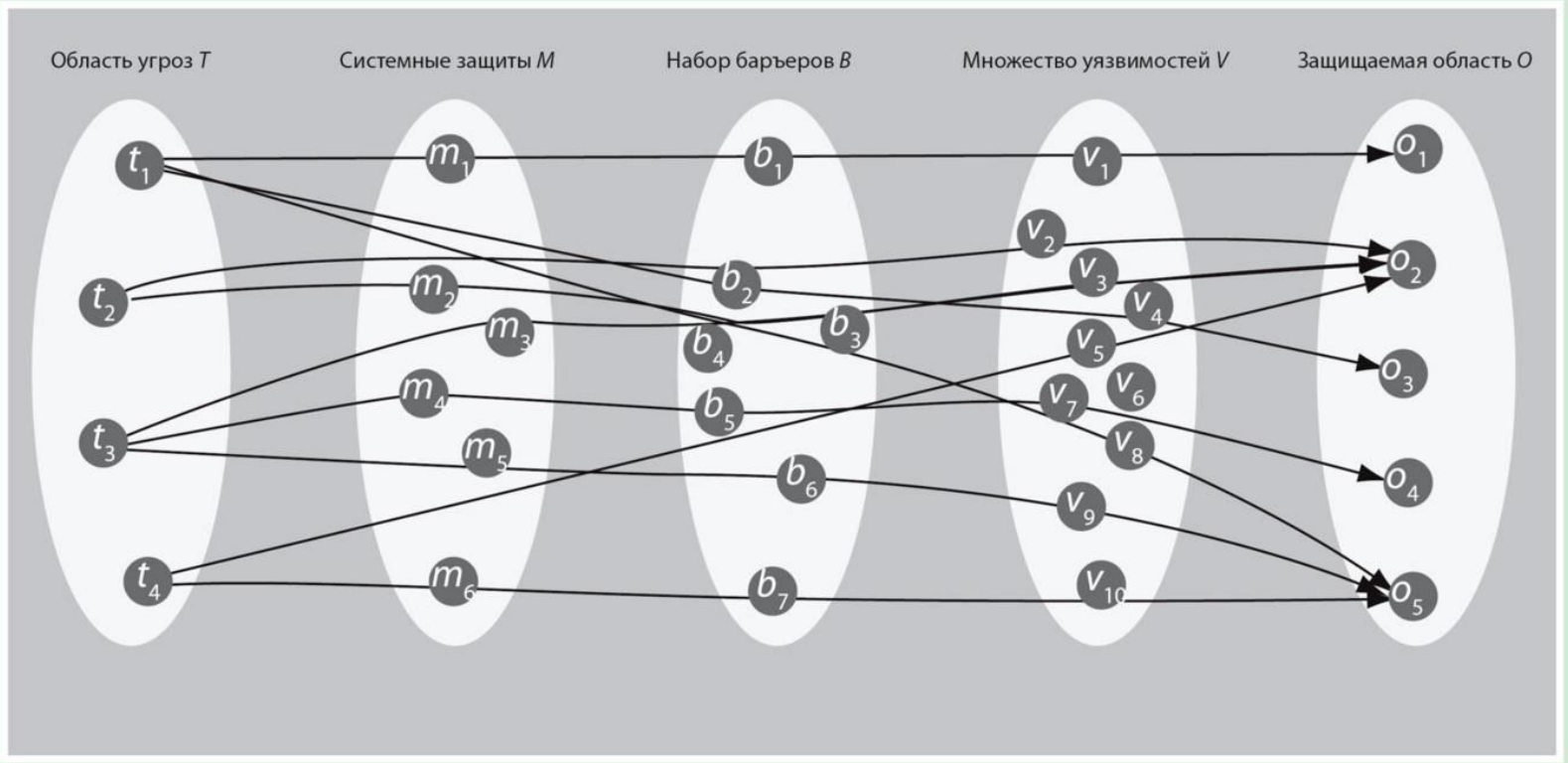
Примерная величина защищенности системы:

$$S = 1/Risk_0, \quad Risk_0 = \Sigma\, Risk_k,$$

где $k = 1,\ldots,K$, $\quad 0 < (P_k, L_k) < 1, \quad (0 \le R_k < 1)$,

P_k – вероятность появления угрозы, L_k – величина ущерба при удачном осуществлении угрозы в отношении защищаемых объектов (уровень серьезности угрозы),
R_k – степень сопротивляемости механизма защиты m_k,
то есть вероятность его преодоления.

Модель системы защиты с полным перекрытием



$\{T^*O\}: v_r = \langle t_i , o_j \rangle$ $\{V^*M\}: b_l = \langle t_i , o_j , m_k \rangle$

Принципы построения защищенной ИС

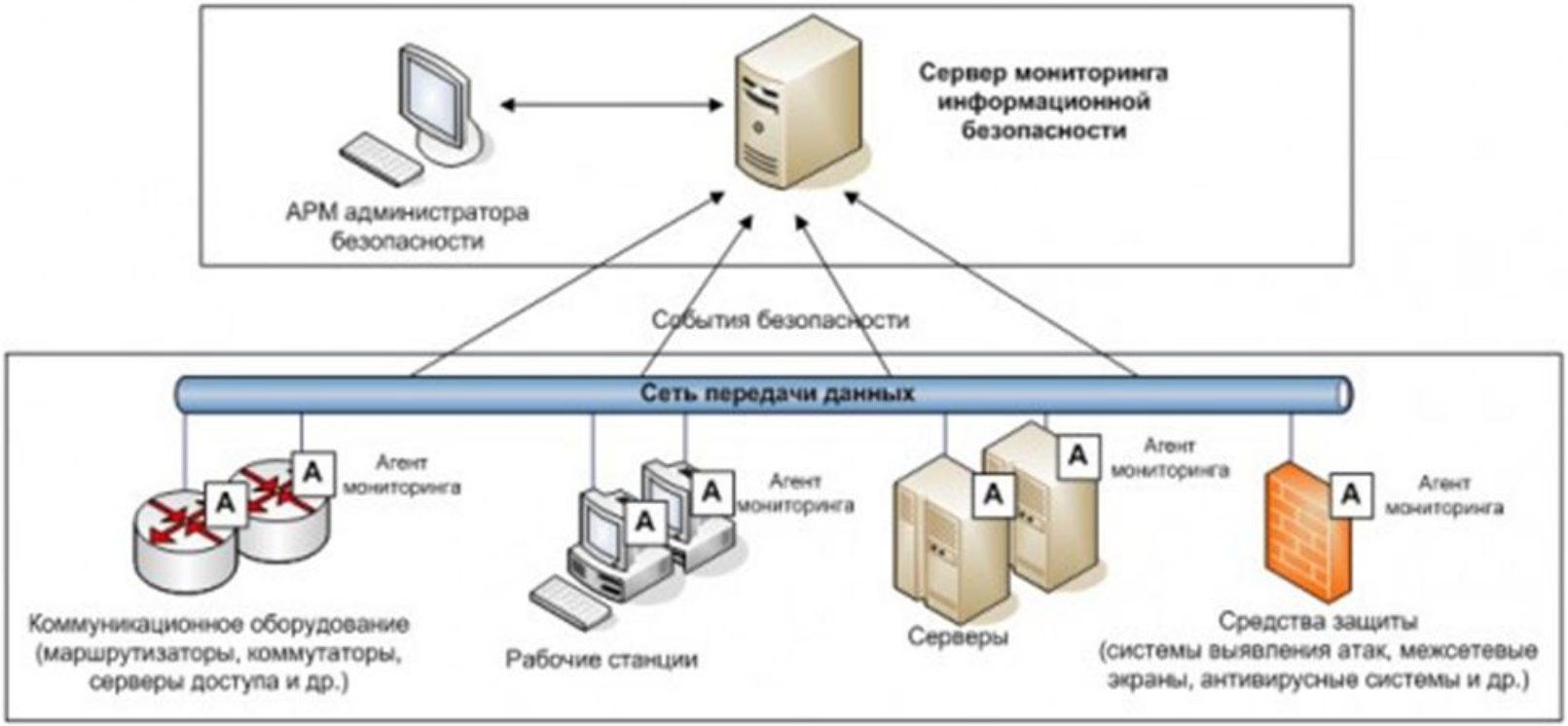
Для того чтобы построить защищенную ИС, необходимо:

- **провести анализ реальных и возможных угроз информации, инфраструктуре и ресурсам ИС**
- **составить перечень требований к защите, исходя из характера использования и архитектуры ИС**
- **реализовать их выполнение путем создания комплексной системы защиты информации(СЗИ)**
- **сформулировать и зафиксировать в нормативных документах правила взаимодействия СЗИ с пользователями ИС**
- **пересматривать содержание нормативных документов по мере развития ИС**

Основные облачные риски

Неполный контроль ИБ	Зависимость от конкретного поставщика облачных сервисов	Нарушение изолированности от других потребителей облачных сервисов
Несоответствие поставщика облачных сервисов требованиям регуляторов	Нарушение безопасности интерфейсов управления облачными сервисами	Нарушение безопасности данных
Неполное удаление данных	Действия внутренних нарушителей поставщика облачных сервисов	Незаконная деятельность с применением облачных сервисов

IBM Security QRadar SIEM – **средство управления событиями и инцидентами информационной безопасности**, являющееся одним из трех модулей, входящих в решение QRadar, которое представляет собой современную интеллектуальную платформу для комплексного мониторинга информационной безопасности предприятия.


Сервер мониторинга информационной безопасности
АРМ администратора безопасности
События безопасности
Сеть передачи данных
A
Агент мониторинга
Коммуникационное оборудование (маршрутизаторы, коммутаторы, серверы доступа и др.)
Рабочие станции
Серверы
Средства защиты (системы выявления атак, межсетевые экраны, антивирусные системы и др.)