

Программно- аппаратная защита

ФИО преподавателя: Оцоков Ш.А.

2021



Содержание дисциплины

1. Основные термины в области информационной безопасности
2. Российское и международное законодательство в области информационной безопасности
3. Классификация средств защиты данных
4. Классификация и характеристики биометрических систем идентификации
5. Классы защищенности средств вычислительных техники от НСД
6. Криптография
7. Математические основы криптографии.
8. Аппаратные и программные средства защиты информации

Лекция 1

Основные термины и определения в области информационной безопасности

ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Информационные системы

Информационная система * - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

ГОСТ Р 51275-2006



Защита информации

**ОБЪЕКТ ИНФОРМАТИЗАЦИИ.
ФАКТОРЫ, ВОЗДЕЙСТВУЮЩИЕ
НА ИНФОРМАЦИЮ**

Общие положения

Издана официально

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Система обработки информации * - совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

Автоматизированная система * - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

СВТ + Персонал

ГОСТ Р 50922-2006



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Информационная безопасность

Информационная безопасность * - свойство информации сохранять конфиденциальность, целостность и доступность.

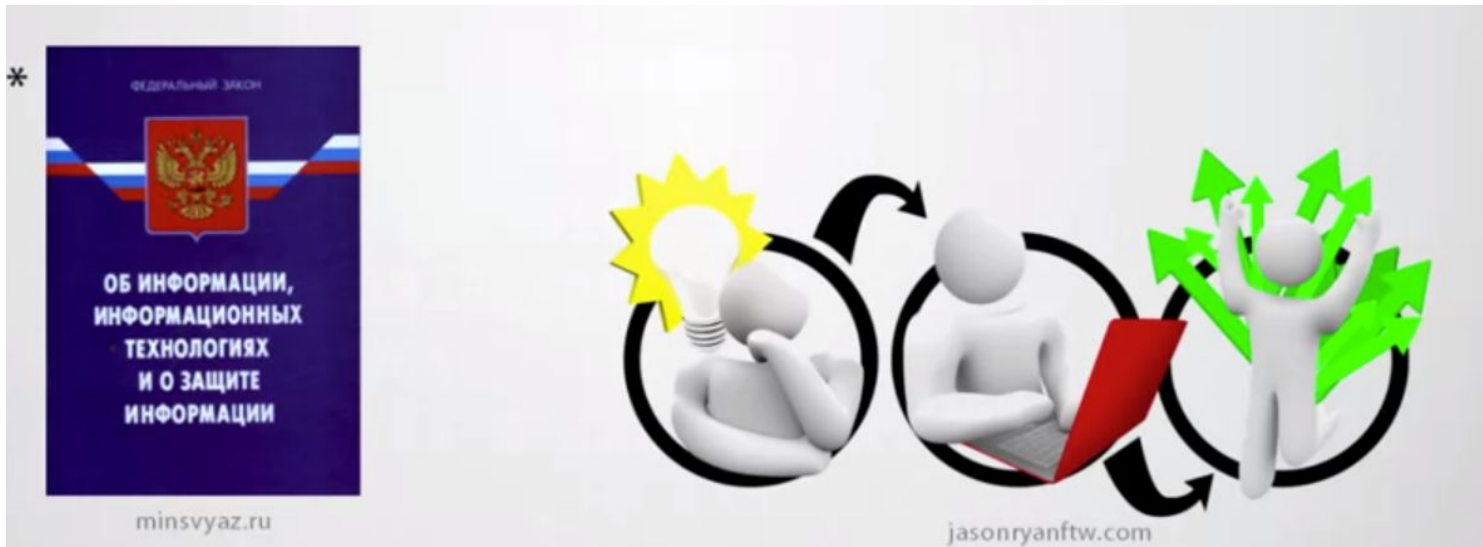
Политика раз разрабатывается в соответствии с имеющейся нормативной базой, многие ее разделы являются законодательно необходимыми, а положения могут быть формализованы без потери качества документа:

- ГОСТ 15408–02
- «Критерии оценки безопасности информационных технологий» и руководящие документы Гостехкомиссии (ныне ФСТЭК) России «Безопасность информационных технологий.
- Критерии оценки безопасности информационных технологий»; международный стандарт ISO/IEC 17799 «Информационные технологии. Свод правил по управлению защитой информации».

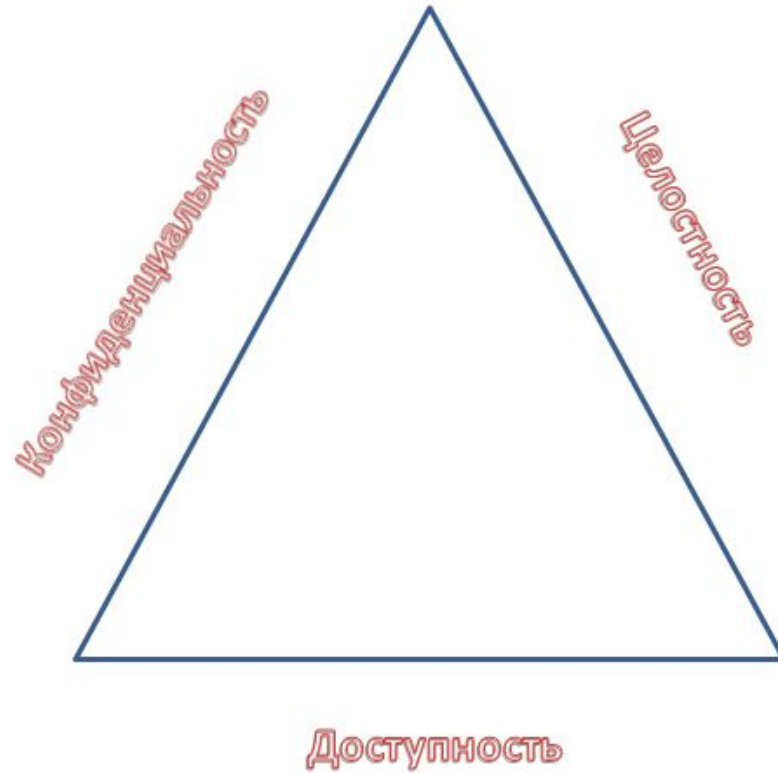
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Обладатель информации * - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.

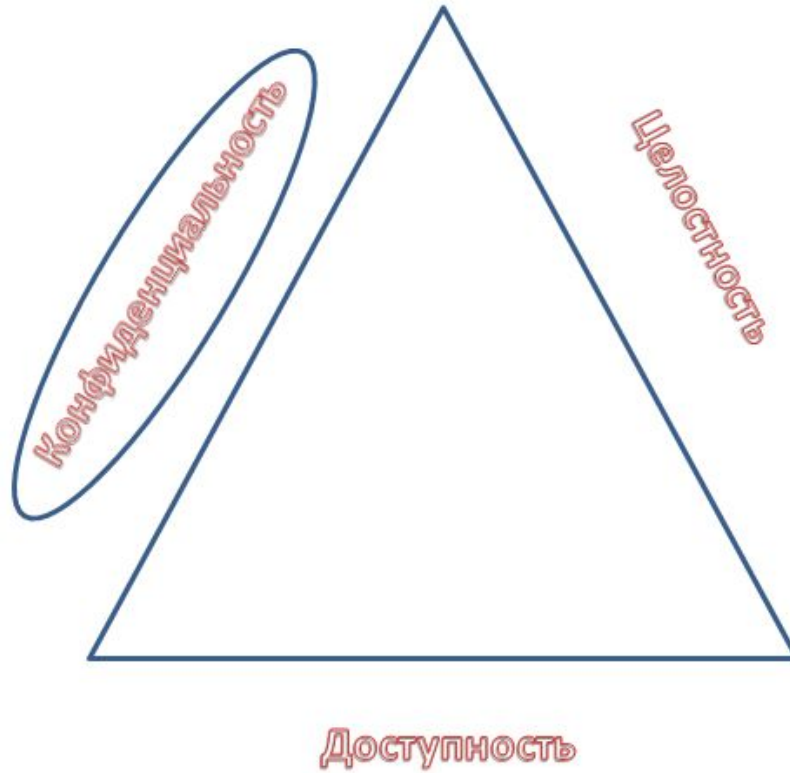
Доступ к информации * - возможность получения информации и ее использования.



ТРИАДА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



ТРИАДА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Управление доступом

Шифрования

Стеганография

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Система обработки информации * - совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

Автоматизированная система * - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Информационная система * - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

ГОСТ Р 50922-2006



ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Контролируемая зона – это охраняемое пространство (территория, здание, офис и т.п.), в пределах которого располагается коммуникационное оборудование и все точки соединения локальных периферийных устройств информационной сети предприятия.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа пользователей к ресурсам информационной системы.

Санкционированный доступ к информации не нарушает правил разграничения доступа.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и/или правил разграничения доступа к информации.

ЗАЩИТА ИНФОРМАЦИИ

Защита информации

Защищаемая информация * - информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Защита информации

Объект защиты информации * – информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

*



У защиты информации должны быть цель и в соответствии с этой целью выделяют объекты, на которые должны быть направлены усилия по защите информации. Это может быть некоторый, носитель информации

ГОСТ Р ИСО/МЭК 27001-2006

Идентификация — процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно определяющий этого субъекта в информационной системе.

Аутентификация — процедура проверки подлинности, например проверка подлинности пользователя путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

Авторизация — предоставление определенному лицу или группе лиц прав на выполнение определенных действий.

Для начала система запрашивает логин, пользователь его указывает, система распознает его как существующий — это **идентификация**.

После этого система просит ввести пароль, пользователь его вводит, и система соглашается, что пользователь, похоже, действительно настоящий, раз пароль совпал, — это **аутентификация**.

После этого система предоставит пользователю право читать письма в его почтовом ящике и все в таком духе — это **авторизация**.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



По положению относительно контролируемой зоны

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАС

| Параметры классификации | Значения параметров | Содержание значения |
|-----------------------------|--|---|
| Виды угроз | <p>Физическая целостность Логическая структура Содержание</p> <p>Конфиденциальность</p> <p>Право собственности</p> | <p>Уничтожение (искажение) Искажение структуры Несанкционированная модификация Несанкционированное получение, утечка информации Присвоение чужого труда</p> |
| Происхождение угроз | <p>Случайное</p> <p>Преднамеренное</p> | <p>Отказы, сбои, ошибки Стихийные бедствия Побочные влияния Злоумышленные действия людей</p> |
| Предпосылки появления угроз | <p>Объективное</p> <p>Субъективное</p> | <p>Количественная и качественная недостаточность элементов системы Промышленный шпионаж, недобросовестные сотрудники, криминальные и хулиганствующие элементы, службы других государств</p> |
| Источники угроз | <p>Люди</p> <p>Технические устройства</p> <p>Модели, алгоритмы, программы Технологические схемы обработки данных Внешняя среда</p> | <p>Пользователи, персонал, посторонние люди Регистрации, ввода, обработки, хранения, передачи и выдачи Общего назначения, прикладные, вспомогательные Ручные, интерактивные, внутримашинные, сетевые Состояние среды, побочные шумы, побочные сигналы</p> |

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источник угрозы безопасности информации – субъект, являющийся непосредственной причиной возникновения угрозы безопасности информации.

Основными источниками нарушения безопасности в АС являются:

- аварии и стихийные бедствия (пожар, землетрясение, ураган, наводнение и т.п.);
- сбои и отказы технических средств;
- ошибки проектирования и разработки компонентов АС (программных средств, технологий обработки данных, аппаратных средств и др.);
- ошибки эксплуатации;
- преднамеренные действия нарушителей.

Существует много критериев классификации угроз. Рассмотрим наиболее распространённые из них.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- 1. По природе возникновения:** естественные и искусственные. Естественные угрозы – это угрозы, вызванные воздействиями на АС и её элементы объективных физических процессов или стихийных природных явлений, независящих от человека. В свою очередь искусственные угрозы – это угрозы АС, вызванные деятельностью человека.
- 2. По степени мотивации:** непреднамеренные (случайные) и преднамеренные. К основным случайным угрозам можно отнести следующие:
 - неумышленные действия, приводящие к нарушению нормального функционирования системы либо её полной остановке.
 - неумышленное отключение оборудования;
 - неумышленная порча носителей информации;
 - использование программ, которые не нужны для выполнения должностных обязанностей.
 - утрата, передача кому-то или разглашение идентификаторов, к которым относятся пароли, ключи шифрования, пропуска, идентификационные карточки;
 - построение системы, технологии обработки данных, создание

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К основным преднамеренным угрозам можно отнести следующие:

- физическое воздействие на систему или отдельные её компоненты (устройства, носители, люди), приводящее к выходу из строя, разрушению, нарушению нормального функционирования;
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.);
- действия по нарушению нормальной работы системы (изменение режимов работы устройств или программ, создание активных радиопомех на частотах работы устройств системы и т.п.);
- перехват данных, передаваемых по каналам связи, и их анализ в целях выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путём, используя халатность пользователей, путём подбора, путём имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных «спецвложений»

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. **По положению относительно контролируемой зоны:** внутренние и внешние угрозы. В качестве примера внешних угроз может быть *перехват данных*, передаваемых по сети, или утечка через ПЭМИН. К внутренним угрозам можно отнести хищение носителей с конфиденциальной информацией, порчу оборудования, применение различного рода закладок.

2. **По степени воздействия на АС:** пассивные и активные.

Пассивные угрозы – угрозы, не нарушающие состав и нормальную работу АС. Пример – копирование конфиденциальной информации, утечка через технические каналы утечки, подслушивание и т.п. Активная угроза, соответственно, нарушает нормальное функционирование АС, её структуру или состав.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

По типу системы, на которую направлена угроза: системы на базе автономного рабочего места и система, имеющая подключение к сети общего пользования.

По способу реализации:

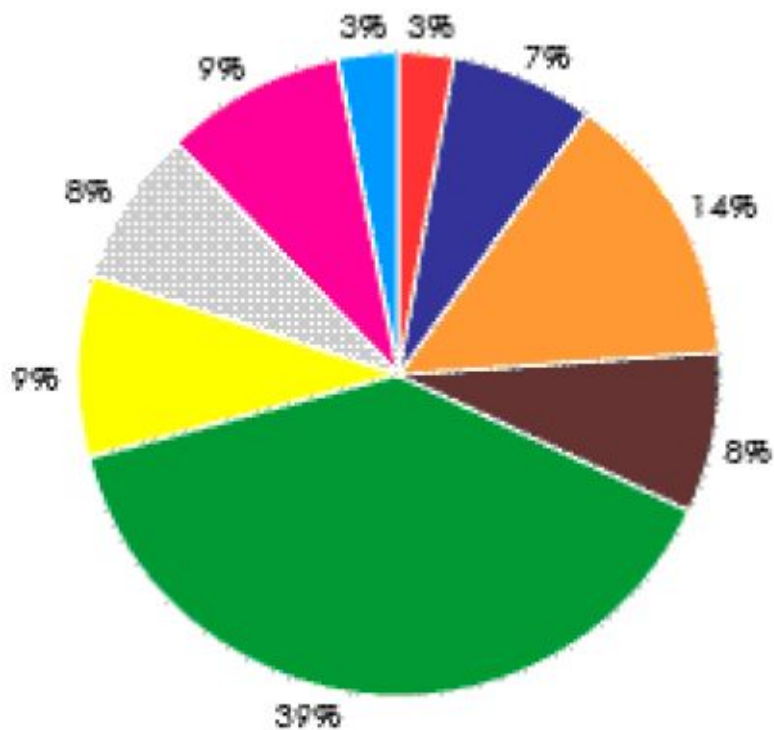
- несанкционированный доступ (в том числе случайный) к защищаемой информации,
- специальное воздействие на информацию,
- утечка информации через технические каналы утечки.

Наиболее распространёнными являются классификации по способу реализации и виду

- нарушаемого свойства информации.

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Каналы умышленных утечек



- электронная почта/факс
- съёмные носители (CD, флеш-накопители)
- ноутбуки/ПК
- другое
- настольные
- интернет/ин

МЕТОДЫ ОЦЕНКИ ОПАСНОСТИ УГРОЗ

При определении угроз на конкретном объекте защиты важно понимать, что нельзя учесть абсолютно все угрозы, а тем более защититься от них. При идентификации угрозы необходимо установить все возможные источники этой угрозы, так как зачастую угроза возникает вследствие наличия определённой уязвимости и может быть устранена с помощью механизма защиты

К идентификации угроз можно подходить двумя путями – по уязвимостям, повлекшим за собой появление угрозы, или по источникам угроз.

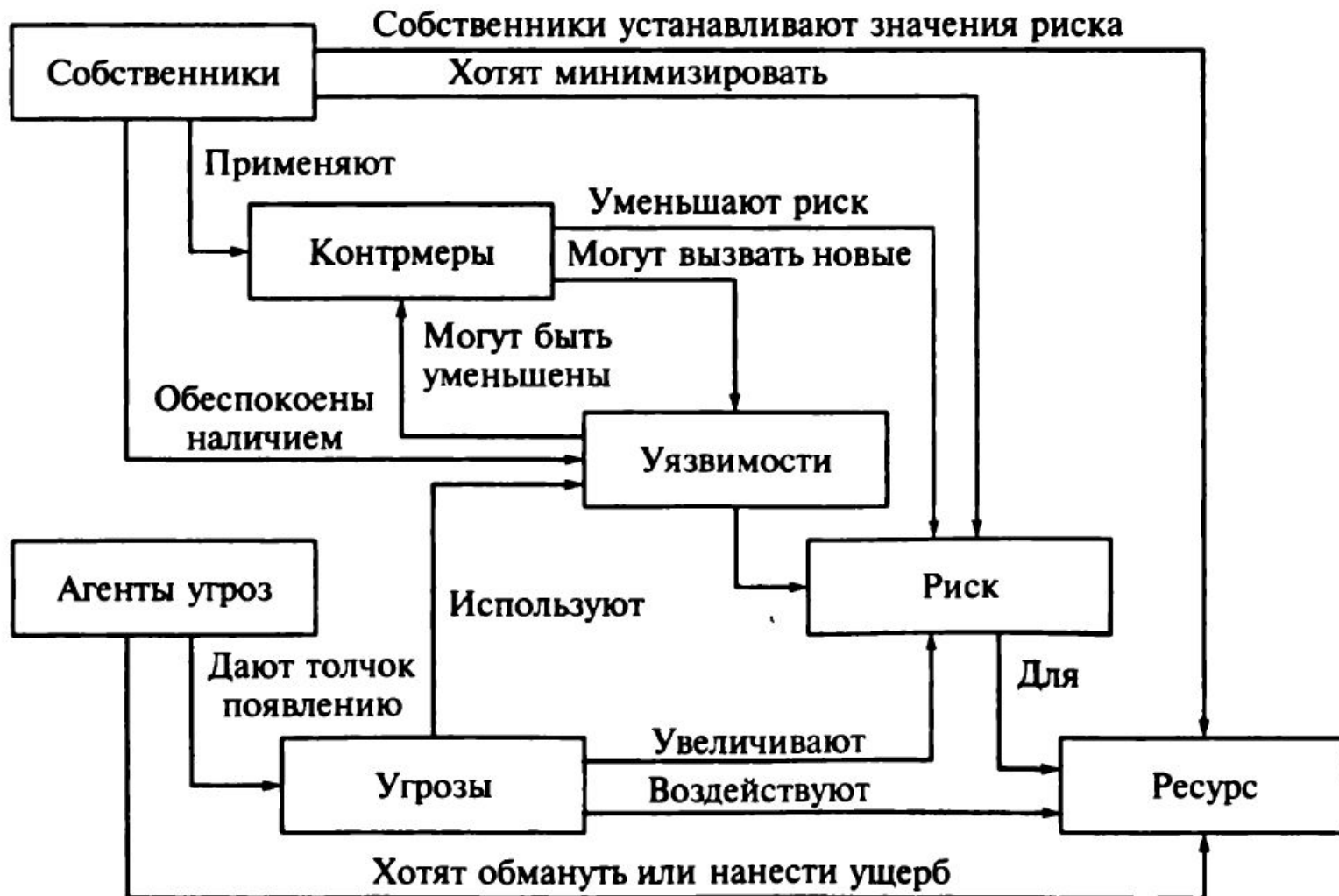
Опасность угрозы определяется риском в случае её успешной реализации. Риск – потенциально возможный ущерб. Допустимость риска означает, что ущерб в случае реализации угрозы не приведёт к серьёзным негативным последствиям для владельца информации.

МЕТОДЫ ОЦЕНКИ ОПАСНОСТИ УГРОЗ

Ущерб подразделяется на опосредованный и непосредственный. Непосредственный связан с причинением материального, морального, финансового, физического вреда владельцу информации.

Опосредованный (косвенный) ущерб связан с причинением вреда государству или обществу, но не владельцу информации.

ОЦЕНКИ РИСКА



**Спасибо за
внимание!**

