Раздел 1. Технические каналы утечки информации

Тема 1. Основные понятия и определения

Что необходимо сделать в течение семестра

1. Посещение лекций (предоставить конспект лекций на экзамен) – не менее 90%
2. Участие в семинарах и практических работах – не менее 90%
3. Выполнение итогового тестирования.
4. Подготовка проекта.

Проект

1) Выбор предприятия для защиты (его организационная структура, месторасположение, вид деятельности, общая информация о предприятии)
2) Создание службы безопасности
3) Написание модели угроз нарушителя
4) Написание политики безопасности

Лекция 1. Цели и задачи защиты информации от утечки информации по техническим каналам

Учебные вопросы:

1. Теория защищаемой информации. Информация, виды, ценность, демаскирующие признаки.
2. Понятие информационного сигнала. Модуляция сигналов. Опасные сигналы и их источники.
3. Термины и определения в области технической защиты информации. Классификация технических каналов утечки информации.
4. Место технической защиты информации в государственной системе защиты информации в Российской Федерации. Цели и задачи защиты информации от утечки информации по техническим каналам (технической защиты информации) .
5. Нормативные документы по технической защите информации

1. Теория защищаемой информации

В теории информации определяются свойства и характеристики информации. Наиболее разработанные положения в настоящее время по информации в телекоммуникационных системах. Проблема заключается в том, что теория не достаточно разработана для информации в информационных системах. В связи с этим далее рассматриваются некоторые особенности информации в области информационной безопасности.

1.1. Информация, свойства, ценность

- Практическая реализация правового регулирования в какой-либо области общественных отношений становится невозможной, если не определить объект, по отношению к которому такое правовое регулирование осуществляется. Единым объектом для рассматриваемой в настоящей работе сферы является информация. Первоисточником данного термина является латинское слово informatio -изложение, истолкование, разъяснение, а вошло оно в русский язык, в эпоху Петра I.
- Обширная область, которую охватывает информация, привело к появлению общей теории информации, но она не охватывает все многообразие ее проявления. В различных областях приводят определения, решающие задачи направления. Приведем еще несколько определений рассматриваемого нами понятия.

- Информация - обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления (Норберт Винер).
- Информация - это результат отражения и обработки в человеческом сознании многообразия внутреннего и окружающего мира, это сведения об окружающих человека предметах, явлениях природы, деятельности других людей и т.д., а также сведения о его внутреннем состоянии. Сведения, которыми человек обменивается через Машину с другим человеком или с машиной и являются предметом защиты в автоматизированной системе.
- Информация - универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и мнений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения (ЮНЕСКО).
- Данное определение в наименьшей степени претендует на академичность, однако в нем присутствует ценная характеристика информации как "универсальной субстанции".

- Существует также целый ряд кратких определений, которые невозможно использовать применительно к потребностям юридической науки, однако они в определенной мере характеризуют информацию как общенаучную категорию, как "универсальную субстанцию":

- информация - это передача разнообразия (Уильям Росс Эшби);

- информация - это оригинальность, новизна (Абрахам Моль);

- информация - это вероятность выбора (Исаак Моисеевич и Акива Моисеевич Яглом);

- информация - это отраженное разнообразие (Аркадий Дмитриевич Урсул).

- Из данной серии представляет интерес еще одно определение, данное Молем: информация - это мера сложности структур. Действительно, чем сложнее объект или процесс, тем больше информации в нем содержится и тем больше информации необходимо для его описания.

Информация
(парадигмы концепций)

Неотъемлемое свойство материи (атрибутивная концепция)

Неотъемлемая составляющая самоуправляемых (технических, биологических, социальных) систем, как функция этих систем (функционально-кибернетическая концепция)

- В Федеральном законе Российской Федерации от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация определяется - сведения (сообщения, данные) независимо от формы их представления.
- В связи с приобретением колоссальной ценности, в ряде стран для социально - экономической информации были приняты государственные законы, определяющие компоненты информации.

- В любом случае во всех аспектах для человека главное то, что информация необходима для познания мира, является "продуктом научного познания", средством изучения реальной действительности и интеллектуального развития общества цивилизации в целом.
- В ведущих странах распространена концепция "третьего мира" , согласно которой существуют три мира; **первый** - мир физических объектов, **второй**- состояний сознания и **третий**- мир знаний, теорий идей, концепций, гипотез, экспериментов, художественных образов (мир объективного содержания мышления)". Последний главной составляющей имеет информацию.

- Информация, как объект, имеет ряд характеристик, свойств:

- ценность,
- жизненный цикл,
- время жизни,
- старение и др.

- Вся информация в целом подразделяется на **два глобальных класса:**

1. **Структурная (связанная) информация**, которая присуща всем объектам неживой и живой природы естественного и искусственного происхождения. Эта информация есть мера сложности данного предмета, она как бы "зашита" в нем, отражая его сущность.
2. **Оперативная (рабочая) информация** - информация, порождаемая перемещением материи и энергии в пространстве и во времени, а также создающаяся в процессе взаимодействия живых организмов.

- Между этими классами информации существует глубокая и постоянная связь. Структурная информация является **предпосылкой** для возникновения оперативной информации. В свою очередь, в результате действий субъектов, порождаемых оперативной информацией, после воздействия на объект неживой или живой природы, может изменяться структурная информация.

Информационные ресурсы

"-Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных других информационных системах)- (**Закон «Об информации, информационных технологиях и защите информации»)**

- Отметим, что параметры ресурсов и информации отличаются, хотя и близки между собой. Ресурсы, фактически, - **информация на носителях информации**.
- В связи с приобретением колоссальной ценности, в ряде стран для социально - экономической информации были приняты государственные законы, определяющие компоненты информации.
- Ценность информации столь значительно выросла, что ее ставят наряду с обычными овеществленными продуктами. Рассмотрим понятия ценности информации.

ЗАДАНИЕ 1: заполните таблицу на основе 149-ФЗ (раздаточный материал)

Виды информационных ресурсов

Вид ресурса	Определение	Признаки

ЗАДАНИЕ 2: заполните таблицу на основе 149-ФЗ (раздаточный материал)

Признаки для отнесения информации к служебной или коммерческой тайне

Вид информации	Признак	Особенности

ЗАДАНИЕ 3: заполните таблицу на основе 149-ФЗ (раздаточный материал)

Задачи системы защиты информации

Задача системы защиты информации по 149-ФЗ

ЗАДАНИЕ 4: заполните таблицу на основе 149-ФЗ (раздаточный материал)

Перечень сведений конфиденциального характера

ЗАДАНИЕ 5: заполните таблицу на основе 149-ФЗ (раздаточный материал)

Информация, не относящаяся к конфиденциальной

ЗАДАНИЕ 6: заполните таблицу на основе 98-ФЗ (раздаточный материал)

Коммерческая тайна

Виды информации, составляющей коммерческую тайну	Краткое описание

ЗАДАНИЕ 7: заполните таблицу на основе 98-ФЗ (раздаточный материал)

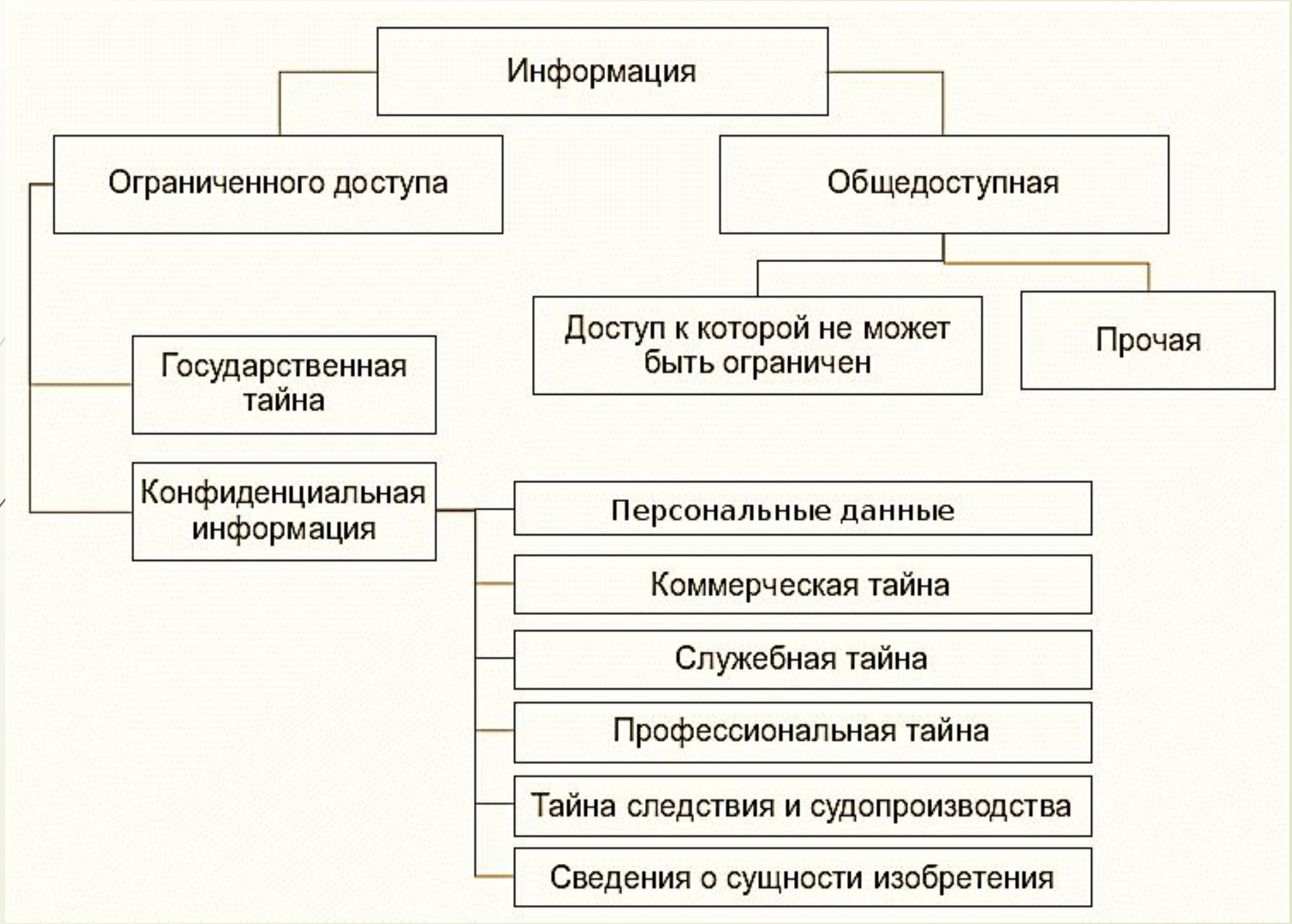
Режим коммерческой тайны

Виды режима коммерческой тайны	Краткое описание

ЗАДАНИЕ 8: заполните таблицу на основе 152-ФЗ (раздаточный материал)

Основные понятия закона о персональных данных

Понятие	Определение


Информация
Ограниченного доступа
Общедоступная
Государственная тайна
Конфиденциальная информация
Доступ к которой не может быть ограничен
Прочая
Персональные данные
Коммерческая тайна
Служебная тайна
Профессиональная тайна
Тайна следствия и судопроизводства
Сведения о сущности изобретения

1.1.1. Ценность информации

- Под ценностью информации понимается ее свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженные в стоимостном, временном либо ином эквиваленте.

- Среди подходов к построению моделей защиты ИС, основанных на **понятии ценности информации** наиболее известными являются:
- оценка,
- анализ и управление рисками ИБ,
- порядковые шкалы ценностей,
- модели решетки ценностей.

- При оценке ценности информации в государственных структурах используется линейная порядковая шкала ценностей. Всю информацию сравнивают экспертным путем и относят к различным уровням ценности. В этом случае документам отнесенным к уровню по шкале присваиваются соответствующие грифы секретности. Сами грифы секретности образуют порядковую шкалу, например (принятую почти всеми государствами):

ЖУРНАЛ
регистрации документов с грифом "Конфиденциально"

№ п/п	Дата регистрации документа	Дата и номер документа (для входящих)	Откуда поступил или куда направлен	Краткое содержание (заголовок)	Кол-во листов	Кол-во экземпляров	Исполнитель	Примечание

Журнал регистрации конфиденциальных документов

- Более высокий класс имеет более высокую ценность и поэтому требования по его защите от несанкционированного доступа более высокие.

- Рассматриваемая шкала хронологически была самой ранней и перестала удовлетворять требованиям информационных технологий, более детальной классификации. Разработка формализованных моделей информационных систем привело к разработке ценностной модели в виде решетки ценностей, которая является обобщением порядковой шкалы. Ее элементы представляют дискретную модель на базе введенной алгебры: требования рефлексивности, транзитивности, антисимметричности, а также верхней и нижней грани.
- **Уровни секретности**, поддерживаемые системой, образуют множество, упорядоченное с помощью отношения доминирования. Такое множество может выглядеть следующим образом: **сов. секретно, секретно**, **конфиденциально, несекретно** и т. д.
- Система в мандатной модели представляется в виде множеств субъектов **S**, объектов **O**, решетки уровней безопасности **L** и матрицы доступа **M**.
- С помощью решетки уровней безопасности задается соотношение между уровнями безопасности, субъектами и объектами.
- В данной модели набор прав ограничен двумя: **read** (чтение) и **write** (запись).

Решетка уровней безопасности

Уровень безопасности	Субъекты	Объекты	R	W
Совершенно секретно	S_1, S_2	O_5		
Секретно	S_3	O_1, O_2		
Конфиденциально	S_4	O_4		
Несекретно	S_5, S_6	O_3, O_6		

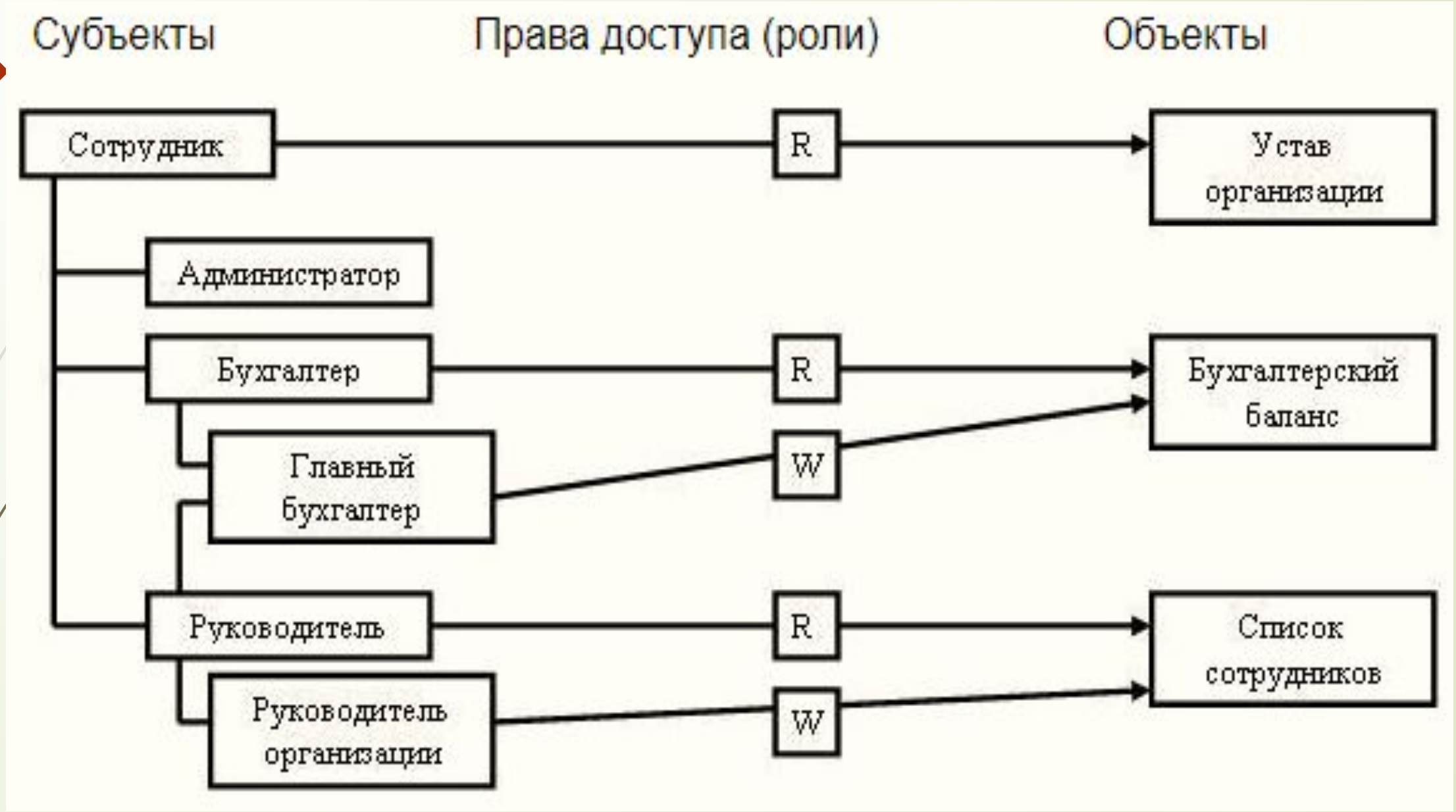
- **Контроль доступа осуществляется** в зависимости от уровней безопасности взаимодействующих сторон на основании двух правил.

1. Уполномоченное лицо (субъект) имеет право читать только те документы, уровень безопасности которых не превышает его собственный уровень безопасности. Данное правило обеспечивает защиту информации, обрабатываемой более доверенными (высокоуровневыми) лицами, от доступа со стороны менее доверенных (низкоуровневых).

- 2. Уполномоченное лицо (субъект) имеет право заносить информацию только в те документы, уровень безопасности которых не ниже его собственного уровня безопасности. Это правило предотвращает утечку информации (сознательную или несознательную) со стороны высокоуровневых участников процесса обработки информации к низкоуровневым.

Матрица доступа

	O_1	O_2	O_3	O_4	O_5	O_6
S_1	R	R	R	R	RW	R
S_2	R	R	R	R	RW	R
S_3	RW	RW	R	R	W	R
S_4	W	W	R	RW	W	R
S_5	W	W	RW	W	W	RW
S_6	W	W	RW	W	W	RW


Субъекты
Права доступа (роли)
Объекты
Сотрудник
R
Устав организации
Администратор
Бухгалтер
R
Бухгалтерский баланс
Главный бухгалтер
W
Руководитель
R
Список сотрудников
Руководитель организации
W

- Рассматриваемая шкала хронологически была самой ранней и перестала удовлетворять требованиям информационных технологий, более детальной классификации. Разработка формализованных моделей информационных систем привело к разработке ценностной модели в виде решетки ценностей, которая является обобщением порядковой шкалы. Ее элементы представляют дискретную модель на базе введенной алгебры: требования **рефлексивности, транзитивности, антисимметричности, а также верхней и нижней грани.**
- **Уровни секретности**, поддерживаемые системой, образуют множество, упорядоченное с помощью отношения доминирования. Такое множество может выглядеть следующим образом: **сов. секретно**, **секретно**, **конфиденциально, несекретно** и т. д.
- Система в мандатной модели представляется в виде множеств субъектов **S**, объектов **O**, решетки уровней безопасности **L** и матрицы доступа **M**.
- С помощью решетки уровней безопасности задается соотношение между уровнями безопасности, субъектами и объектами.

- В основе государственных стандартов оценки ценности информации обычно используют **MLS решетку (Multilevel Security).** Свойства данной решетки используются при классификации новых объектов в ИС, полученных в результате вычислений.

Risk Rating Level Table*

*as specified in the Yellow Book

Rating	Info Sensitivity	User Clearance
0	Unclassified	Uncleared
1	Restricted	Restricted
2	Restricted (categories) Confidential	Confidential
3	Confidential (categories) Secret	Secret
4	Secret (1+ categories)	Top Secret
5	Secret (2+ categories) Top Secret	Top Secret
6	Top Secret (1+ categories)	Top Secret - 1 category
7	Top Secret (2+ categories)	Top Secret - many categories

ДСП

18:58 / 23:30

Recommended Systems

This table states what type of system should be used given the risk index computed.

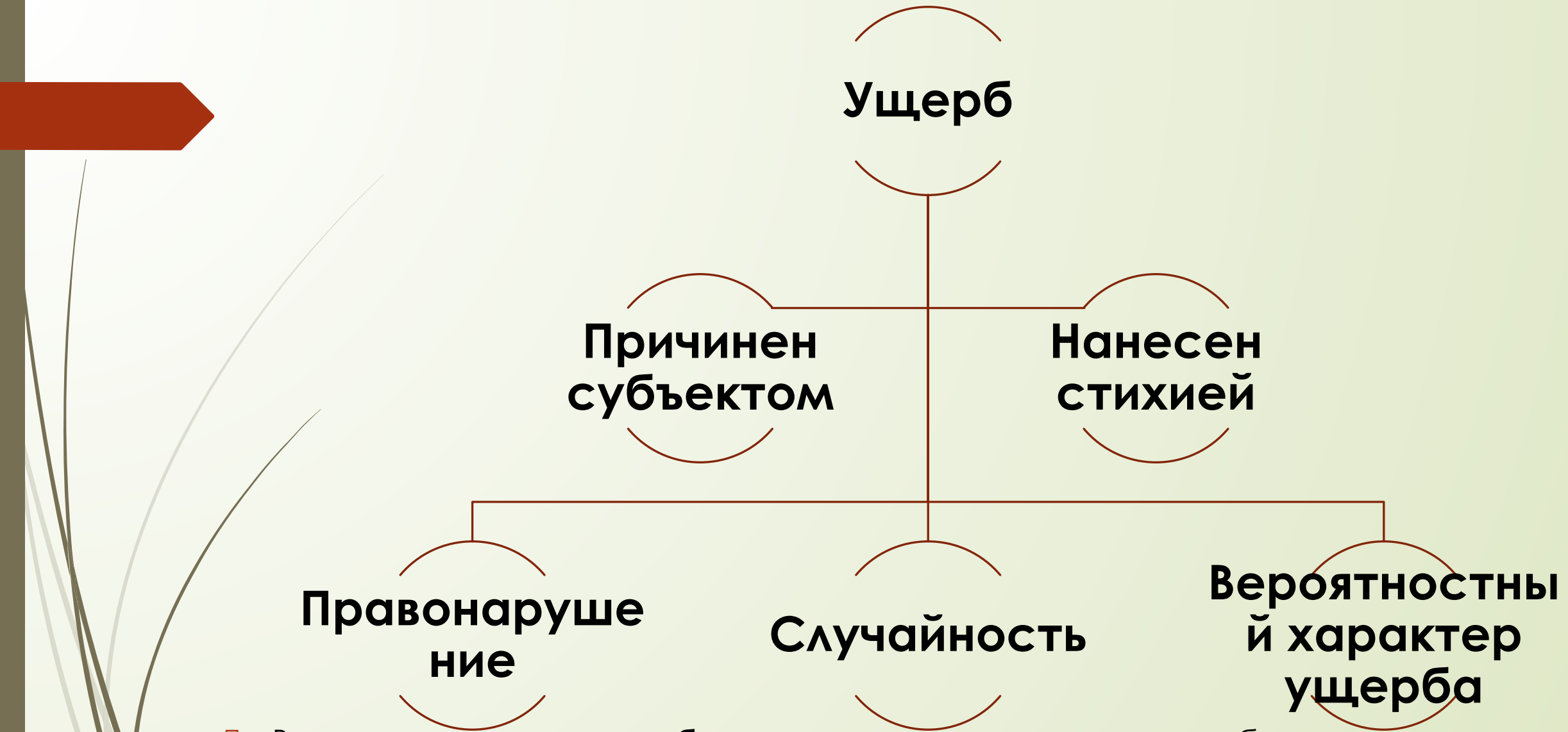
Risk Index	Security Mode	Min Class Open E	Min Class Closed E
0	dedicated	none	none
0	system high	C2	C2
1	limited access, controlled, compartmented, multi-level	B1	B1
2	limited access, controlled, compartmented, multi-level	B2	B2
3	controlled, multi-level	B3	B3
4	multi-level	A1	B3
5	multi-level	beyond A1	A1
>=6	multi-level	beyond A1	beyond A1

Выделенный

Разделенный

Проявления ущерба:

- моральный и материальный ущерб деловой репутации организации;
- моральный, физический или материальный ущерб, связанный с разглашением персональных данных отдельных лиц;
- материальный (финансовый) ущерб от разглашения защищаемой (конфиденциальной) информации;
- материальный (финансовый) ущерб от необходимости восстановления нарушенных защищаемых информационных ресурсов;
- материальный ущерб (потери) от невозможности выполнения взятых на себя обязательств перед третьей стороной;
- моральный и материальный ущерб от дезорганизации деятельности организации;
- материальный и моральный ущерб от нарушения международных отношений.



- В теории права **под ущербом понимается** невыгодные для собственника имущественные последствия, возникшие в результате правонарушения. Ущерб выражается в уменьшении имущества, либо в недополучении дохода, который был бы получен при отсутствии правонарушения (**упущенная выгода**).

- **Примеры составов преступления**, определяемых Уголовным Кодексом Российской Федерации .
- **Хищение -** совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.
- **Копирование компьютерной информации** - повторение и устойчивое запечатление информации на машинном или ином носителе.
- **Уничтожение** - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.
- **Уничтожение компьютерной информации** - стирание ее в памяти ЭВМ.
- **Повреждение** - изменение свойств имущества при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится полностью или частично непригодным для целевого использования.
- **Модификация компьютерной информации** - внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.
- **Блокирование компьютерной информации** - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.
- **Несанкционированное уничтожение, блокирование модификация, копирование информации** - любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.
- **Обман** (отрицание подлинности, навязывание ложной информации) - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Обобщая изложенное, можно утверждать, что **угрозами безопасности информации являются:**

- хищение (копирование) информации;
- уничтожение информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации.

Классификация угроз информации проведена рядом государств и органов, например, Интерполом.

Особенность атрибутивной концепции информации заключается в том ,что признаки объекта проявляются в признаках информации, особенно в технических подсистемах. Рассмотрим эти признаки более подробно.

1.1.2. Виды защищаемой информации

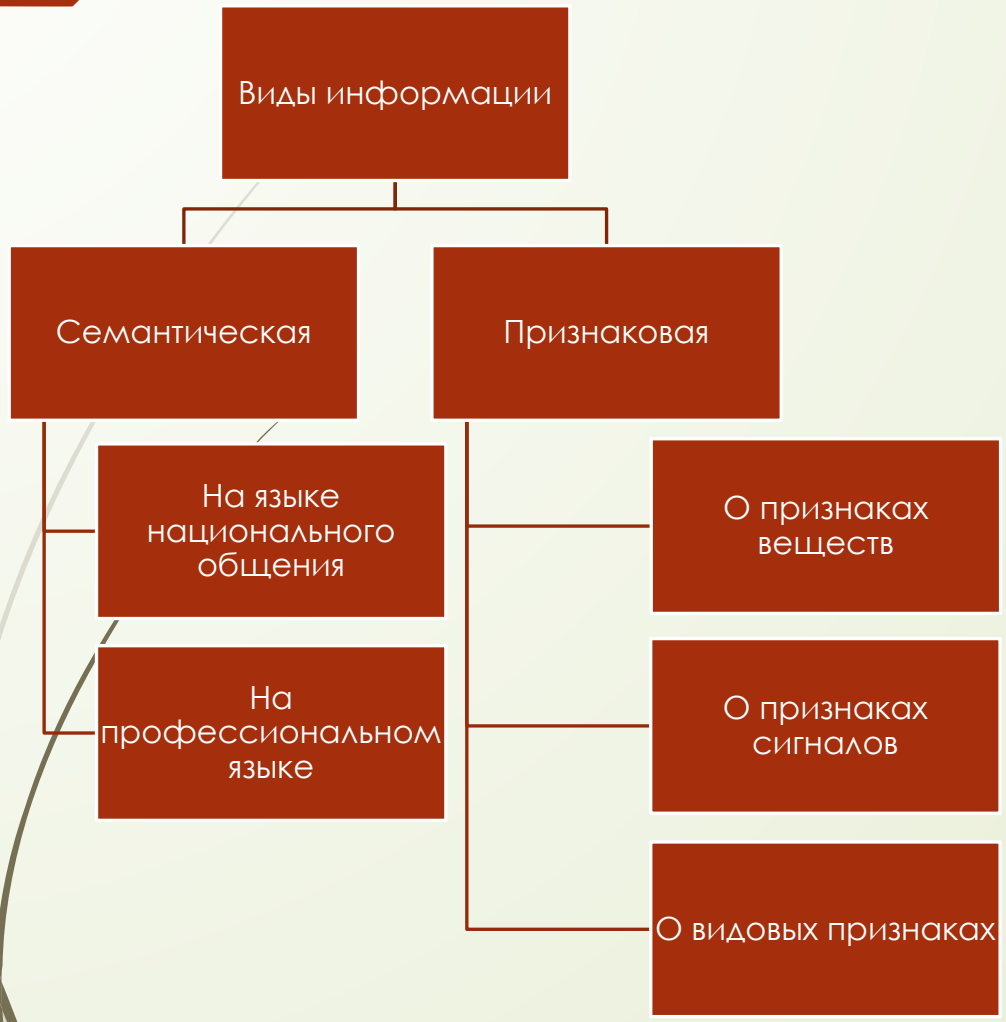
СЕМАНТИЧЕСКАЯ

ПРИЗНАКОВАЯ

- Семантическая информация (от лат. - содержащая смысл) на языке национального общения представляется в виде упорядоченной последовательности знаков (букв, цифр, иероглифов) алфавита этого языка и записывается на любом материальном носителе. В области средств регистрации и консервации семантической информации изыскиваются носители, обеспечивающие все более высокую плотность записи и меньшее энергопотребление. Не зависит от характеристик носителя.
- Профессиональные языки создаются специалистами для экономного и компактного отображения информации. Существует множество профессиональных языков: математики, музыки, радиоэлектроники, автодорожного движения, химии и т. д. В ситуациях. когда нельзя использовать для информирования человека зрительные или акустические сигналы или эти каналы перегружены, воздействуют на его тактильные рецепторы.

- **Информация признаковая** описывает конкретный материальный объект на языке его признаков. Описание объекта содержит признаки его внешнего вида, излучаемых им полей и элементарных частиц, состава и структуры веществ, из которых состоит объект. Источниками признаковой информации являются сами объекты. К ним в первую очередь относятся интересующие;
- зарубежную разведку или отечественного конкурента люди, новая продукция и материалы, помещения и даже здания, в которых может находиться конфиденциальная информация. В зависимости от вида описания объекта признаковая информация делится на информацию о внешнем виде видовых признаках о его полях (признаках сигналов), о структуре и составе его веществ (признаках веществ).
- Защищаемая информация неоднородна по содержанию, объему и ценности. Следовательно защита будет рациональной в том случае, когда уровень защиты, а следовательно, затраты, соответствуют количеству и качеству информации. Если затраты на защиту информации выше ее цены, то уровень защиты неоправданно велик, если существенно меньше, то повышается вероятность уничтожения, хищения или изменения информации. Для обеспечения рациональной защиты возникает необходимость структурирования конфиденциальной информации, т. е. разделения ее на так называемые информационные элементы.
- Информационный элемент представляет собой информацию на носителе с достаточно четкими границами, и удовлетворяет следующим требованиям:
- - принадлежит конкретному источнику (документу, человеку, образцу продукции и т. д.);
- - содержится на отдельном носителе;
- - имеет конкретную цену.

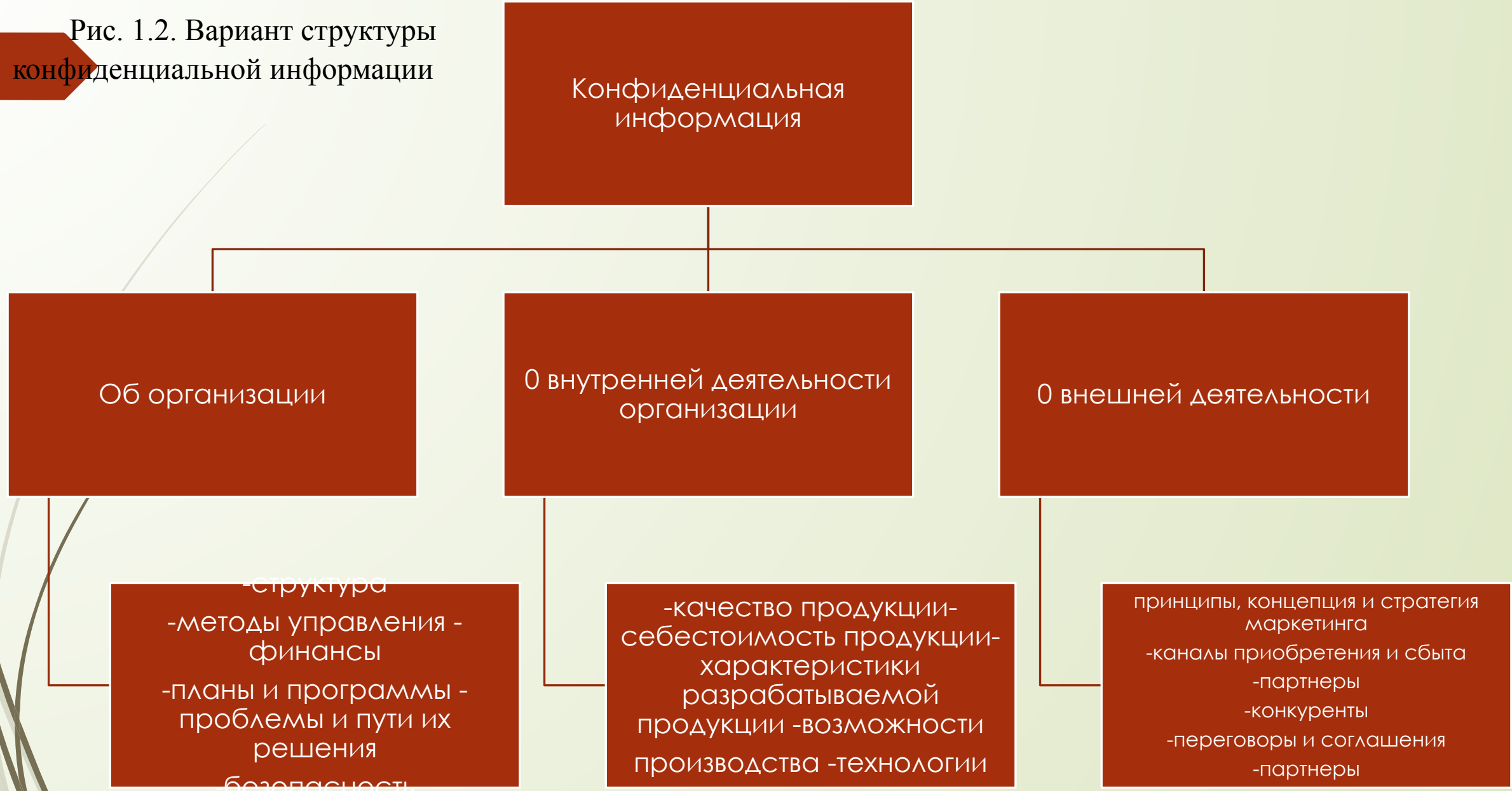
Рис. 1.1. Классификация информации, защищаемом техническими средствами



Структурирование информации проводится путем последовательной детализации защищаемой информации, начиная с перечней сведений, содержащих тайну. Детализация предусматривает иерархическое разбиение информации в соответствии со структурой тематических вопросов, охватывающих все аспекты организации и деятельности частной фирмы или государственной структуры.

Вариант укрупненной типовой структуры конфиденциальной информации, составляющей коммерческую тайну.

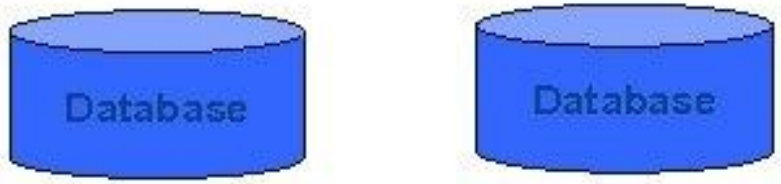
Рис. 1.2. Вариант структуры конфиденциальной информации



Два типа информации:

Структурированная 10-20%

Business Intelligence



Неструктурированная 80-90%

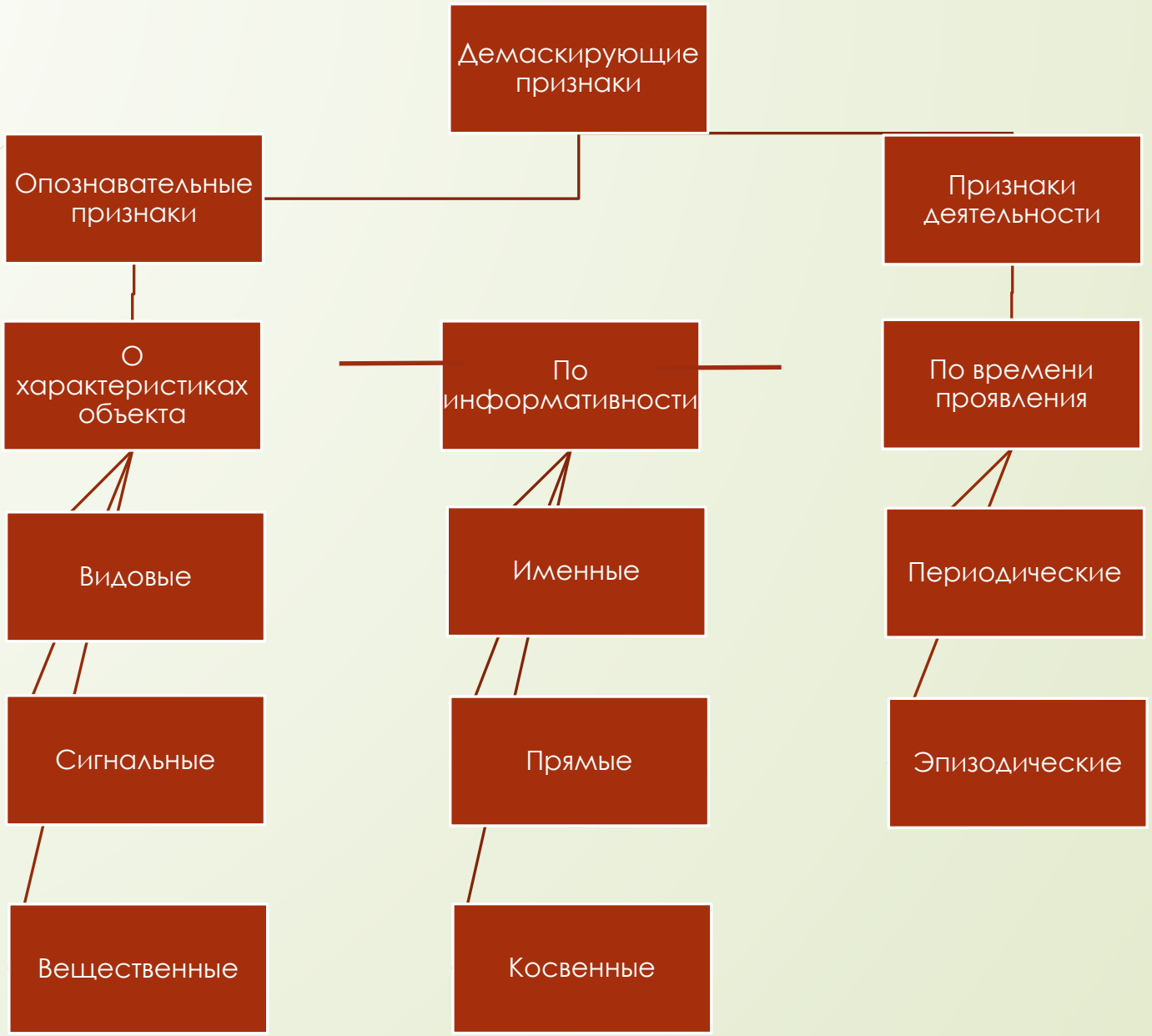
1.2. Демаскирующие информационные признаки объектов

- Задача **защиты признаковой информации** решается путем предотвращения обнаружения и распознавания объектов, содержащих эти признаки. Среди множества признаков, присущих конкретному объекту, существуют признаки, которые позволяют обнаруживать его среди других похожих объектов и распознать его **принадлежность, назначение, функции, свойства, особенности и характеристики**.
- Признаки, позволяющие отличить один объект от другого, называются **демаскирующими**. Демаскирующие признаки объекта составляют часть его признаков, а значения их отличаются от значений соответствующих признаков других объектов. Одинаковые признаки разных объектов не относятся к демаскирующим. Например, признак «рост человека» без указания его значения не является демаскирующим, так как он относится ко всем людям.

1.2.1. Классификация демаскирующих признаков

- Демаскирующие признаки объекта описывают его различные состояния, характеристики и свойства.
- В общем случае демаскирующие признаки объектов разделяются на опознавательные признаки и признаки деятельности. Опознавательные признаки описывают объекты в статическом состоянии: его назначение, принадлежность, параметры. Признаки деятельности объектов характеризуют этапы и режимы функционирования объектов, например, этапы создания новой продукции: научные исследования, подготовка к производству, изготовление новой продукции, ее испытания и т. д.

1.3. Классификация демаскирующих признаков



- Демаскирующие признаки характеристик объекта можно разделить на **3 группы**:

- **Видовые признаки** (форма, цвет, размеры, структура поверхности, составные части);
- **Признаки сигналов** (параметры полей и сигналов, излучаемых объектом - мощность, частоту, спектральную плотность, тип модуляции и т.д.);
- **Признаки веществ** (физические и химические характеристики).

По информативности демаскирующие признаки делят на:

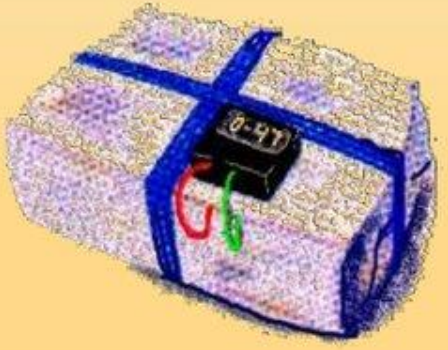
- Именные
- Прямые
- Косвенные

Демаскирующие признаки обнаружения взрывных устройств

ОБНАРУЖЕНИЕ ПРЕДМЕТОВ ДОМАШНЕГО ОБИХОДА (ЧАЩЕ ДОРОГОСТОЯЩИХ), ЯКОБЫ УТЕРЯННЫХ ИЛИ ЗАБЫТЫХ

- НАЛИЧИЕ НА ОБНАРУЖЕННОМ ПРЕДМЕТЕ ПРОВОДОВ, ИЗОЛЕНТЫ, ВЕРЕВОК

- ПОДОЗРИТЕЛЬНЫЕ ЗВУКИ (ЩЕЛЧКИ, ТИКАНЬЕ ЧАСОВ И Т.П.) ИЗДАВАЕМЫЕ ПРЕДМЕТОМ



- ОТ ПРЕДМЕТА ИСХОДИТ НЕОБЫЧНЫЙ ЗАПАХ

Демаскирующие признаки удаленных атак

- Повтор определенных действий (сканирование портов в поисках доступных сетевых сервисов, подбор пароля и др.)
- Неправильные или некорректные команды
- Несоответствующие параметры сетевого трафика (нестандартные комбинации бит, полуоткрытые соединения, признаки подмены адресов)
- Иные формы аномального поведения

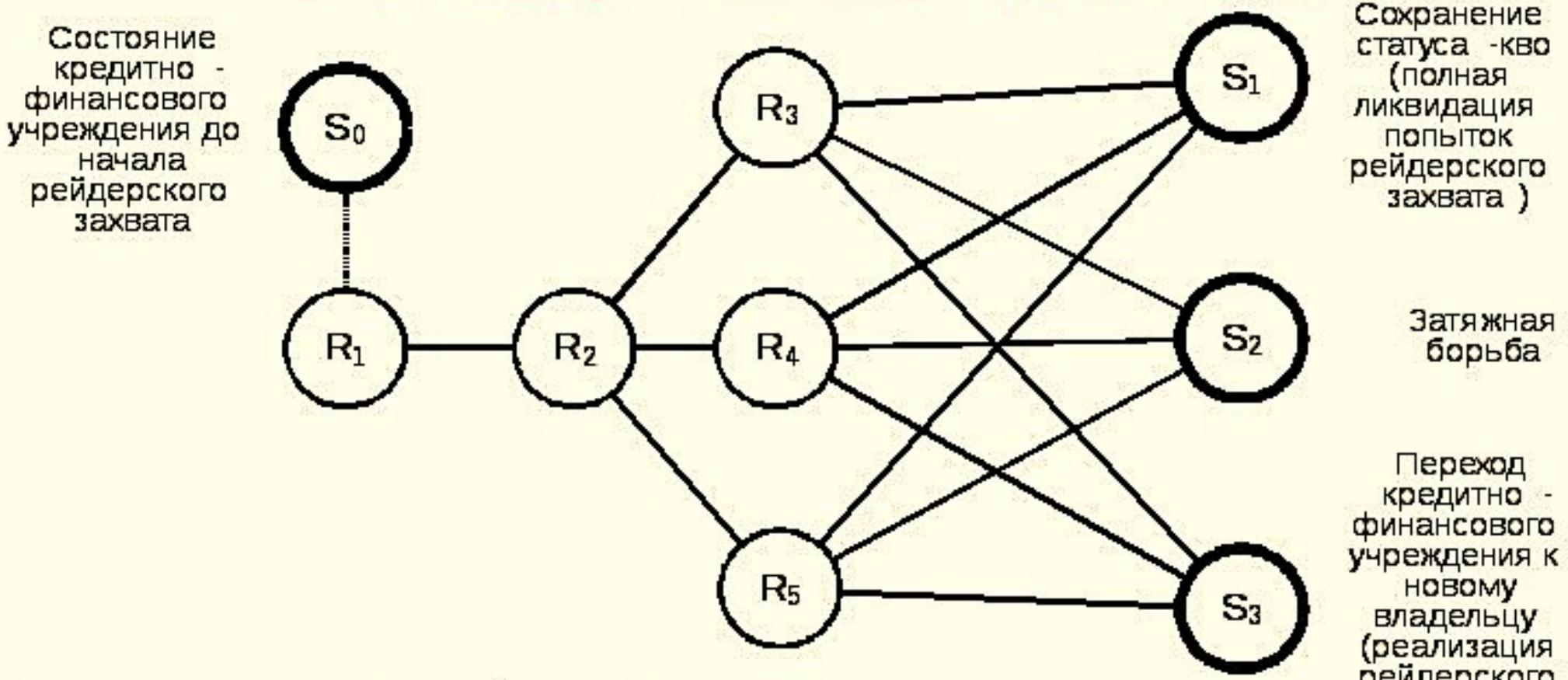
Демаскирующие признаки вредоносного кода

- Присутствие интерпретируемого кода в шаблонах, документах и временных файлах
- Замедление или неестественное выполнение операций при работе с файлами, текстом, таблицами, рисунками
- Генерация сообщений об ошибках при некорректном выполнении программы

Демаскирующие признаки электронных закладок

- Признаки внешнего вида – малогабаритный предмет неизвестного назначения
- Тонкий провод, проложенный от микрофона в другое помещение
- Наличие в предмете автономных источников питания (батарей, аккумуляторов)
- Наличие полупроводниковых элементов
- Наличие сосредоточенных источников модулированного радиоизлучения из помещения

АГРЕГИРОВАННАЯ ТНФОРМАЦИОННО-ПРИЗНАКОВАЯ (СЕТЕВАЯ) МОДЕЛЬ РЕЙДЕРСКОГО ЗАХВАТА КРЕДИТНО-ФИНАНСОВОГО УЧРЕЖДЕНИЯ



R_1 - принятие решения о рейдерском захвате;
R_2 - сбор информации о кредитно-финансовом учреждении;
R_3 - белый рейдерский захват;
R_4 - серый рейдерский захват;
R_5 - черный рейдерский захват.

Опознавательные демаскирующие признаки

Описываютстатические характеристикиобъектов:

- **Внешний вид** (цвет, форма, размер)
- **Излучение** (светимость, радиоактивность, электро-магнитное излучение)
- **Физические свойства** (масса, плотность, вязкость, проводимость)
- **Химические свойства** (химический состав, кислотность)

Демаскирующие признаки деятельности

Характеризуют *динамические свойства*объектов. Признаки деятельности представляют собой последовательность во времени событий или действий составных элементов рассматриваемого объекта и взаимодействующих с ним объектов (скорость, упругость ударов, изменения статистических свойств объекта во времени).

- Таким образом, совокупность демаскирующих признаков рассмотренных трех групп представляет собой **модель объекта**, описывающую его внешний вид, излучаемые им поля, внутреннюю структуру и химический состав содержащихся в нем веществ.
- Важнейшим показателем признака является его **информативность**. Информативность можно оценивать мерой в интервале [0-1], соответствующей значению вероятности обнаружения объекта по конкретному признаку. Чем признак более индивидуален, т. е. принадлежит меньшему числу объектов, тем он более информативен.
- Наиболее информативен именной признак, присущий только одному конкретному объекту. Такими признаками являются фамилия, имя, отчество человека, капиллярный узор его пальцев, инвентарный номер прибора или образца мебели. Факты, например, о совпадении капиллярных узоров пальцев разных людей не известны.
- Информативность остальных демаскирующих признаков, принадлежащих рассматриваемому объекту и называемых прямыми, колеблется в пределах [0-1]. Признаки, непосредственно не принадлежащие объекту, но отражающие свойства и состояние объекта, называются косвенными. Эти признаки являются, как правило, результатом взаимодействия рассматриваемого объекта с окружающей средой. К ним относятся, например, следы ног или рук человека, автомобиля и других движущихся объектов. Информативность косвенных признаков в общем случае ниже информативности прямых. Однако есть исключения, например информативность четких отпечатков пальцев соответствует информативности именных признаков.

- **По времени проявления признаки** могут быть:

- **Постоянные** - присущие объекту на всем протяжении его существования
- **Периодические** - проявляемые в определенные периоды времени (на некоторых этапах) существования объекта
- **Эпизодические** - проявляются при определенных условиях и могут не повторится на всем протяжении существования объекта

- **По времени проявления признаки** могут быть:

Набор признаков, принадлежащих объекту, образует его признаковую структуру **Хст Ее** можно представить в виде объединения всех демаскирующих признаков объектов:

- $X_{ct}(t) = \bigcup_{i=1}^{n} X_i^j(t),$
- где -j-ое значение i-го признака в момент времени t. В общем случае для описания объекта имеет значение не только количество и информативность признаков, но последовательность и время их проявления. Каждый i-ый признак обеспечивает возможность обнаружения объекта с вероятностью Pi. Если признаковая структура содержит n независимых признаков, то вероятност[illegible]ется до величины.

- **Постоянные** - присущие объекту на всем протяжении его существования
- **Периодические** - проявляемые в определенные периоды времени (на некоторых этапах) существования объекта
- **Эпизодические** - проявляются при определенных условиях и могут не повторится на всем протяжении существования объекта

- $Q_n = 1 - \prod_{i=1}^{n} 1 -$
- Н[illegible] вероятность обнаружения объекта хотя бы по одному из этих признаков существенно выше - более 0.14.
- Если признаки зависимы, т. е. проявление какого-либо признака статистически связано с проявлением другого, то вероятность обнаружения объекта уменьшается по сравнению с вариантом независимых признаков. Например, значения признака «тень» при наблюдении объекта зависит от значения признака «размеры» и от взаимного пространственного положения объекта и внешнего источника света.
- В общем случае признаковая структура представляет собой набор независимых или зависимых признаков, о которых достоверно известно, что они относятся к рассматриваемому объекту.

Информативность признаков

x/y	a	b	c	d	e	f	g	h	
0	m_{00}	m_{01}	m_{02}	m_{03}	m_{04}	m_{05}	m_{06}	m_{07}	m_0
1	m_{10}	m_{11}	…					…	m_1
2	…	…							m_2
3	…	…							m_3
4	m_{40}	m_{41}	…					…	m_4
	n_0	n_1	n_2	n_3	n_4	n_5	n_6	n_7	M

$$H_x = -\sum_i \frac{m_i}{M} \log \frac{m_i}{M}$$

$$H_y = -\sum_j \frac{n_j}{M} \log \frac{n_j}{M}$$

$$H_{x \otimes y} = -\sum_i \sum_j \frac{m_{ij}}{M} \log \frac{m_{ij}}{M}$$

$$H_{x:y} = H_x + H_y - H_{x \otimes y}$$

$$S_{x:y} = H_{x:y} * 2 \Big/ \left(H_x + H_y \right)$$

СПЕЦИАЛИЗИРОВАННАЯ ЛАБОРАТОРИЯ «ПОИСК И ВЫЯВЛЕНИЕ ДЕМАСКИРУЮЩИХ ПРИЗНАКОВ ЭУНПИ»

ОТПРАВИТЬ ЗАЯВКУ

Назначение лаборатории: обеспечивает возможности получения слушателями теоретических знаний и практических навыков по следующим направлениям:

- физические основы, структурная модель и общая характеристика основных видов электронных ЗУ;
- организация работ по обследованию помещений;
- основные этапы проведение поисковых мероприятий и их особенности;
- проведение поисковых мероприятий в учебных классах «Радиомониторинга», «Проводной локации» и «Нелинейной локации»:
- с использованием технических средств радиомониторинга по выявлению радиоизлучающих ЗУ и ЗУ, использующих для передачи информации ИК-канал;
- с использованием средств контроля проводных коммуникаций по выявление ЗУ, использующих для передачи информации проводные коммуникации;
- с использованием нелинейного локатора по выявлению ЗУ, в составе которых есть элементы, обладающие нелинейной вольтамперной характеристикой;
- выявление посторонних внедрений во внутренние структуры ограждающих конструкций и предметов интерьера помещений, указывающих на наличие ЗУ;
- особенности выявления металлических включений, указывающих на наличие ЗУ;
- визуально-оптический контроль с использованием средств визуального контроля;
- анализ выявленных по результатам поиска демаскирующих признаков ЗУ;
- создание комплекса организационно-технических мероприятий в рамках создания и сопровождения комплексной системы защиты информации на объекте;
- проведение периодического инструментального контроля эффективности мер защиты информации, контроля работоспособности отдельных элементов комплексной системы защиты информации.

СОСТАВ ЛАБОРАТОРИИ

Поисковое оборудование	
ST-107 (индикатор поля, 50-2500МГц, обнаружение сигналов GSM, DECT, BLUETOOTH, WLAN, 802.1g)	1
ST 03.Test (контрольное устройство, имитатор сигналов универсальный)	3
РИЧ-8 (MFP-8000) (индикатор поля, 200кГц-8ГГц, регулировка чувств., индик.: ЖКИ, звук.; режим: поиск, мониторинг)	1
OSCOR Green OGR-24 (портативный анализатор для оперативного радиоконтроля)	1
NR-900EMS (профессиональный нелинейный радиолокатор)	1
ST 131 «ПИРАНЬЯ II» (многофункциональное поисковое устройство)	1
АКА-7215М (ручной селективный металлодетектор, для выявления включений металла, режим селекции цветных и черных металлов, высокая чувствительность)	1
Поиск-2У (досмотровый комплект, 6 зеркал, комплект щупов, чехол)	1
Parat (комплект инструментов)	
Оптик-2 (оптический обнаружитель скрытых видеокамер, бинокуляр)	1
TALAN DPA-7000 (Цифровой анализатор проводных линий. Анализ и тестирование цифровых телефонных линий на наличие устройств негласного съема информации)	1

Выставка демонстрационного оборудования	
NR-mu (муляж)	1
ST-107 (детектор электромагнитного поля, 50-7000МГц)	1
ST-165 (селективный обнаружитель цифровых радиопередающих устройств)	1