Основные определения
Информационной безопасности

На определенном этапе развития информационной индустрии рождается **информационное общество**, в котором большинство работающих занято производством, хранением, переработкой и реализацией информации, т.е. творческим трудом, направленным на развитие интеллекта и получение знаний. Создается единое, не разделенное национальными границами информационное сообщество людей.

Информационная война - информационное противоборство с целью нанесения ущерба важным структурам противника, подрыва его политической и социальной систем, а также дестабилизации общества и государства противника.

Информационное противоборство - форма межгосударственного соперничества, реализуемая посредством оказания информационного воздействия на системы управления других государств и их вооруженных сил, а также на политическое и военное руководство и общество в целом, информационную инфраструктуру и средства массовой информации этих государств для достижения выгодных для себя целей при одновременной защите от аналогичных действий от своего информационного пространства.

Информационная преступность - проведение информационных воздействий на информационное пространство или любой его элемент в противоправных целях. Как ее частный вид может рассматриваться информационный терроризм, то есть деятельность, проводимая в политических целях.

Информационное воздействие - акт применения информационного оружия.

Под **угрозой безопасности информации** понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Рис. 1 Структура понятия «Информационная безопасность»

Рис. 2 Действия и события, нарушающие информационную безопасность

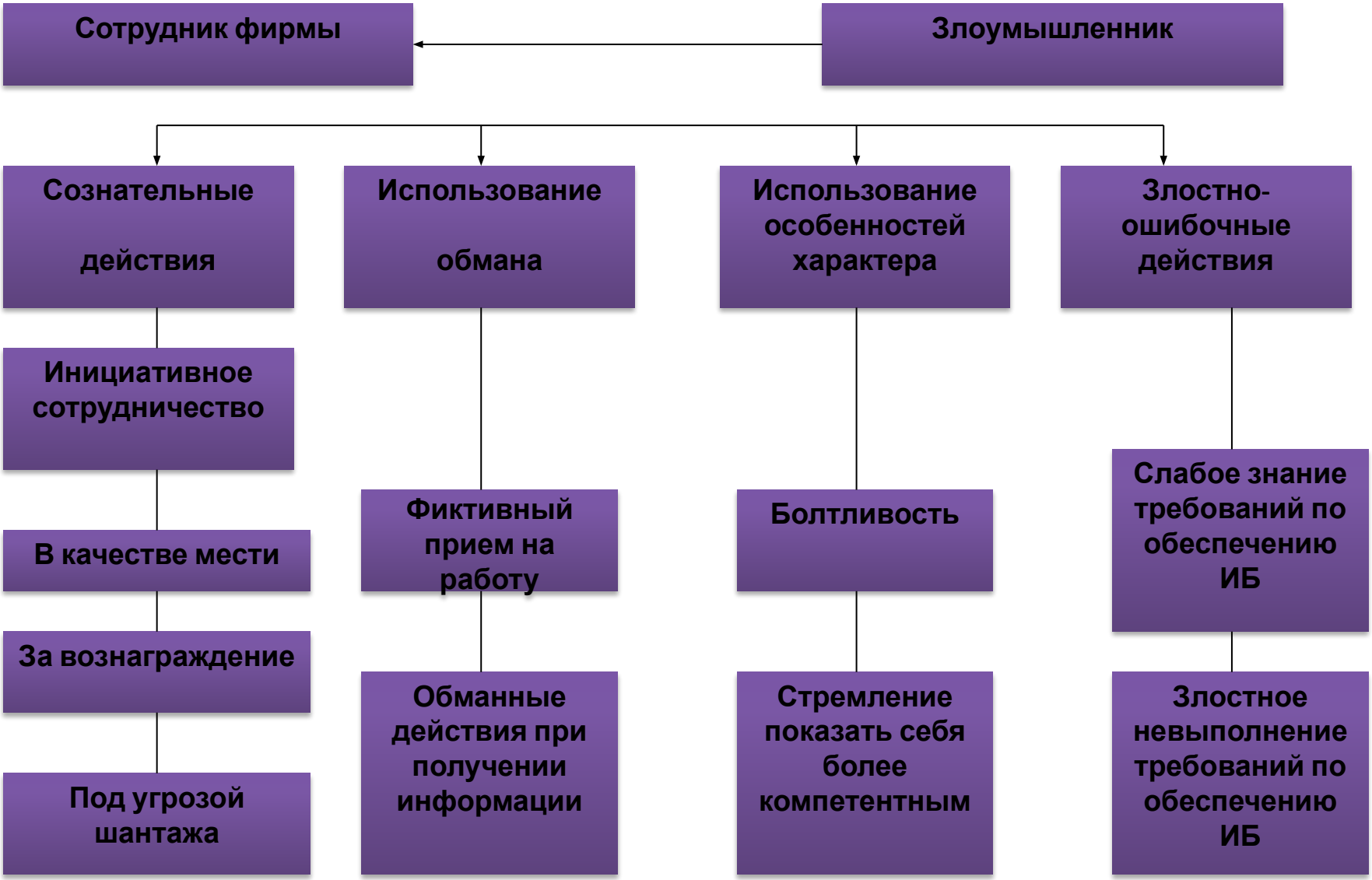


Рис. 3 Личностно-профессиональные характеристики и действия сотрудников, способствующие реализации угроз информационной безопасности

Среда обитания:	Сетевые	Распространяются по компьютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Рис. 4 Основные классы вирусов

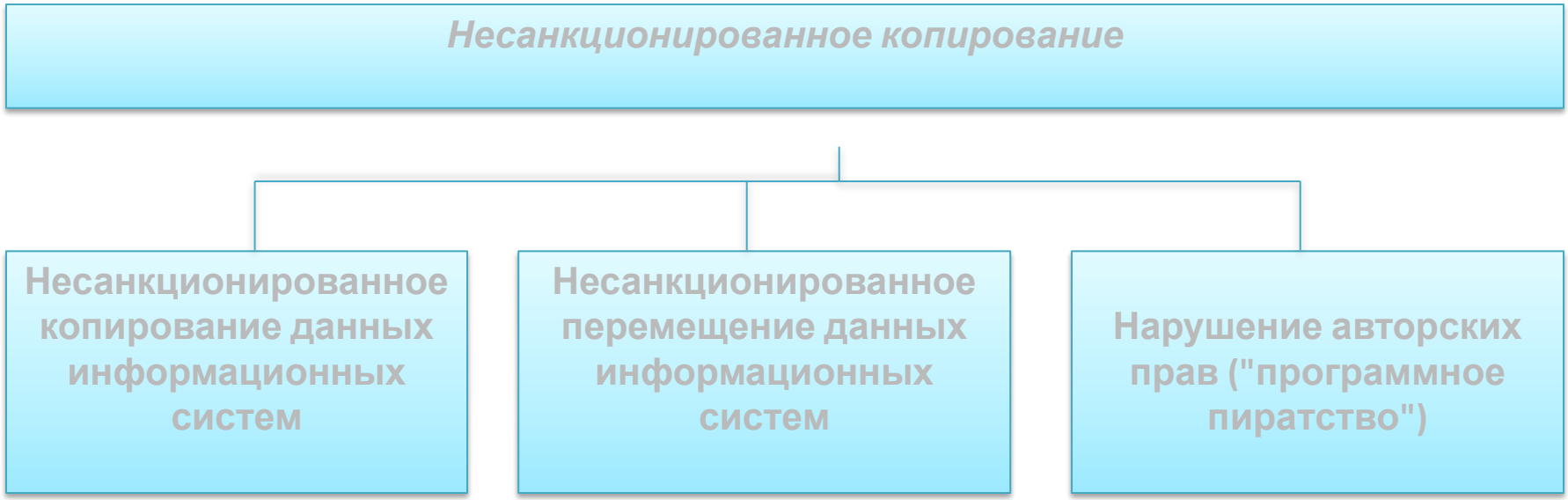
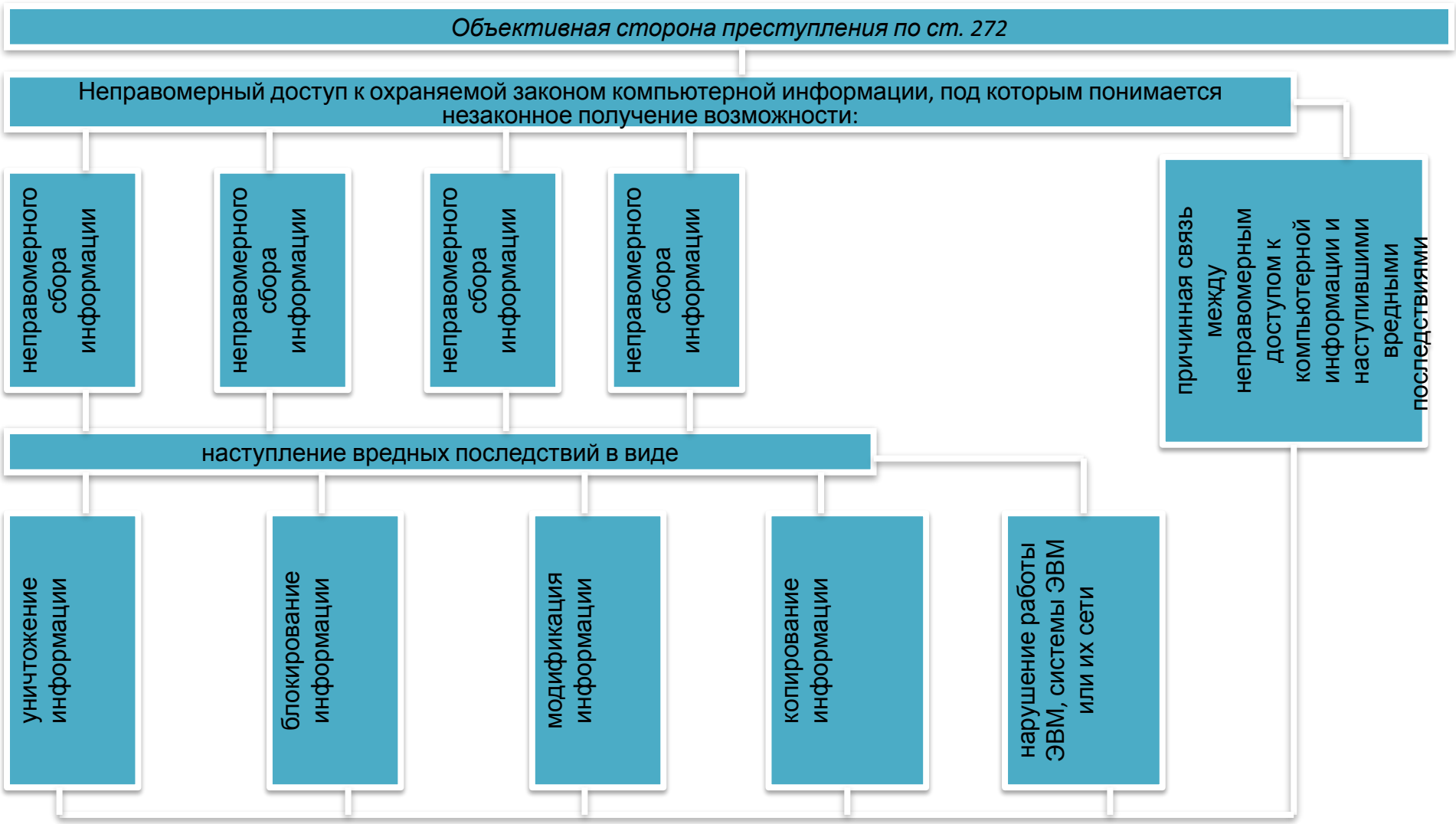


Рис.5 Копированием информации

Рис.6 Перехват информации


Объективная сторона преступления по ст. 272
Неправомерный доступ к охраняемой законом компьютерной информации, под которым понимается незаконное получение возможности:
неправомерного сбора информации
неправомерного сбора информации
неправомерного сбора информации
неправомерного сбора информации
причинная связь между неправомерным доступом к компьютерной информации и наступившими вредными последствиями
наступление вредных последствий в виде
уничтожение информации
блокирование информации
модификация информации
копирование информации
нарушение работы ЭВМ, системы ЭВМ или их сети

Отягчающие обстоятельства, предусмотренные ч.2 ст.272

Совершение преступления группой лиц по предварительному сговору т.е. с участием лиц, заранее договорившихся о совместном совершении преступления

Совершение преступления организованной группой лиц, т.е. устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений (ч.3 ст.35 УК РФ)

Совершение преступления лицом с использованием своего служебного положения либо лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, т.е. виновный получает доступ к компьютерной информации, незаконно используя права, предоставл ему в силу выполн. им служеб. деятельности

Рис.8 Отягчающие обстоятельства, предусмотренные

Рис.9 Объективная сторона преступления

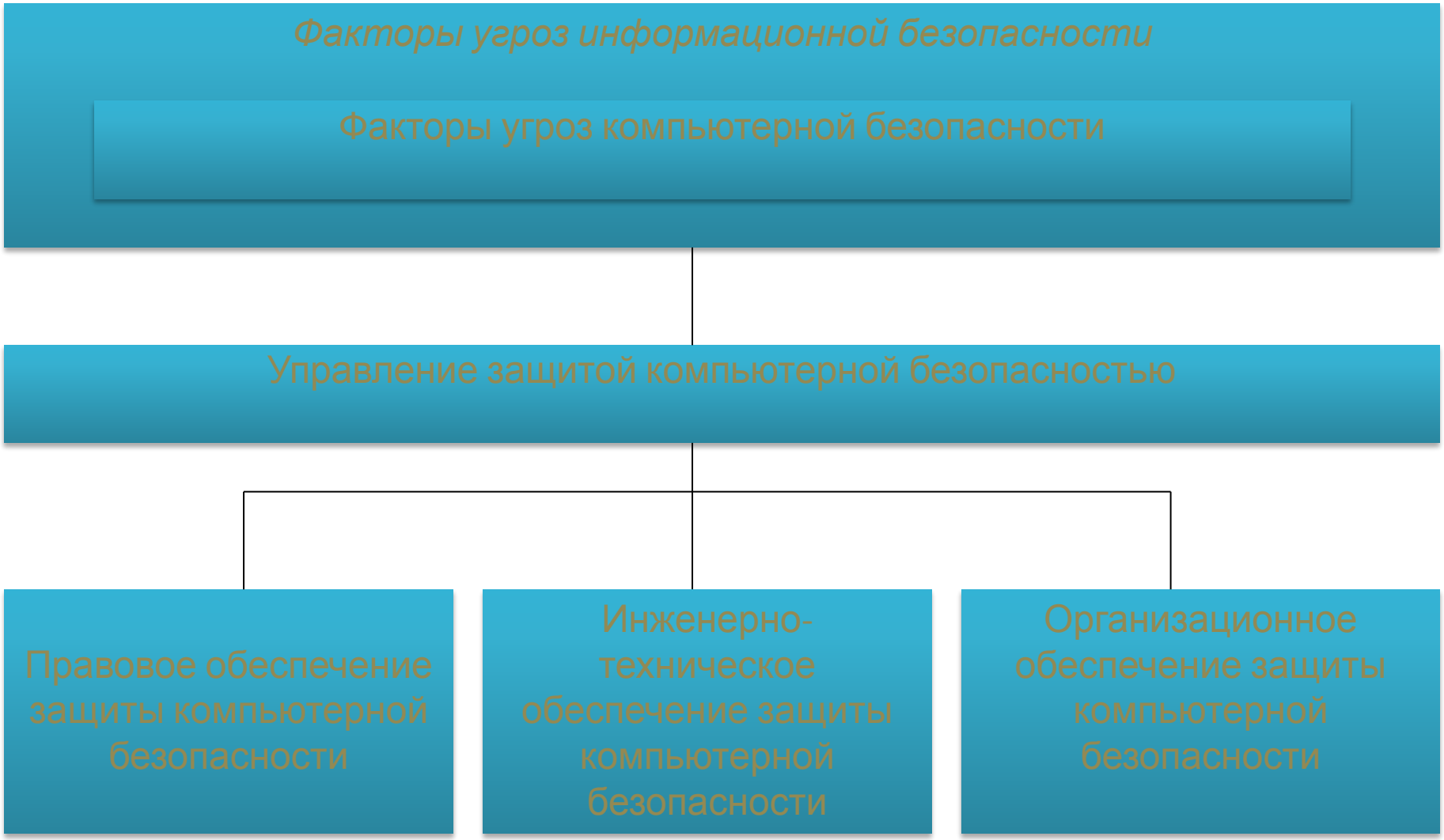

Факторы угроз информационной безопасности
Факторы угроз компьютерной безопасности
Управление защитой компьютерной безопасностью
Правовое обеспечение защиты компьютерной безопасности
Инженерно-техническое обеспечение защиты компьютерной безопасности
Организационное обеспечение защиты компьютерной безопасности

Рис. 10

Рис.11 Управление защитой информации

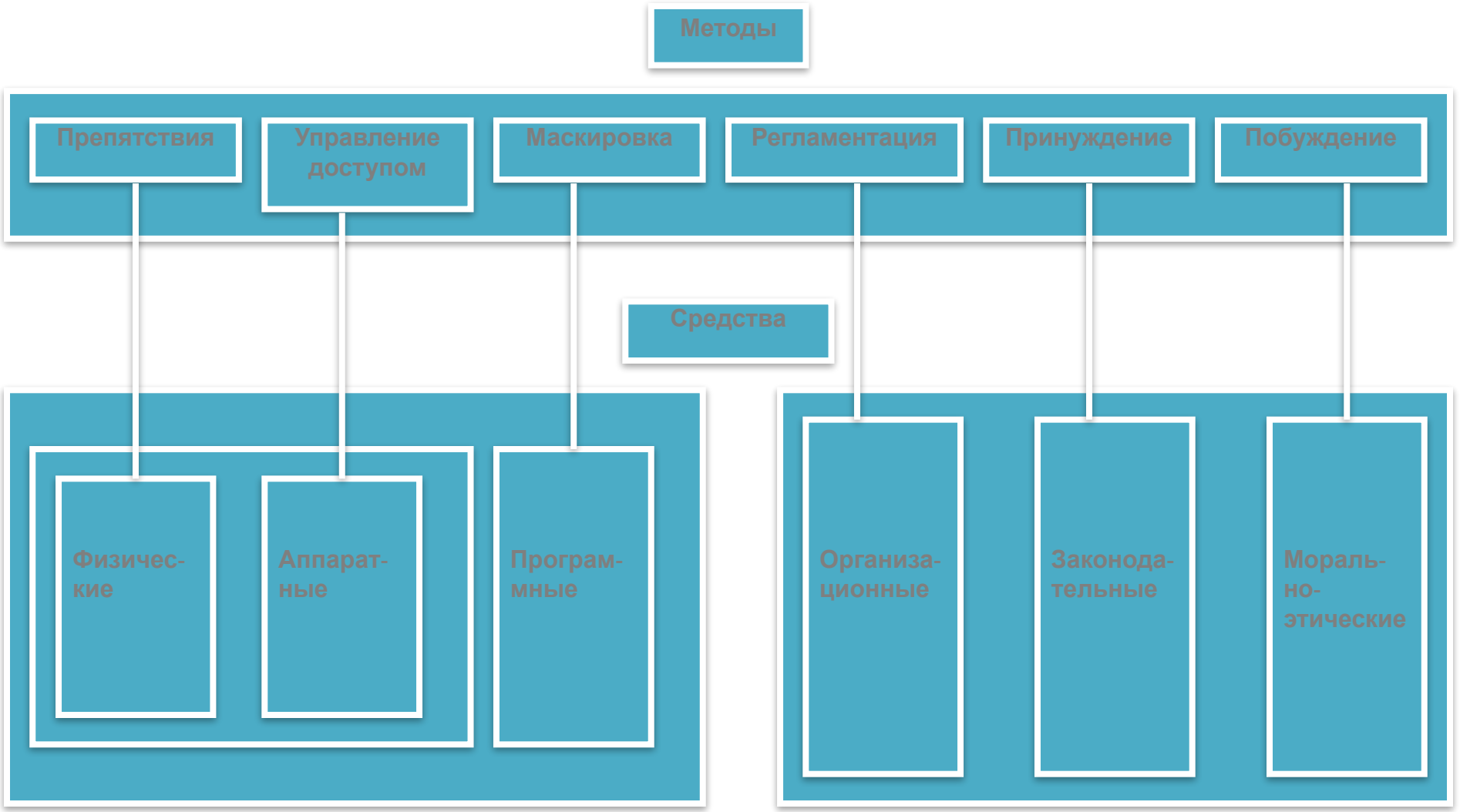


Рис. 12 Методы и средства информационной безопасности экономического объекта