**Лекция 1:**

**Концепции и аспекты обеспечения информационной безопасности**

**Аннотация:**Понятия экономической и информационной безопасности. Ключевые вопросы ИБ. Виды угроз информационной безопасности и классификация источников угроз. Основные виды защищаемой информации. Правовое обеспечение информационной безопасности. Основные аспекты построения системы информационной безопасности.

**Понятия экономической и информационной безопасности. Ключевые вопросы ИБ**

*Информация* давно перестала быть просто необходимым для производства материальных ценностей вспомогательным ресурсом — она приобрела ощутимый стоимостный *вес*, который четко определяется реальной прибылью, получаемой при её использовании, или размерами ущерба, наносимого владельцу информации. Создание технологий и индустрии сбора, переработки, анализа информации и её доставки конечному пользователю порождает ряд сложных проблем. Одной из таких проблем является надежное обеспечение сохранности и установленного статуса информации (актуальности, полноты, непротиворечивости, конфиденциальности), циркулирующей и обрабатываемой в информационно-вычислительных системах и сетях, а также *безопасность* самих систем и технологий.

Современное развитие информационных технологий и, в частности, технологий *Internet*/Intranet, приводит к необходимости защиты информации, передаваемой в рамках распределенной корпоративной сети, использующей сети открытого доступа. При использовании своих собственных закрытых физических каналов доступа эта проблема так остро не стоит, так как в эту *сеть* закрыт *доступ* посторонним. Однако выделенные каналы может себе позволить далеко не любая компания. Поэтому приходится довольствоваться тем, что есть в распоряжении компании. А есть чаще всего *Internet*. Поэтому приходиться изобретать способы защиты конфиденциальных данных, передаваемых по фактически незащищенной сети.

*Безопасность* информационных технологий (ИТ) и систем (ИС) является одной из важнейших составляющих проблемы обеспечения экономической безопасности организации. Переход к новым формам государственного и хозяйственного управления экономикой в России в условиях дефицита и противоречивости правовой базы породил *целый* комплекс проблем в области защиты данных, информации, знаний и самих ИКТ. Это и своеобразие становления рыночных отношений, и отсутствие обоснованных концепций реформ, и отставание в области применения современных информационных технологий в управлении и производстве. Обострение этих проблем выдвинули на первый план вопросы обеспечения национальной, социальной и корпоративной безопасности, в том числе и в информационной сфере.

В 1983 году министерство обороны США выпустило "Оранжевую книгу" — "Критерии оценки надежных компьютерных систем" ["Trusted *Computer* *System* *Evaluation* *Criteria* (*TCSEC*)". — USA, *Department* of Defense, 5200.28-STD, 1993], положив тем самым начало систематическому формированию знаний об информационной безопасности (ИБ) за пределами правительственных ведомств.

Во второй половине 1980-х годов аналогичные по назначению документы были изданы в ряде европейских стран [*Information Technology* *Security* *Evaluation* *Criteria* (*ITSEC*). Harmonised *Criteria* of France-Germany-Netherlands-United Kingdom. — *Department* of Trade *and* *Industry*, London, 1991].

В 1992 году в России Государственная техническая комиссия при Президенте РФ (Гостехкомиссия РФ) издала серию документов, посвященных проблеме защиты от несанкционированного доступа.

"*Оранжевая книга*" и последующие подобные издания были ориентированы в первую *очередь* на корпоративных разработчиков программного обеспечения и информационных систем, а не на пользователей или системных администраторов. Динамичное развитие вычислительной техники, компьютерных технологий и широкое применение их в бизнесе показало, что информационная *безопасность* является одним из важнейших аспектов интегральной безопасности на всех уровнях — национальном, корпоративном или персональном. Для иллюстрации можно привести несколько примеров.

В 2012 году в США был опубликован годовой отчет "Компьютерная преступность и *безопасность*: проблемы и тенденции" ("Issues *and* Trends: 2012 CSI/FBI *Computer Crime* *and* *Security* Survey"). В отчете отмечается увеличивающийся рост числа компьютерных преступлений (39% из числа опрошенных). *Информационные системы* 28% респондентов были взломаны внешними злоумышленниками. Атакам через *Internet* подвергались 77%, в 59% случаев отмечались нарушения со стороны собственных сотрудников. В большом числе компаний (31%) вообще не следили за состоянием безопасности своих компьютерных и сетевых систем, полагаясь на защитные модули компьютерных программ и приложений. В аналогичном отчете, опубликованном в апреле 2013 года, тенденция осталась прежней:

* 90% опрошенных (преимущественно из крупных компаний и правительственных структур) сообщили, что за последние 12 месяцев в их организациях имели место нарушения информационной безопасности;
* 78% констатировали значительные финансовые потери от этих нарушений;
* 49% оценили потери количественно — их общая сумма составила более 640 млн. долларов.

Согласно результатам совместного исследования Института информационной безопасности США и ФБР, в 2012 году *ущерб* от компьютерных преступлений достиг более 900 миллионов долларов, что на 34% больше, чем в 2011 году. Каждое компьютерное преступление наносит *ущерб* примерно в 200-300 тысяч долларов. Потери крупнейших компаний, вызванные компьютерными вторжениями, продолжают увеличиваться, несмотря на рост затрат на средства обеспечения безопасности ("*Internet* Week", 2013 г.).

Наибольший *ущерб*, по исследованиям Gartner *Group*, нанесло манипулирование доступом во внутреннее информационное *пространство*: кражи данных и информации из корпоративных сетей и баз данных, подмена информации, подлоги документов в электронном виде, промышленный шпионаж. Наряду с возрастанием числа внешних атак в последние годы отмечается резкий рост распространения вирусов через *Интернет*.

Однако, увеличение числа атак и распространение вирусов еще не самая большая неприятность — постоянно обнаруживаются новые уязвимые места в программном обеспечении. В информационных письмах Национального центра защиты инфраструктуры США (National *Infrastructure* *Protection* *Center* USA — *NIPC*) сообщается, что за период с 2000 по 2012 годы выявлено несколько десятков существенных проблем с программным обеспечением, риск использования которых оценивается как средний или высокий. Среди "пострадавших" операционных платформ — почти все разновидности ОС Unix, *Windows*, *Mac* OS, .*NET*. В таких условиях специалисты и системы информационной безопасности должны уметь противостоять внешним и внутренним угрозам, выявлять проблемы в системах защиты программного обеспечения и на основе соответствующей политики вырабатывать адекватные меры по компенсации угроз и уменьшению рисков.

При анализе проблематики, связанной с информационной безопасностью (ИБ), необходимо учитывать специфику данного аспекта безопасности, состоящую в том, что информационная *безопасность* есть составная часть разработки, внедрения и эксплуатации информационных систем и технологий — области, развивающейся беспрецедентно высокими темпами.

К сожалению, современная технология программирования не позволяет создавать полностью безошибочные и безопасные программы. Поэтому следует исходить из того, что необходимо создавать надежные системы ИБ с привлечением не стопроцентно надежных программных компонентов (программ)!

В принципе, это возможно, но требует соблюдения определенных принципов архитектурного построения программных комплексов и контроля состояния защищенности программно-аппаратного обеспечения, телекоммуникационных устройств и сетей на всем протяжении жизненного *цикла* ИС.

**Экономическая и информационная безопасность. Составляющие информационной безопасности**

Для чего необходимы знания по основам информационной безопасности? Как строить безопасные, надежные системы и сети? Как поддерживать режим безопасности информации в системах и сетях? Бурное развитие техники, новейших компьютерных технологий и широкое применение их в бизнесе показало, что информационная безопасность является одним из важнейших аспектов интегральной безопасности, на каком бы уровне ни рассматривать эту проблему — национальном, корпоративном или персональном.

Необходимость реализации, сопровождения и развития систем ИБ — это оборотная сторона широкого использования информационных технологий, так как наступление нового этапа развития ИТ закономерно приводит к быстрому падению уровня информационной безопасности ([рис. 1.1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=1#image.1.1)).



**Рис. 1.1.**Изменение уровня информационной безопасности в соответствии с уровнем развития ИТ

Отметим ещё одну существенную — можно сказать парадоксальную — особенность развития информационных технологий: технологии постоянно усложняются, однако квалификация нарушителей и злоумышленников понижается ([рис. 1.2](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=1#image.1.2)). Это происходит оттого, что новые средства создания программного кода и сетевые технологии изначально строятся так, чтобы они были доступны пользователям, не обладающим высокой профессиональной подготовкой.



**Рис. 1.2.**Соотношение возрастания сложности ИТ и квалификации злоумышленников

В "Доктрине информационной безопасности Российской Федерации" защита от несанкционированного доступа к информационным ресурсам, обеспечение безопасности информационных и телекоммуникационных систем выделены в качестве важных составляющих национальных интересов РФ в информационной сфере. К настоящему времени сложилась общепринятая точка зрения на концептуальные основы ИБ. Суть ее заключается в том, что подход к обеспечению ИБ должен быть комплексным, сочетающим меры следующих уровней:

* законодательного — федеральные и региональные законы, подзаконные и нормативные акты, международные, отраслевые и корпоративные стандарты;
* административного — действия общего и специального характера, предпринимаемые руководством организации;
* процедурного — меры безопасности, закрепленные в соответствующих методологиях и реализуемые ответственными менеджерами и персоналом предприятия;
* научно-технического — конкретные методики, программно-аппаратные, технологические и технические меры.

Главными принципами обеспечения безопасности в соответствии с законом РФ "О безопасности" являются: законность, соблюдение баланса жизненно важных интересов личности, общества и государства, взаимная ответственность перечисленных субъектов, интеграция системы безопасности в рамках компании, общества, государства, взаимодействие с международными системами безопасности.

Экономическая безопасность предпринимательской деятельности и хозяйствующего субъекта можно определить как "защищенность жизненно важных интересов государственного или коммерческого предприятия от внутренних и внешних угроз, защиту кадрового и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, которая обеспечивается системой мер правового, экономического, организационного, информационного, инженерно-технического и социального характера" [Грунин О. А., Грунин С. О., 2002].

Стратегия обеспечения экономической безопасности Российской Федерации строится на основании официально действующих правовых и нормативных актов, основными из которых являются:

* Конституция Российской Федерации;
* Закон "О безопасности" от 5 марта 1992 г. с изменениями и дополнениями от 25 декабря 1992 г.;
* Государственная стратегия экономической безопасности РФ (Основные положения), одобренная Указом Президента РФ № 608 от 29 апреля 1996 г.;
* Концепция национальной безопасности Российской Федерации, введенная Указом Президента РФ № 24 от 10 января 2000 г.

Исходя из необходимости достижения целей обеспечения экономической безопасности предпринимательской деятельности, можно выделить следующие основные проблемные направления:

* организацию эффективной защиты материальной, финансовой и интеллектуальной собственности,
* защиту информационных ресурсов предприятия,
* эффективное управление ресурсами и персоналом.

В современных условиях коммерческий успех любого предприятия в большой степени зависит от оперативности и мобильности бизнеса, от своевременности и быстроты принятия эффективных управленческих решений. А это невозможно без надежного и качественного информационного взаимодействия между различными участниками бизнес-процессов. Сегодня предприятия в качестве среды для информационного обмена все чаще используют открытые каналы связи сетей общего доступа (Internet) и внутреннее информационное пространство предприятия (Intranet). Открытые каналы Internet/Intranet намного дешевле по сравнению с выделенными каналами. Однако сети общего пользования имеют существенный недостаток — открытость и доступность информационной среды. Компании не могут полностью контролировать передачу и приём данных по открытым каналам и при этом гарантировать их целостность и конфиденциальность. Злоумышленникам не составляет особого труда перехватить деловую информацию с целью ознакомления, искажения, кражи и т. п.



**Рис. 1.3.**Общая структура информационной безопасности

Информационная безопасность. В общем случае ИБ можно определить как "защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений — производителям, владельцам и пользователям информации и поддерживающей инфраструктуре" [Галатенко В. А., 2006].

Информационная безопасность не сводится исключительно к защите от несанкционированного доступа к информации — это принципиально более широкое понятие, включающее защиту информации, технологий, систем, материальных и нематериальных активов и персонала ([рис. 1.3](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=1#image.1.3)).

Требования по обеспечению безопасности в различных аспектах информационной деятельности могут существенно отличаться, однако они всегда направлены на достижение следующих трёх основных составляющих информационной безопасности ([рис. 1.4](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=1#image.1.4)):



**Рис. 1.4.**Основные составляющие информационной безопасности

* целостность — это, в первую очередь, актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения: данные и информация, на основе которой принимаются решения, должны быть достоверными, точными и защищенными от возможных непреднамеренных и злоумышленных искажений;
* конфиденциальность — засекреченная информация должна быть доступна только тому, кому она предназначена: такую информацию невозможно получить, прочитать, изменить, передать, если на это нет соответствующих прав доступа;
* доступность (готовность) — это возможность за приемлемое время получить требуемую информационную услугу: данные, информация и соответствующие службы, автоматизированные сервисы, средства взаимодействия и связи должны быть доступны и готовы к работе всегда, когда в них возникает необходимость.

Деятельность по обеспечению информационной безопасности направлена на то, чтобы не допустить, предотвратить или нейтрализовать:

* несанкционированный доступ к информационным ресурсам (НСД, Unauthorized Access — UAA);
* искажение, частичную или полную утрату конфиденциальной информации;
* целенаправленные действия (атаки) по разрушению целостности программных комплексов, систем данных и информационных структур;
* отказы и сбои в работе программно-аппаратного и телекоммуникационного обеспечения.

Для большинства государственных и коммерческих организаций вопросы защиты от несанкционированного доступа и сохранности данных и информации имеют более высокий приоритет, чем проблемы локальных неисправностей компьютерного и сетевого оборудования. Напротив, для многих открытых организаций (общественных, учебных) защита от несанкционированного доступа к информации стоит по важности отнюдь не на первом месте. Таким образом, правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений и интересов этих субъектов, связанных с использованием информационных технологий и систем (ИТ/ИС).

**Ключевые вопросы информационной безопасности**

Современное развитие информационных технологий и, в частности, технологий Internet/Intranet, приводит к необходимости всесторонней защиты информационных технологий и систем, данных и информации, передаваемой в рамках распределенной корпоративной сети, использующей внутренние и внешние сети открытого доступа.

Оценка реальной ситуации сводится в большинстве случаев к ответу на следующие ключевые вопросы, составляющие системную основу обеспечения информационной безопасности:

* надо ли защищаться и что следует защищать?
* от кого надо защищаться?
* от чего надо защищаться?
* как надо защищаться?
* что обеспечит эффективность защиты?
* во что обойдется разработка, внедрение, эксплуатация, сопровождение и развитие систем защиты?



**Рис. 1.5.**Ключевые вопросы информационной безопасности

Первые три вопроса непосредственным образом относятся к проблеме оценки реальных угроз ([рис. 1.5](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=2#image.1.5)) [Лукацкий А. В., 2007].

**Надо ли защищаться и что следует защищать?**

Ответов на этот вопрос неоднозначен — многое зависит от структуры, области деятельности и целей компании. Для одних первоочередной задачей является предотвращение утечки информации (маркетинговых планов, перспективных разработок, величина и распределение прибыли и т.д.) к конкурентам. Другие могут пренебречь конфиденциальностью своей информации и сосредоточить свое внимание на ее целостности (например, для научно-исследовательских организаций, имеющих открытые Web-серверы). Для провайдера Internet-услуг, оператора связи или общедоступного справочного сервера на первое место поднимается задача обеспечения максимальной доступности и безотказной работы корпоративных информационных систем — первейшей задачей является именно обеспечение безотказной работы всех (или наиболее важных) узлов своей информационной системы. Расставить такого рода приоритеты и определить необходимость и объекты защиты можно только в результате анализа деятельности компании.

При интеграции индивидуальных и корпоративных информационных систем и ресурсов в единую информационную инфраструктуру определяющим фактором является обеспечение должного уровня информационной безопасности для каждого субъекта, принявшего решение войти в это пространство. В едином информационном пространстве должны быть созданы все необходимые предпосылки для установления подлинности пользователя (субъекта), подлинности содержания и подлинности сообщения (т.е. созданы механизмы и инструмент аутентификации). Таким образом, должна быть создана система информационной безопасности, которая включает необходимый комплекс мероприятий и технических решений по защите:

* от нарушения функционирования информационного пространства путем исключения воздействия на информационные каналы и ресурсы;
* от несанкционированного доступа к информации путем обнаружения и ликвидации попыток использования ресурсов информационного пространства, приводящих к нарушению его целостности;
* от разрушения встраиваемых средств защиты с возможностью доказательства неправомочности действий пользователей и обслуживающего персонала;
* от внедрения программных "вирусов" и "закладок" в программные продукты и технические средства.

Особо следует отметить задачи обеспечения безопасности разрабатываемых и модифицируемых систем в интегрированной информационной среде, т. к. в процессе модификации неизбежно возникновение дополнительных ситуаций незащищенности системы. Для решения этой проблемы наряду с общими методами и технологиями следует отметить введение ряда требований к разработчикам, создания регламентов внесения изменений в системы, а также использования специализированных средств.

**От кого надо защищаться?**

В абсолютном большинстве случаев ответом на этот вопрос является фраза: "Как от кого - конечно, от хакеров!". Исследования показали, что, по мнению большинства российских предпринимателей, основная опасность исходит от внешних злоумышленников, которые проникают в компьютерные системы банков и корпораций, перехватывают управление бизнес-процессами, "взламывают" сайты, запускают "троянских коней". Такая опасность существует и нельзя её недооценивать. В системах информационной защиты обязательно должны быть соответствующие модули защиты от внешних угроз подобного рода.



**Рис. 1.6.**Ранжированные ИТ-угрозы

Но эта опасность часто преувеличена. До 75-85% всех компьютерных угроз и преступлений связаны с внутренними нарушениями, т.е. осуществляются действующими или уволенными сотрудниками компании. По исследованиям 2013 года в 82% случаев источником реальных атак были сотрудники компаний. Для сравнения: хакеры, атакующие корпоративные сети извне, оказывались источником атак в 73% случаев. На [рис. 1.6](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=2#image.1.6) показаны усредненные данные по ранжированию ИТ-угроз за последние три года.

В публикациях достаточно примеров, когда сотрудник компании, считая, что его на работе не ценят, совершает компьютерное или информационное преступление, приводящее к многомиллионным убыткам. Нередки случаи, когда после увольнения бывший сотрудник компании в течение долгого времени пользуется корпоративным доступом в Internet. При увольнении этого сотрудника никто не подумал о необходимости отмены его пароля на доступ к данным и ресурсам, с которыми он работал в рамках своих служебных обязанностей. Если администрирование доступа поставлено плохо, то часто никто не замечает, что бывшие сотрудники пользуются доступом в Internet и могут наносить ущерб своей бывшей компании. Спохватываются лишь тогда, когда замечают резко возросшие счета за Internet-услуги и утечку конфиденциальной информации. Такие случаи достаточно показательны, т.к. иллюстрируют очень распространенные практику и порядок увольнения в российских компаниях.

Однако самая большая опасность может исходить не просто от уволенных или обиженных рядовых сотрудников (например, операторов различных информационных подсистем), а от тех, кто облечён большими полномочиями и имеет доступ к широкому спектру самой различной информации. Обычно это сотрудники ИТ-отделов (аналитики, разработчики, системные администраторы), которые знают пароли ко всем системам, используемым в организации. Их квалификация, знания и опыт, используемые во вред, могут привести к очень большим проблемам. Кроме того, таких злоумышленников очень трудно обнаружить, поскольку они обладают достаточными знаниями о системе защиты ИС компании, чтобы обойти используемые защитные механизмы и при этом остаться "невидимыми".

Согласно ежегодному исследованию Computer Security Institute (CSI, USA) в 2012 году суммарный ущерб от всех внутренних угроз корпоративным информационным системам превысил 378 миллионов долларов (по опросу представителей 600 компаний из разных секторов экономики). По России достоверная статистика пока отсутствует. Тем не менее, при построении системы защиты необходимо защищаться не только и не столько от внешних злоумышленников, сколько от злоумышленников внутренних.

При создании защищенных корпоративных систем нередко упускается из виду распределение и текущее перераспределение прав доступа к информации, и оставляются открытыми такие очевидные причины утечки конфиденциальной информации, как "слабые" (или "долгоживущие") пароли или не внедренные, не "работающие" положения политики корпоративной безопасности. Некоторые специалисты предлагают радикальный метод - запретить любое обращение к данным, если оно не санкционировано высшим руководством. Повторим, однако, что ни административная, ни физическая защита от НСД не предотвратит хищение конфиденциальной информации сотрудниками, если они имеют к ней свободный программно-аппаратный доступ. Приведём конкретный пример. Риск неконтролируемого использования различных устройств передачи и хранения информации в своё время резко увеличился с выходом Windows XP и поддержкой в ней технологии универсальной последовательной шины доступа (Universal Serial Bus, USB). Пакет обновления Service Pack 2 для Windows XP с множеством улучшений подсистемы безопасности не содержал в себе средств разграничения доступа к портам USB и FireWire.

Вообще Windows XP (а также NT/2000/ Server 2003) обладает широкими возможностями по контролю доступа пользователей к различным ресурсам и позволяет настраивать разнообразные политики безопасности. Однако полноценный контроль доступа к USB-портам невозможен с помощью только встроенных средств администрирования. Windows разрешает любому пользователю устанавливать USB-устройства и работать с ними. Поэтому USB-порт представляет собой неконтролируемый канал утечки конфиденциальных данных и заражения корпоративной сети вирусами и "червями" в обход серверных шлюзов и антивирусов - и таких точек неконтролируемого доступа в большой распределенной компании может быть множество. Точно так же дело обстоит и с записывающими CD-ROM и многими другими устройствами.

Самый простой способ решения проблемы - отключение USB-портов через BIOS - часто является и самым неэффективным, так как современные внешние устройства (мышь, клавиатура, принтер, сканер и т.д.) всё чаще снабжены BТ-коннекторами.

Защита информации от несанкционированного доступа (НСД) к сетям и информационным ресурсам - это комплексная задача, она не может быть решена одними лишь административными или техническими мерами. Защита от НСД должна строиться как минимум на трех уровнях - административном, физическом и программно-аппаратном.

**От чего надо защищаться?**

Во-первых, это вирусы (Virus, Worm) и всевозможные виды практически бесполезной информации, рассылаемой абонентам электронной почты (Spam). По различным данным в 2013 году вирусным и спамовым атакам было подвержено 85-90 % компаний во всем мире. Далее следует назвать программы типа "троянский конь" (Trojan Horse), которые могут быть незаметно для владельца установлены на его компьютер и так же незаметно функционировать на нем. Следующим распространенным типом атак являются действия, направленные на выведение из строя того или иного узла сети. Эти атаки получили название "отказа в обслуживании" (Denial of Service - DoS), на сегодняшний день известно более сотни различных вариантов этих действий. Выше отмечалось, что выведение из строя узла сети на несколько часов может привести к очень серьезным последствиям. Например, выведение из строя сервера транзакционной системы крупной корпорации или банка приведет к невозможности осуществления платежей и, как следствие, к большим прямым и косвенным финансовым и рейтинговым потерям.

Укажем ещё один существенный источник угроз, который с точки зрения размера ущерба может быть отнесён к одному из самых распространённых в России - непреднамеренные ошибки пользователей ИС, операторов, системных администраторов и других лиц, обслуживающих информационные системы. Иногда такие ошибки являются угрозами (неправильно введенные данные, ошибка в программе), а иногда они создают уязвимости, которыми могут воспользоваться злоумышленники - таковы обычно ошибки администрирования и предоставления доступа.

Согласно данным В.А. Галатенко [Галатенко В.А., 2006], 65% потерь - следствие непреднамеренных ошибок из-за компьютерной неграмотности и безответственности сотрудников компаний и пользователей ИС. Очевидно, самый радикальный способ борьбы с непреднамеренными ошибками - максимальная автоматизация информационных процессов, системы программной и технической "защиты от дурака" (Fool Proof), эффективное обучение персонала, неукоснительное следование положениям политики ИБ и строгий процедурный контроль правильности совершаемых действий.

**Как надо защищаться?**

Наиболее простой способ — купить новейшие рекламируемые средства защиты, установить у себя в организации, не утруждая себя обоснованием её полезности и эффективности. Если компания богата, то она может позволить себе этот путь. Однако истинный руководитель должен системно оценивать ситуацию и правильно расходовать средства.

Во всем мире сейчас принято строить комплексную систему защиты информации и информационных систем в несколько этапов — на основе формирования концепции и программы информационной безопасности, имея в виду в первую очередь взаимосвязь её основных понятий ([рис. 1.7](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=2#image.1.7)) [Лапонина О. Р., 2005].

Первый этап — информационное обследование предприятия — самый важный. Именно на этом этапе определяется, от чего, в первую очередь, необходимо защищаться компании. Вначале строится так называемая модель нарушителя, которая описывает вероятный облик злоумышленника, т. е. его квалификацию, имеющиеся средства для реализации тех или иных атак, обычное время действия и т. п. На этом этапе можно получить ответ на два вопроса, которые были заданы выше: "Зачем и от кого надо защищаться?" На этом же этапе выявляются и анализируются уязвимые места и возможные пути реализации угроз безопасности, оценивается вероятность атак и ущерб от их осуществления.

По результатам этапа вырабатываются рекомендации по устранению выявленных угроз, правильному выбору и применению средств защиты. На этом этапе может быть рекомендовано не приобретать достаточно дорогие средства защиты, а воспользоваться имеющимися в распоряжении. Например, в случае использования в небольшой компании мощного маршрутизатора можно рекомендовать воспользоваться встроенными в него защитными функциями, а не приобретать более дорогой межсетевой экран (Firewall).



**Рис. 1.7.**Взаимосвязанные параметры поля информационной безопасности

Наряду с анализом существующих в компании конкретных средств защиты следует разработать общую и частные политики в области информационной безопасности и совокупности организационно-распорядительных мер и документов, а также методологий и технических решений, являющихся основой для создания инфраструктуры информационной безопасности ([рис. 1.8](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27496?page=2#image.1.8)) [Соколов А. В., Шаньгин В. Ф., 2002].



**Рис. 1.8.**Составляющие инфраструктуры информационной безопасности

Эти документы, основанные на международном законодательстве и законах Российской федерации и нормативных актах, дают необходимую правовую базу службам безопасности и отделам защиты информации для проведения всего спектра защитных мероприятий, взаимодействия с внешними организациями, привлечения к ответственности нарушителей и т. п.

Следующим этапом построения комплексной системы информационной безопасности служит приобретение, установка и настройка рекомендованных на предыдущем этапе средств и механизмов защиты информации. К таким средствам можно отнести системы защиты информации от несанкционированного доступа, системы криптографической защиты, межсетевые экраны, средства анализа защищенности и другие.

Для правильного и эффективного применения установленных средств защиты необходим квалифицированный персонал.

С течением времени имеющиеся средства защиты устаревают, выходят новые версии систем обеспечения информационной безопасности, постоянно расширяется список найденных слабых мест и атак, меняется технология обработки информации, изменяются программные и аппаратные средства, приходит и уходит персонал компании. Поэтому необходимо периодически пересматривать разработанные организационно-распорядительные документы, проводить обследование ИС или ее подсистем, обучать новый персонал, обновлять средства защиты.

Следование описанным выше рекомендациям как строить комплексную систему обеспечения информационной безопасности поможет достичь необходимого и достаточного уровня защищенности вашей автоматизированной системы.