Лекция 11-12

**Обеспечение интегральной безопасности**

**Аннотация:**В лекции рассказывается об интегральной безопасности информационных систем. |

**Обеспечение интегральной безопасности информационных систем и сетей**

Вследствие высокой степени глобализации организационных структур, бизнес-моделей, знаний и технологий современная высокотехнологичная компания часто географически распределена в пространстве, а её *деятельность* — во времени ([рис. 7.1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=1#image.7.1)). Всё это налагает особые условие на формирование структуры вычислительных и информационных систем, поддерживающих такую *деятельность*, и на обеспечение их безопасности.



**Рис. 7.1.**Распределенная информационная система

Развитие информационных и нанотехнологий, методов и средств программирования, цифровой обработки сигналов и технологий распознавания образов привело, в свою *очередь*, к быстрому развитию средств защиты информации, информационных систем и сетей ([рис. 7.2](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=1#image.7.2)).

В связи с многообразием задач защиты информации и программно-аппаратных средств, реализующих защиту, сформировалось три основных подхода осуществления информационной безопасности:

1. Частный подход основывается на решении локальных задач обеспечения информационной безопасности. Этот подход является малоэффективным, но достаточно часто используется, так как не требует больших финансовых и интеллектуальных затрат.
2. Комплексный подход реализуется решением совокупности локальных задач по единой программе. Этот подход в настоящее время применяется наиболее часто.
3. Интегральный подход основан на объединении различных вычислительных подсистем ИС, подсистем связи, подсистем обеспечения безопасности в единую информационную систему с общими техническими средствами, каналами связи, программным обеспечением и базами данных.



**Рис. 7.2.**Развитие технологий защиты информации

Наряду с системной и функциональной интеграцией ИС в последнее время стала активно развиваться сфера интегральной информационной безопасности (*Integral* *Information* *Safety* — *IIS*).

Это такое состояние условий функционирования сотрудников, объектов, технических средств и систем, при котором они надежно защищены от возможных угроз в ходе непрерывного процесса подготовки, хранения, передачи и обработки информации.

Интегральная *безопасность* информационных систем включает в себя следующие составляющие:

* физическая безопасность — защита зданий, помещений, подвижных средств, людей, а также аппаратных средств (компьютеров, носителей информации, сетевого оборудования, кабельного хозяйства, поддерживающей инфраструктуры);
* безопасность сетей и телекоммуникационных устройств — защита каналов связи от воздействий любого рода;
* безопасность системного и прикладного программного обеспечения — защита от вирусов, логических "мин", несанкционированного изменения конфигурации систем и программного кода;
* безопасность данных — обеспечение конфиденциальности, целостности и доступности данных.

Задача обеспечения ИИБ появилась вместе с проблемой надежного хранения информации и безопасной передачи её пользователю. На современном этапе интегральный подход предполагает обязательную непрерывность процесса обеспечения безопасности как во времени (в течение всей "жизни" ИС), так и в пространстве (по всему технологическому циклу деятельности) с обязательным учетом всех возможных видов угроз (несанкционированный *доступ*, съем информации, терроризм, пожар, *стихийные бедствия* и т. п.).

В какой бы форме ни применялся интегральный подход, он связан с решением ряда сложных разноплановых частных задач в их тесной взаимосвязи. Наиболее очевидными из них являются задачи разграничения доступа к информации, ее технического и криптографического "закрытия", устранение паразитных излучений технических средств, технической и физической укрепленности объектов, охраны и оснащения их тревожной сигнализацией.

На [рис. 7.3](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=1#image.7.3) представлена *блок-схема* интегрального комплекса физической защиты объекта, обеспечивающего функционирование всех рассмотренных выше систем, а на [рис. 7.4](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=1#image.7.4) — соотношение эффективности современных электронных средств контроля физического доступа [Барсуков В., [http://www.jetinfo.ru](http://www.jetinfo.ru/)].

Стандартный набор средств комплексной защиты информации в составе современной ИС обычно содержит следующие компоненты:

* средства обеспечения надежного хранения информации с использованием технологии защиты на файловом уровне (File Encryption System — FES);
* средства авторизации и разграничения доступа к информационным ресурсам, а также защита от несанкционированного доступа к информации с использованием систем биометрической авторизации и технологии токенов (смарт-карты, touch-memory, ключи для USB-портов, скрытые цифровые маркеры и т.п.);
* средства защиты от внешних угроз при подключении к общедоступным сетям связи (Интернет), а также средства управления доступом из Интернет с использованием технологии межсетевых экранов (Firewall) и содержательной фильтрации (Content Inspection);
* средства защиты от вирусов с использованием специализированных комплексов антивирусной профилактики;
* средства обеспечения конфиденциальности, целостности, доступности и подлинности информации, передаваемой по открытым каналам связи с использованием технологии защищенных виртуальных частных сетей (VPN);
* средства обеспечения активного исследования защищенности информационных ресурсов с использованием технологии обнаружения атак (Intrusion Detection);
* средства обеспечения централизованного управления системой ИИБ в соответствии с согласованной и утвержденной "Политикой безопасности компании". Пример реализации одной из политик, относящейся к взаимодействию локальной вычислительной или информационной сети с сетью Internet показан на [рис. 7.5](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27507?page=1#image.7.5).



**Рис. 7.3.**Блок-схема интегрального комплекса физической защиты информационной инфраструктуры



**Рис. 7.4.**Сравнение эффективности современных электронных средств, используемых для контроля доступа



**Рис. 7.5.**Схема взаимодействия внутренней ЛВС компании с внешним пространством Internet