## Введение

Информация имеет первостепенное значение. Современное общество называют информационным.

В 1972 году американский специалист в области связи и вычислительной техники Роберт Фано говорил: «Стремление сохранить тайну предприятий и отдельных лиц – не единственный повод для поиска надежных средств обеспечения неприкосновенности информации, хранимой в вычислительных системах, а также для поиска средств контроля над ее применением. Такие средства требуются также для выполнения договорных обязательств, заключаемых между создателями программного обеспечения и банков данных, с одной стороны, и потребителями этой продукции, с другой. Следует иметь в виду и то, что бесконтрольный сбор, хранение и распределение информации неизбежно сопровождается «загрязнением» информационной среды – явлением, которое уже начало приводить если не к серьезным, то, во всяком случае, к тревожным последствиям. Наконец, соображения общественной безопасности диктуют необходимость надежного контроля над информацией, способной оказаться источником угрожающего положения, скажем вследствие распространения среди населения панических настроений либо вследствие потворствования незаконным действиям»

Проблема безопасности информационных технологий (ИТ) возникла на пересечении двух активно развивающихся направлений – безопасности технологий и информатизации.

Обеспечение собственной безопасности – задача первостепенной важности для любой системы независимо от ее сложности и назначения, будь то биологический организм или система обработки информации. Однако когда средства нападения имеют форму информационных воздействий, необходимо разрабатывать и применять совершенно новые технологии, методы зашиты.

Научные и технические предпосылки кризисной ситуации.

Современные компьютеры приобрели гигантскую вычислительную мощь, но одновременно с этим стали и проще в эксплуатации.

Все большее количество новых (и неквалифицированных) людей получает доступ к компьютерам, что приводит к снижению средней квалификации пользователей. Большинство пользователей имеют личные компьютеры и осуществляют их администрирование самостоятельно. Они не в состоянии постоянно поддерживать безопасность своих систем на должном уровне, т.к. это требует соответствующих знаний, времени и средств. Распространение сетевых технологий объединило отдельные машины в локальные сети, совместные использующие общие ресурсы, а применение технологий клиент-сервер и кластеризации преобразовало такие сети в распределенные вычислительные среды.

Безопасность сети определяется защищенностью всех входящих в нее компьютеров и сетевого оборудования и достаточно нарушить работу только одного компьютера, чтобы скомпрометировать всю сеть.

Если компьютер, который является объектом атаки, подключен к глобальной вычислительной сети (Internet), то независимо от характера обрабатываемой в нем информации то не имеет значения, где он находится – в соседней комнате или на другом континенте.

Бурное развитие программного обеспечения.

В настоящее время большинство операционных систем не отвечает требованиям безопасности, хотя в последнее время и осуществляют определенные усилия в этом направлении. Существует огромное количество различных недокументированных возможностей, обеспечивающих реализацию намеренных злоумышленных действий.

Развитие гибких и мобильных технологий привело к тому, что практически исчезает грань между обрабатываемыми данными и исполняемыми программами за счет появления и широкого распространения виртуальных машин и интерпретаторов. Теперь любое развитое приложение не просто обрабатывает данные, а интерпретирует интегрированные в них инструкции специальных языков программирования, т.е. по сути дела является отдельной машиной с привычной фон-неймановской архитектурой, для которых можно создавать средства нападения. Это увеличивает возможности злоумышленников и затрудняет задачу зашиты таких систем, т.к. наличие «вложенных» систем требует и реализации защиты для каждого уровня.

Несоответствие бурного развития средств обработки информации и медленного процесса разработки теории информационной безопасности привело к разрыву между теоретическими моделями, оперирующими абстрактными понятиями и реальными категориями современных информационных технологий. Кроме того, многие средства защиты (например, средства борьбы с компьютерными вирусами) и системы защиты корпоративных систем на данный момент вообще не имеют системной научной базы. Такое положение является следствием отсутствия общей теории защиты информации, комплексных моделей безопасности обработки информации, отсутствие средств, позволяющих эффективно промоделировать адекватность тех или иных решений в области безопасности. Сегодня нет даже общепринятой терминологии, адекватно воспринимаемой всеми специалистами в области безопасности.

Необходимость создания глобального информационного пространства и обеспечение безопасности протекающих в нем процессов потребовала разработки международных стандартов, следование которым может обеспечить необходимый уровень гарантий обеспечения ИБ. Причем в современных условиях важным является не только стандартизация требований безопасности, но и обоснование их применения, а также методов подтверждения адекватности реализованных средств защиты и корректности самой реализации.

Перед разработчиками современных ИС стоят следующие задачи:

* Обеспечение безопасности новых типов информационных ресурсов. Это означает, что системы защиты должны обеспечивать безопасность не отдельных документов, файлов или сообщений, а решать задачи ИБ на уровне информационных ресурсов (Например, гипертекст, мультимедиа).

Гипертекст – информационный массив, на котором заданы и автоматически поддерживаются ассоциативные и смысловые связи между выделенными элементами, понятиями, терминами или разделами.

Мультимедиа – комплексное представление информации – вывод данных в текстовом, графическом, видео-, аудио-, мультипликационном видах.

* Организация доверенного взаимодействия сторон.
* Защита от автоматических средств нападения – разрушающих программных средств (РПС) т.е. компьютерных вирусов, «троянских коней» программных закладок. Средства разграничения доступа не решают в полной мере этой проблемы.
* Интеграция защиты информации в процессе автоматизации ее обработки в качестве обязательного элемента. Это означает, что средства безопасности не должны вступать в конфликт с существующими приложениями и сложившимися технологиями обработки информации, а напротив, должны стать неотъемлемой частью этих средств и технологий.

Понятие «защищенная система».

Защищенная система обработки информации для определенных условий эксплуатации обеспечивает безопасность (конфиденциальность и целостность) обрабатываемой информации и поддерживает свою работоспособность в условиях воздействия на нее заданного множества угроз.

Защищенная система должна обладать следующими свойствами.

1. Она должна автоматизировать процесс обработки конфиденциальной информации, включая все аспекты этого процесса, связанные с обеспечением безопасности.
2. Успешно и эффективно противостоять угрозам безопасности.
3. Соответствовать требованиям и критериям стандартов информационной безопасности. Наличие общепринятых стандартов позволяет согласовать подходы различных участников процесса создания защищенных систем (требования потребителей, технологии и методы производителей, критерии независимой экспертизы).