РАЗДЕЛ I

ОСНОВЫ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Глава 1. АКТУАЛЬНОСТЬ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Автоматизированные системы, в состав которых входят информационные технологии (ИТ), основанные на новейших разработках в области средств вычислительной техники (СВТ) и связи, находят все более широкое применение практически во всех сферах жизни и деятельности (в отличие от индустриальных технологий, где основным объектом переработки являются сырье и материалы, информационные технологии «потребляют» и «перерабатывают» информацию). С развитием ИТ объемы обрабатываемой и передаваемой информации, как в абсолютных значениях, так и по отношению к объемам переработки сырья и материалов в индустриальных технологиях, непрерывно возрастают.

1.1. Место и роль автоматизированных систем в управлении бизнес-процессами

Почему же современные компьютеры и средства телекоммуникации так широко востребованы? Что они умеют делать, что становятся необходимыми практически везде? В ответ на эти вопросы, как правило, можно услышать: «Компьютеры позволяют автоматизировать умственный труд». Но разве физический труд они не автоматизируют и как объяснить понятие «умственный труд»?

Ответим на поставленные вопросы. Компьютерные технологии дают возможность автоматизировать процессы управления (умственный труд по управлению — по принятию решений в конкретных ситуациях на основе имеющейся информации). А поскольку управление необходимо везде, всегда и всем, то и средства автоматизации управления применяются повсеместно. Автоматизация на основе современных ИТ позволяет принимать решения более оперативно и

обоснованно, учитывая при этом большой объем сведений, повышая качество и эффективность управления — управления чем бы то ни было — от отдельных узлов и агрегатов (например, в автомобилях), деятельностью отдельных людей до технологических процессов на производстве, бизнес-процессов компаний, экономических и социально-политических процессов в обществе.

Широкое внедрение АС во все сферы жизни общества требует повышенного внимания к защите применяемых для автоматизации управления информационных технологий и непосредственно информации. Любые нарушения и неполадки в работе автоматизированных/информационных систем (ИС), систем обработки и передачи информации приводят к снижению качества или полной потере управления критичными процессами и, соответственно, к убыткам.

Следует отметить, что любая информационная система всегда является частью соответствующей системы управления, а любая автоматизированная информационная система (АИС) — частью автоматизированной системы управления (АСУ).

Практически каждое фундаментальное техническое или технологическое новшество, предоставляя возможности для решения каких-либо социальных проблем и открывая широкие перспективы для развития личности и общества, вызывает обострение существующих или порождает новые, ранее неизвестные, проблемы, становится источником новых потенциальных опасностей.

Без должного внимания к вопросам обеспечения безопасности последствия перехода общества к новым технологиям могут быть катастрофическими как для отдельных граждан, так и общества в целом. Именно так обстоит дело в области атомных, химических и других экологически опасных технологиях, в сфере транспорта.

Аналогичная ситуация и с информатизацией общества. Искажение или фальсификация, уничтожение или разглашение определенной части информации, а также дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах автоматизированного информационного взаимодействия.

Жизненно важные интересы этих субъектов, как правило, заключаются в том, чтобы определенная часть информации, касающаяся их экономических, политических и других сфер деятельности, конфиденциальная коммерческая и персональная информация была бы легко доступна для пользователя и в то же время надежно защищена.

1.2. Обострение проблемы обеспечения безопасности автоматизированных систем на современном этапе

Актуальность проблемы защиты АС в современных условиях определяется следующими основными факторами:

• обострением противоречий между объективно существующими потребностями общества в расширении свободного обмена информацией и чрезмерными (недостаточными) ограничениями на ее распространение и использование;

• расширением сферы применения электронно-вычислительных машин (ЭВМ), многообразием и повсеместным распространением информационно-управляющих систем, высокими темпами увеличения парка средств вычислительной техники и связи;

• повышением уровня доверия к автоматизированным системам управления и обработки информации, использованием их в критических областях деятельности;

• вовлечением в процесс информационного взаимодействия все большего числа людей и организаций, резким возрастанием их информационных потребностей, наличием интенсивного обмена информацией между участниками этого процесса;

• концентрацией больших объемов информации различного назначения и принадлежности на электронных носителях;

• количественным и качественным совершенствованием способов доступа пользователей к информационным ресурсам;

• отношением к информации как к товару, переходом к рыночным отношениям в области предоставления информационных услуг;

• многообразием видов угроз и возникновением новых каналов несанкционированного доступа к информации;

• увеличением числа квалифицированных пользователей средствами вычислительной техники и возможностей по созданию ими нежелательных программно-математических воздействий на системы обработки информации;

• возрастанием уязвимости субъектов вследствие увеличения потерь от уничтожения, фальсификации, разглашения или незаконного тиражирования информации;

• развитием рыночных отношений в сфере ИТ (в области разработки, поставки, обслуживания вычислительной техники, разработки программных средств, в том числе средств защиты).

Проблема обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более обостряется по следующим объективным п р и ч и н а м:

• *расширение сферы применения СВТ и возросший уровень доверия к автоматизированным системам управления и обработки информации.* С помощью компьютерных систем выполняют самую ответственную работу, от которой зависит жизнь и благосостояние многих людей. Автоматизированные системы позволяют управлять технологическими процессами на предприятиях и атомных электростанциях (АЭС), движением самолетов и поездов, выполнять финансовые операции, обрабатывать секретную и конфиденциальную информацию;

• *изменение подхода к самому понятию «информация»*. Данный термин все чаще используется для обозначения особого товара, стоимость которого нередко превышает стоимость автоматизированной системы, в рамках которой он существует;

• *переход к рыночным отношениям* в области создания и предоставления информационных услуг с присущей этим отношениям *конкуренцией и промышленным шпионажем*;

• *развитие и распространение информационно-телекоммуникационных сетей, территориально распределенных систем и систем с удаленным доступом* как совместно используемых ресурсов;

• *распространение компьютерной грамотности* в широких слоях населения из-за доступности СВТ и прежде всего персональных компьютеров (ПК), что вызвало увеличение числа попыток неправомерного вмешательства в работу государственных и коммерческих АСУ как случайных, так и умышленных;

• *отсутствие стройной и непротиворечивой системы законодательно-правового регулирования отношений* в сфере накопления, использования и защиты информации создает условия для возникновения и широкого распространения «компьютерного хулиганства» и «компьютерной преступности»;

• *бурное развитие и широкое распространение компьютерных вирусов*, способных скрытно существовать в системе и совершать любые несанкционированные действия;

• *наличие злоумышленников — специалистов-профессионалов в области вычислительной техники и программирования*, досконально знающих все достоинства и слабые места АС и занимающихся анализом и взломом механизмов защиты.

Исследование в области информационной безопасности, проведенное английской консалтинговой компанией «Ernst & Young» в России и странах СНГ, показало, что более 65 % российских компаний сталкивались с нарушениями информационной безопасности, при этом в 50 % случаев данные нарушения были вызваны хакерскими атаками, в том числе с проникновением в информационную систему извне, несанкционированным доступом непосредственно в компании, атаками, имеющими целью вызвать отказ в обслуживании, саботажем, финансовым мошенничеством и хищением коммерческой информации.

Проблема обеспечения безопасности АС относится к числу трудноразрешимых, что связано со следующими объективными обстоятельствами:

• недостаточным (неадекватным реалиям) пониманием необходимости защиты используемых АС;

• высокой степенью неопределенности рисков при применении новейших АС;

• сложностью АС как объектов защиты;

• необходимостью комплексного подхода к защите АС с учетом их значительной зависимости от человеческого фактора;

• сложностью разрешения конфликтов интересов между различными категориями субъектов (операторами информационных систем, системными и сетевыми администраторами, администраторами безопасности, пользователями, обслуживающим персоналом систем и менеджерами различных уровней);

• отставанием методов и средств защиты от развития информационных технологий, а также методов и средств нападения;

• недостатком квалифицированных специалистов в сфере компьютерной безопасности и низким уровнем компьютерной культуры пользователей (слабой осведомленностью в вопросах безопасности ИТ).

1.3. Защита автоматизированных систем как процесс управления рисками

Создание абсолютно непреодолимой системы защиты принципиально невозможно. До тех пор пока информация находится в обращении, принимаемые меры могут только снизить вероятность негативных воздействий или ущерб от них, но не исключить полностью. При достаточном количестве времени и средств можно преодолеть любую защиту, поэтому имеет смысл рассматривать некоторый приемлемый уровень обеспечения безопасности, соответствующий реально существующим угрозам (рискам).

Под *угрозой* обычно понимают потенциально возможное событие, вызванное действием, процессом или явлением, которое может (воздействуя на что-либо) привести к нанесению ущерба чьим-либо интересам.

Риск — это оценка опасности определенной угрозы.

Риск выражает вероятностно-стоимостную оценку возможных потерь (ущерба) и характеризуется:

• вероятностью успешной реализации угрозы;

• стоимостью потерь (ущерба) в случае реализации угрозы.

Стоимостную составляющую информационной безопасности хорошо иллюстрирует упрощенная формула оценки издержек, связывающая количественные характеристики рисков, стоимость реализации мер защиты и суммарные издержки:

$$R = \sum_{i=1}^{n} (A_i B_i + C_i) < R_{\max},$$

где n — количество рисков (угроз); A — вероятностная оценка риска (0-1); B — стоимостная оценка риска; C — стоимость реализации мер защиты; $R_{\max}$ — допустимые издержки.

Анализ рисков заключается в выявлении существующих угроз и оценке их опасности. На этапе анализа рисков выявляют все значимые угрозы, т. е. угрозы, характеризующиеся большой частотой (вероятностью) реализации и/или приводящие к существенным (ощутимым) потерям.

Суть защиты ресурсов АС — управление рисками, связанными с использованием этих АС.

Известно два основных подхода к анализу рисков — качественный и количественный. Наиболее привлекательным, на первый взгляд, является количественный подход, позволяющий сравнивать защищенность различных систем, но его внедрение осложнено следующими причинами:

- отсутствием достоверной статистики в быстро меняющемся мире ИТ;
- трудностью оценки ущерба по нематериальным активам (репутация, конфиденциальность сведений, идеи, бизнес-планы, здоровье персонала);
- сложностью оценки косвенных потерь от реализации угроз;
- обесцениванием результатов длительной количественной оценки рисков из-за постоянной модификации и реконфигурации АС.

В связи с этим для анализа рисков в настоящее время используется качественный подход, предусматривающий простое ранжирование угроз и связанных с ними рисков по степени их опасности.

Управление рисками предполагает принятие мер защиты (контрмер), направленных на снижение частоты успешной реализации угроз и/или ущерба в случае их реализации. Защитные меры выбирают на основе принципа разумной достаточности (экономической целесообразности, сопоставимости возможного ущерба и затрат на защиту), исходя из минимизации общих издержек — затрат на защиту и остаточных потерь от угроз.

Существует несколько вариантов противодействия выявленным рискам (угрозам):

1) признание допустимости риска от конкретной угрозы (например, если вероятность реализации угрозы ничтожна мала или затраты на защиту от нее катастрофически велики);

2) частичная передача ответственности за инциденты в сфере безопасности ИТ сторонней организации (например, страховой компании);

3) проведение комплекса мероприятий (мер противодействия), позволяющих уменьшить или полностью исключить риск.

Основные этапы анализа рисков и управления ими:

- определение границ системы и методологии оценки рисков;
- идентификация и оценка информационных ресурсов системы (ценностей);
- идентификация угроз и оценка вероятностей их реализации;
- определение риска и выбор средств защиты;
- внедрение средств защиты и оценка остаточного риска.

1.4. Методы оценки целесообразности затрат на обеспечение безопасности

К методу оценки целесообразности затрат на обеспечение безопасности АС предъявляются определенные требования:

- метод должен обеспечивать количественную оценку затрат на безопасность АС, используя качественные показатели оценки вероятностей событий и их последствий;

• быть прозрачным с точки зрения пользователя и давать возможность вводить собственные эмпирические данные;

• быть универсальным, т. е. одинаково применимым к оценке затрат на приобретение аппаратных средств, специализированного и универсального программного обеспечения, затрат на услуги, перемещение персонала, обучение конечных пользователей и т. д.;

• позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенных угроз, в разной степени влияющих на сокращение вероятности происшествия.

Перечислим категории затрат, связанных с безопасностью АС.

Организационные затраты на формирование и поддержание звена управления системой защиты информации включают следующие статьи расходов:

• формирование политики безопасности АС;

• приобретение и ввод в эксплуатацию программно-технических средств (серверов, компьютеров конечных пользователей — настольных и переносных), периферийных устройств и сетевых компонентов;

• приобретение и настройку средств защиты информации;

• содержание персонала (стоимость работ и аутсорсинг).

Затраты на контроль — определение и подтверждение достигнутого уровня защищенности ресурсов АС — состоят из следующих позиций:

• контроль реализации функций, обеспечивающих управление безопасностью АС;

• организация взаимодействия между подразделениями для решения конкретных задач по обеспечению безопасности АС;

• проведение аудита безопасности по каждой части АС;

• материально-техническое обеспечение системы контроля доступа к объектам и ресурсам;

• плановые проверки и испытания средств защиты информации;

• проверка навыков эксплуатации средств защиты персоналом;

• создание условий для нормальной работы лицам, ответственным за реализацию конкретных процедур безопасности по подразделениям;

• контроль правильности ввода данных в прикладных системах;

• оплата труда инспекторов по контролю выполнения требований, предъявляемых к средствам защиты при разработке систем (контроль на стадии проектирования и спецификации требований);

• внеплановые проверки и испытания (оплата труда испытательного персонала специализированных организаций; обеспечение испытательного персонала материально-техническими средствами);

• контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере безопасности АС.

Внутренние затраты на ликвидацию последствий нарушений политики безопасности АС, т. е. пересмотр политики безопасности АС (проводится периодически):

• идентификация угроз безопасности АС;

• поиск уязвимостей системы безопасности АС;

• оплата труда специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска;

• ликвидация последствий нарушения режима безопасности;

• восстановление системы безопасности АС до соответствия требованиям политики безопасности;

• установка патчей или приобретение последних версий программных средств защиты информации;

• приобретение новых технических средств взамен пришедших в негодность;

• проведение дополнительных испытаний и проверок технологических информационных систем;

• утилизация скомпрометированных ресурсов;

• восстановление информационных ресурсов — баз данных и прочих информационных массивов;

• проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность;

• выявление причин нарушения политики безопасности — проведение расследований нарушений политики безопасности АС (сбор данных о способах совершения неправомерного деяния, поиск предметов посягательства, выявление мотивов неправомерных действий и т. д.);

• обновление планов обеспечения непрерывности деятельности службы безопасности;

• переделки — внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности АС;

• повторные проверки и испытания системы безопасности АС.

Внешние затраты на ликвидацию последствий нарушения политики безопасности АС объединяют следующие позиции:

• невыполнение обязательств перед государством и партнерами;

• юридическое сопровождение и выплата компенсаций;

• проведение дополнительных исследований и разработка новой рыночной стратегии;

• отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, разработка новых средств ведения конкурентной борьбы;

• потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения;

• заработная плата служащих, организационные и прочие расходы, непосредственно связанные с предупредительными мероприятиями;

• другие виды возможного ущерба, в том числе невозможность выполнения функциональных задач.

Затраты на техническое обслуживание системы безопасности ИТ, т. е. на мероприятия по предотвращению нарушений политики безопасности ИТ (предупредительные мероприятия) включают следующие статьи:

• управление системой безопасности ИТ;

• планирование системы безопасности ИТ;

• изучение возможностей инфраструктуры по обеспечению безопасности ИТ;

• техническая поддержка персонала при внедрении средств защиты информации и процедур, а также планов по безопасности ИТ;

• проверка сотрудников на лояльность, выявление угроз безопасности ИТ;

• организация системы допуска исполнителей и сотрудников к защищаемым ресурсам;

• регламентное обслуживание средств защиты информации;

• обслуживание и настройка программно-технических средств защиты информации, операционных систем (ОС) и сетевого оборудования;

• организация сетевого взаимодействия и безопасного использования ИС;

• поддержание системы резервного копирования и ведения архива данных;

• проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, СВТ и т. п.;

• аудит системы безопасности ИТ — контроль изменений состояния информационной среды и действий исполнителей;

• обеспечение соответствия используемых ИТ заданным требованиям по безопасности, совместимости и надежности, в том числе анализ возможных негативных аспектов ИТ, влияющих на целостность и доступность;

• доставка (обмен) конфиденциальной информации;

• удовлетворение субъективных требований пользователей (стиль, удобство интерфейса и др.);

• обеспечение соответствия требованиям стандартов;

• повышение квалификации сотрудников по вопросам использования имеющихся средств защиты, выявления и предотвращения угроз безопасности ИТ;

• развитие нормативной базы и технической оснащенности подразделения безопасности.

Приведенный перечень затрат на обеспечение высокоэффективной системы защиты информации указывает на высокую стоимость компьютерной безопасности. Излишние меры безопасности, помимо экономической неэффективности, приводят к созданию дополнительных неудобств и недовольству персонала. Важно правильно выбрать тот необходимый и достаточный уровень защиты, при котором соотношение затрат на контрмеры и размер возможного ущерба были бы приемлемыми.

1.5. Особенности современных автоматизированных систем как объектов защиты

Большинство современных автоматизированных систем обработки информации представляют собой территориально распределенные системы интенсивно взаимодействующих (синхронизирующихся) между собой по данным (ресурсам) и управлению (событиям) локальных вычислительных сетей (ЛВС) и отдельных ЭВМ.

В распределенных АС возможны все «традиционные» для локально расположенных (централизованных) вычислительных систем способы несанкционированного вмешательства в их работу и доступа к информации, а также

характерные только для них специфические каналы проникновения в систему, что объясняется целым рядом их о с о б е н н о с т е й , среди которых:

• территориальная разнесенность компонентов АС и наличие интенсивного обмена информацией между ними;

• широкий спектр способов представления, хранения и передачи информации;

• интеграция данных, принадлежащих различным субъектам, в рамках единых баз данных и, наоборот, размещение необходимых некоторым субъектам данных в удаленных узлах сети;

• абстрагирование владельцев данных от физических структур и места размещения данных;

• использование режимов распределенной обработки данных;

• участие в процессе автоматизированной обработки информации большого количества пользователей и персонала;

• непосредственный и одновременный доступ к ресурсам (в том числе и информационным) большого числа пользователей;

• разнородность средств вычислительной техники и связи, а также их программного обеспечения;

• отсутствие специальных средств защиты в большинстве типов технических средств, широко используемых в АС.

* * *

Трудности решения практических задач обеспечения безопасности конкретных АС связаны с отсутствием развитой стройной теории и необходимых научно-технических и методических основ обеспечения защиты информации в современных условиях.

Применяемые в настоящее время большинством организаций меры не обеспечивают необходимого уровня безопасности субъектов, участвующих в процессе информационного взаимодействия, и не способны в необходимой степени противостоять разного рода воздействиям в целях доступа к критичной информации и дезорганизации работы автоматизированных систем.

Контрольные вопросы

1. Охарактеризуйте место и роль автоматизированных систем в управлении бизнес-процессами.

2. Какие факторы определяют актуальность проблемы защиты АС в современных условиях?

3. Перечислите особенности современных автоматизированных систем как объектов защиты.

4. Назовите причины обострения проблемы обеспечения информационной безопасности.

5. Почему проблема обеспечения безопасности АС относится к числу трудноразрешимых?

6. Что понимается под риском информационной безопасности? Каковы составляющие риска?

7. В чем заключается анализ рисков и управление ими? Перечислите этапы анализа и управления.

8. Каковы требования к методам оценки целесообразности затрат на обеспечение безопасности АС?

9. Назовите категории затрат, связанных с безопасностью АС; кратко охарактеризуйте каждую категорию и перечислите статьи расходов для каждой из них.

ГЛАВА 2. ОСНОВНЫЕ ПОНЯТИЯ В ОБЛАСТИ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Прежде всего, необходимо понять, что же такое безопасность АС и определить *что (кого), от чего (от кого), почему (зачем), как (в какой степени и какими средствами) надо защищать*. Получив четкие ответы на данные вопросы, можно правильно сформулировать общие требования к системе обеспечения безопасности АС и перейти к обсуждению проблем построения соответствующих систем защиты. Основные понятия безопасности и их взаимосвязь приведены в ГОСТ Р ИСО/МЭК15408-1–2012 «Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий».

2.1. Определение безопасности автоматизированных систем

Что же такое безопасность вообще и безопасность АС в частности? Нередко можно слышать, что безопасность — это отсутствие опасностей. Данное определение не совсем верно, поскольку полностью устранить все возможные опасности нельзя.

Безопасность — это защищенность от опасностей, более точно, защищенность от возможного ущерба, наносимого при реализации этих опасностей (угроз).

Различают материальный, моральный и физический ущерб. Ущерб может быть причинен как напрямую, так и косвенно. *Субъектами нанесения ущерба, в конечном счете, всегда являются люди*. Даже если пострадают материальные объекты или информационные ресурсы, косвенный ущерб, проблемы возникнут у пользователей, каким-либо образом связанных с этими объектами или заинтересованных в их сохранности и целостности. И чем с бóльшим числом объектов человека что-то связывает, тем в большей опасности для косвенного нанесения ущерба он находится.

Косвенный ущерб интересам пользователя может быть нанесен либо путем сбоя нормального функционирования автоматизированной системы, либо за счет нарушения необходимых свойств отдельных компонентов и ресурсов АС, среди которых не только непосредственно информация, но и ее носители (устройства хранения, обработки, передачи данных), а также процессы обработки и передачи информации.