УДК 004.056(075.8)
ББК 32.973-018.2я73
У31

У31 Удостоверяющие автоматизированные информационные системы и средства. Введение в теорию и практику: учеб. пособие / С. В. Баушев, И. В. Аристархов, О. Ю. Гаценко и др.; под ред. С. В. Баушева, А. С. Кузьмина. — СПб.: БХВ-Петербург, 2016. — 304 с.: ил.

ISBN 978-5-9775-3733-9

В учебном пособии рассматривается новый класс автоматизированных информационных систем, реализующих функционал обеспечения доверия к циркулирующим в них данным. Исследуются модели их функционирования в условиях априорной неопределенности поведения предполагаемых нарушителей информационной безопасности и методы повышения уровня информационной безопасности.

Издание предназначено для специалистов в области разработки и создания защищенных автоматизированных систем, студентов и аспирантов, а также может быть полезным для научных работников, ведущих исследования в различных областях информатики.

УДК 004.056(075.8)
ББК 32.973-018.2я73

Авторский коллектив: д-р воен. наук, проф. *С. В. Баушев*, д-р физ.-мат. наук, проф. *А. С. Кузьмин*, д-р техн. наук, ст. научн. сотр. *О. Ю. Гаценко*, канд. техн. наук *И. В. Аристархов*, канд. техн. наук, доц. *А. В. Самонов*, *С. Н. Камышев*, канд. техн. наук *И. Е. Горбачев*, канд. техн. наук, доц. *А. Г. Сабанов*, канд. техн. наук *С. В. Максимов*, д-р техн. наук *С. Г. Синев*, канд. техн. наук *Н. В. Нездоровин*, *Г. Б. Маршалко*.

Рецензенты:

П. Д. Зегжда — д-р техн. наук, проф., заслуженный деятель науки РФ;
А. В. Черемушкин — д-р физ.-мат. наук, проф.;
Н. В. Никонов — канд. физ.-мат. наук.

ISBN 978-5-9775-3733-9

СОДЕРЖАНИЕ

Теория без практики — мертва и бесплодна,
практика без теории — слепа и бесполезна.

П. Чебышев,
русский математик XIX века

ВВЕДЕНИЕ

Современный этап развития человеческой цивилизации принято характеризовать как постиндустриальный, то есть переходный от индустриального к информационному, когда снижается доля и значение промышленного производства за счет роста сферы услуг и информации. В свою очередь, формирование области информационной экономики явилось результатом развития и широкого применения автоматизированных информационных систем (АИС).

Вопросу защищенности автоматизированных информационных систем различного назначения посвящено достаточно много научных и практических работ. Однако при этом вопросы возможности подлога информации, навязывания ложной информации, проверки подлинности документов, сигналов, сообщений, данных и подобные им оставались до последнего времени, по нашему мнению, без должного глубокого научного изучения. Отдельно здесь следует обозначить и такую актуальную прикладную область как автоматизированные системы управления войсками и оружием, особенно оружием роботизированным, когда достоверность приказов, команд, сигналов боевого управления и взаимного опознавания играет особую роль.

В подтверждение актуальности поднимаемых вопросов можно утверждать, что существует проблемная ситуация, состоящая в том, что:

– с одной стороны, пользователь АИС хотел бы иметь средство удостовериться в подлинности принимаемой информации, то есть доверять тем данным, которые им получены (присланы в его адрес), а также доверять и соответствующему источнику данных, каналу связи и т. д. и,

– с другой стороны, налицо относительное несовершенство соответствующих средств обеспечения доверия.

Этот аспект информационной безопасности – назовем его доверием или доверительностью в зависимости от контекста – нуждается в самостоятельном научном изучении.

Цель издания состоит во введении в научный оборот нового класса АИС, обеспечивающих доверие к циркулирующим в них документам и сигналам управления через выявление нового показателя качества информации – подлинность происхождения, и введение нового свойства АИС – доверительности, обеспечиваемой реализацией дополнительных функций обеспечения доверия к АИС и циркулирующим в ней данным.

Объектом исследований настоящего издания будут являться АИС, реализующие специальный функционал обеспечения доверия к циркулирующим в ней данным, а предметом исследований – модели их функционирования в условиях априорной неопределенности о поведении предполагаемых нарушителей информационной безопасности и методы повышения уровня информационной безопасности.

Для обеспечения определенной степени доверия к процессам хранения, передачи и обработки электронных документов (и сигналов управления) в настоящее время используются специализированные автоматизированные системы, называемые центрами доверия, которые сегодня представлены в основном удостоверяющими центрами.

Юридическим основанием для использования удостоверяющих центров являются Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Появление юридической базы обусловило становление на территории РФ свыше 300 удостоверяющих центров [81], общее представление об облике которых можно получить, например, из [81, 133].

Распространенность подобных систем в настоящее время можно охарактеризовать как ограниченное использование накануне широкомасштабного внедрения. В системном же научно-теоретическом плане эта область находится в стадии становления, хотя отдельные ее стороны, такие как, например, асимметричное шифрование на основе так называемых открытых ключей, являются интенсивно развивающими ветвями криптографии.

Приходится признать, что монографий и статей системного характера в этой специфической области недостаточно – так, можно назвать лишь учебник [103] и монографию [106], а также разрозненные электронные ресурсы.

Исследования вероятностно-временных характеристик, методов оценки эффективности функционирования компонентов информационных систем достаточно длительное время интенсивно ведут-

ся и развиваются в России и за рубежом. Изучение теоретических и прикладных проблем проводилось как на уровне распределенных информационных систем и сетей массового обслуживания (например, работы В. Столлингса [130], Л. Клейнрока [88, 95], О. Боксмы [78], Башарина Г. П. [51, 52], Советова Б. Я. [128], Захарова Г. П. [84], Вишневского В. М. ([57] и др.), так и на уровне инфраструктуры УЦ ([106] и др.). Однако существующие аналитические и имитационные модели вычислительных систем, реализующих функционал УЦ, в основном предназначены для оценки эффективности функционирования сетевых справочников и средств издания списка отозванных сертификатов и недостаточно точно отражают реальные процессы и особенности функционирования систем подтверждения подлинности электронной подписи в условиях информационных угроз.

Именно поэтому авторы взяли на себя труд систематизировать существующие научно-практические подходы и развить теоретические основы защиты информации в направлении нового класса информационных систем – удостоверяющих АИС (УАИС).

Книга состоит из восьми разделов и двух приложений, в комплексе рассматривающих как основные этапы и стадии жизненного цикла удостоверяющих АИС, так и акцентирующих особое внимание в отдельное исследование наиболее специфические аспекты их функционирования.

Первый раздел «Место доверенных АИС в общей системе автоматизированных систем» имеет характер системно-постановочного, в котором приводится классификация существующих АИС, вводятся дополнительные новые классификационное признаки, устанавливаются новые свойства-атрибуты удостоверяющих АИС, а также с позиций теории технической диагностики формализуются основные состояния удостоверяющих АИС. Рассматривается понятие единого пространства доверия электронной подписи (далее единое пространство доверия) и исследуются основные подходы к его реализации.

Второй раздел «Анализ показателя доверительности и системно-функциональная модель УЦ» имеет целью исследование введенного в научный оборот в первом разделе показателя доверительности, его декомпозицию на составные элементы и, затем, анализ проблем и путей обеспечения (реализации) требований по назначению показателя. Конструируются облик юридически значимой системы электронного документооборота и системно-функциональная модель удостоверяющего центра как главного элемента инфраструктуры.

В третьем разделе «Разработка модели угроз для элементов ЕПД, построенного на основе технологии инфраструктуры открытых

ключей и удостоверяющих центров» с единых системных позиций методологии управления рисками рассматриваются вопросы идентификации и оценки критичности рисков нарушения безопасности активов единого пространства доверия (ЕПД), определяются цели и возможности потенциальных нарушителей безопасности, а также предлагаются пути оценивания вероятности реализации угроз и потенциального ущерба. Отдельно описываются основные угрозы информационной безопасности удостоверяющих центров.

Четвертый раздел «Комплексные сетевые атаки на удостоверяющие АИС» содержит взгляд авторов на возможность проведения атаки как следствие наличия уязвимости в АИС, в нем приведена обобщенная модель внешнего нарушителя информационной безопасности. Вводятся понятия комплексных компьютерных атак, их профилей, излагаются основы классификации и анализа элементарных компьютерных воздействий и их совокупностей. Предлагаются методы и методики обнаружения комплексных сетевых атак на УЦ посредством построения профилей атак и их автоматизированного выявления в трафике АИС.

С учетом того факта, что в основе функционирования удостоверяющих АИС лежит использование криптографических методов, алгоритмов и устройств, логичным является наличие пятого раздела «Модели управления сертификатами ключей проверки электронной подписи и планирование контрольных мероприятий». Одним из важнейших аспектов при организации жизненного цикла ключевой информации является планирование ее смены. Существующие рекомендации по длительности использования ключевой информации не учитывают отличие возможностей нарушителя для различных информационных систем и влияние периодичности смены ключевой информации на загрузку отдельных подсистем электронного документооборота. В разделе рассматривается задача, состоящая в разработке научно-методического аппарата, позволяющего планировать процесс смены ключевой информации, и мероприятия инструментального аудита контроля их эффективности.

В шестом разделе «Модели и методы оценивания изменения защищенности АИС во времени» представлен оригинальный взгляд авторов на защищенность АИС как изменяющееся во времени соотношение числа обнаруживаемых нарушителем и перекрываемых администраторами АИС уязвимостей. Здесь разрабатывается и исследуется математическая, динамическая модель изменения защищенности и предлагаются методы оценивания уровня текущей

защищенности АИС. Отмечается, что противоборство пары «администратор сети – нарушитель безопасности» происходит в условиях априорной неопределенности об их возможностях и действиях, что предполагает использование в расчетах математического аппарата учета существующей неопределенности. Отмечено, что в ряде случаев противоборство и неопределенность могут быть отнесены к классу уникальных ситуаций, для которых целесообразно использовать не аппарат теории вероятностей, а иные подходы, например так называемой теории ожидаемостей [112].

Седьмой раздел «Практические рекомендации по применению удостоверяющих систем и средств» ориентирован на формулирование ряда прикладных задач, для которых рассмотренные подходы к обеспечению доверительности доведены до конкретных технических решений или концепций применения. В разделе присутствуют методические рекомендации по разработке и созданию структуры и программного обеспечения удостоверяющих центров, описание в качестве демонстрационного примера функционирования типового российского УЦ «Стандарт УЦ». Изложена концепция применения асимметричного шифрования и инфраструктуры открытых ключей для создания системы опознавания «свой–чужой», особенно актуальная, по мнению авторов, для перспективных роботизированных систем и средств. Здесь же намечены пути реализации единого пространства доверия, а также описан способ создания юридически значимых фотоснимков на основе снабжения их электронной подписью в цифровом фотоаппарате в момент фотографирования.

В восьмом разделе «Проблемные вопросы функционирования удостоверяющих АИС и пути их разрешения» рассмотрены организационные и технические вопросы и задачи, которые необходимо выполнить при придании УЦ статуса главного звена единого пространства доверия не только электронным подписям, но и электронным документам и сообщениям в целом. Рассматривается соотношение понятий «юридическая сила» и «юридическая значимость» электронных документов, выдвигаются требования как к электронному документу, так и сервисам, обеспечивающим его юридическую силу. Достаточно подробно изложены проблемы и пути достижения необходимых уровней доверия к процедурам идентификации и аутентификации. С учетом зарубежного опыта намечены перспективы развития удостоверяющих АИС в нашей стране.

Приложение 1 содержит классификацию неопределенностей, в которых функционирует и принимает решения руководящий

состав сложных организационно-технических систем и персонал АИС.

Приложение 2 представляет собой краткий аналитический обзор российских криптографических алгоритмов и основ их стандартизации, а также характеристику участия отечественной научной школы в формировании мировых подходов к обеспечению криптостойкости средств и алгоритмов.

Книга подготовлена творческим коллективом на основе многолетних научных и практических исследований как самих авторов, так и ряда научных коллективов под их руководством или при их участии в разные годы. Усилия соавторов были распределены следующим образом: доктор военных наук профессор Баушев С. В. – подразделы 1.1–1.4, 2.1, 2.5, 4.3, 4.4, 5.3.1, раздел 6, подраздел 7.5, Приложение 1; доктор технических наук старший научный сотрудник Гаценко О. Ю. – подразделы 4.3, 4.4, 5.2, 5.3, 7.5; доктор технических наук Синев С. Г. – подразделы 4.3, 4.4; кандидаты технических наук доценты Самонов А. В. – разделы 3 и 4, Горбачев И. Е. – подразделы 1.1, 1.4, 4.1, раздел 6; Максимов С. В. – раздел 5; кандидаты технических наук Аристархов И. В. – разделы 1, 2, 5, подраздел 7.1; Нездоровин Н. В. – подраздел 7.5; Сабанов А. Г. – раздел 8; Камышев С. Н. – подразделы 1.5, 1.6, 4.2, 7.1, 7.3, 7.4; Маршалко Г. Б. – Приложение 2.

Общая редакция издания выполнена академиком Академии военных наук, доктором военных наук профессором Баушевым С. В. и академиком Академии криптографии, доктором физико-математических наук профессором Кузьминым А. С.

Авторы выражают признательность рецензентам издания — заслуженному деятелю науки РФ, доктору технических наук П. Д. Зегжде, доктору физико-математических наук, профессору А. В. Черемушкину, кандидату физико-математических наук Н. В. Никонову, взявшим на себя труд внимательного изучения рукописи и в немалой степени способствовавшим улучшению содержания книги. Ряд замечаний и предложений был учтен и устранен в ходе подготовки к изданию, при этом часть из них, носящих дискуссионный характер, оставлена в авторском изложении.

Для подтверждения, что ... лицо, прибывшее с приказом от имени начальников ... действительно уполномочено на то соответствующим начальником, устанавливается пароль (секретное слово).

Ст. 129 Устава гарнизонной и караульной служб ВС РФ

1. МЕСТО ДОВЕРЕННЫХ АИС В ОБЩЕЙ СИСТЕМЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

1.1. Информационная безопасность и информационные угрозы

С учетом возрастающей роли информации в жизни общества, а также усиливающегося информационного противоборства имеет место вопрос о различии понятий, определяемых терминами «безопасность информации» и «информационная безопасность». В частности, предлагается вопросы безопасности информации увязывать в первую очередь с техническими аспектами парирования опасности, возникающей от различных источников. Иной аспект проблемы обеспечения безопасности возникает тогда, когда используется термин «информационная безопасность». Здесь, помимо технических, на передний план выходят чисто психологические проблемы, связанные с воздействием информации на сознание людей – их психику [85]. Отсюда следует, что понятие «информационная безопасность» шире понятия «безопасности информации», которое в свою очередь укладывается в понятие «безопасности» вообще.

Под **безопасностью** будем понимать ситуацию, в котором социальный субъект в настоящее время владеет благом и не видит причин для его потери в будущем [85].

Благо – это любые объекты желаний и стремлений какого-либо социального субъекта, наличие которых удовлетворяет его материальные и духовные потребности, а отсутствие побуждает его к совершению действий, направленных на получение данного блага [122].

Информационная безопасность – ситуация, в которой социальный субъект владеет благом в виде достоверной и неустаревшей

информации, может на ее основании прогнозировать результаты своих действий, поступков, поведения и деятельности в целом и не видит причин потери этого блага в пределах интервала прогноза.

Представим несколько основных на наш взгляд определений понятия *безопасность информации*.

В [71] безопасность информации – состояние защищенности информации, обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз.

В [70] безопасность информации – состояние защищенности информации от различных угроз.

В [58] указывается, что безопасность информации есть составное свойство, включающее в себя защищенность информации (свойство КСЗ), надежность аппаратуры, надежность программного обеспечения (ПО), безошибочность действий персонала (свойство персонала).

Заметим, что безопасность информации, применительно к техническим системам, кроме противоборства систем защиты информации (СЗИ) и систем информационного нападения (СИН) в информационном конфликте, отражает и другие аспекты качества обрабатываемой, передаваемой и хранимой информации в автоматизированной системе (АС). Действительно, на свойства информации могут влиять, например, критические отказы аппаратных средств, что характеризует связь свойства «безопасность информации» с технической надежностью. Кроме того, аналогичные связи существуют между безопасностью информации и надежностью программных средств, физической, семантической устойчивостью информации, безошибочностью действий персонала. Эти связи определяются внутренними возмущающими воздействиями, специфика же защищенности состоит в том, что это свойство, являясь по существу свойством КСЗ, определяется в основном под влиянием внешних деструктивных воздействий нарушителя [58].

Следовательно, в более широком понимании целесообразно принять следующее определение безопасности информации.

Безопасность информации – это свойство АС, позволяющее в определенных ситуациях обеспечить санкционированным пользователям информационную безопасность путем разработки и внедрения аппаратно-программных средств защиты информации (СЗИ) и проведения организационных мероприятий по защите АС от несанкционированных действий противника, а также сбоев в аппаратуре и помех в каналах связи.

Конечно, следует учитывать, что СЗИ сама представляет собой распределенный аппаратно-программный комплекс, причем часто

в той или иной мере использующий аппаратные и программные средства базовой структуры АС, а также физическое, структурное и семантическое представление информации (криптографические методы).

В свою очередь, декомпозиция свойства «защищенность информации» в соответствии с целями системы информационного нападения (СИН) по отношению к объектам защиты позволяет выделить элементарные информационные свойства – конфиденциальность, целостность, доступность. При этом, заметим, данные свойства зависят как от защищенности, так и от других составляющих безопасности информации. Применительно к свойству защищенности информации простейшие свойства определяются способностью системы защиты достигать той или иной степени соответствующих элементарных целевых эффектов, заключающихся в препятствии системе нападения получать, разрушать или блокировать информацию [58].

Из вышесказанного следует, что в узком понимании под **безопасностью информации** будем понимать ее свойство именно сохранять состояние защищенности информации АС, так как:

– основной угрозой безопасности информации являются несанкционированные действия нарушителя, а специфика же защищенности информации состоит как раз в том, что это свойство, являясь по существу свойством комплекса средств защиты информации (КСЗ), определяется в основном под влиянием внешних деструктивных воздействий;

– состояние защищенности АС представляет собой временной срез свойства «защищенность информации» и описывается значениями соответствующих показателей в фиксированный момент времени.

Таким образом, будем различать безопасность от физического воздействия и информационную безопасность. Первый вид безопасности связан с защитой от реальных источников опасности, воздействующих непосредственно на «тело» объекта опасности или на его аппаратно-программные средства. В частности, к средствам физического воздействия могут быть отнесены образцы военной техники и оружия, подслушивающая аппаратура, станции радиопомех и сами помехи, «фомки» у взломщиков сейфов и т. д.

Теперь, исходя из вышеизложенного, можно сделать следующие выводы:

– *защищенность информации* является свойством КСЗ АС достигать целевого эффекта при взаимодействии с СИН;

– в динамических моделях состояние защищенности АС представляет собой временной срез свойства «*защищенность инфор-*

мации» и описывается значениями соответствующих показателей в фиксированный момент времени;

– в более широком смысле *безопасность информации* есть свойство АС в определенных ситуациях обеспечить санкционированным пользователям информационную безопасность путем разработки и внедрения аппаратно-программных средств и проведения организационных мероприятий по защите АС от несанкционированных действий противника, а также сбоев в аппаратуре и помех в каналах связи;

– в узком понимании под *безопасностью информации* будем понимать ее свойство сохранять состояние защищенности информации АИС.

На элементарные информационные свойства помимо свойства защищенности АС, влияют и другие свойства, такие как техническая надежность, надежность программных средств, безошибочность действий персонала (свойство персонала).

1.2. Доверительность как новое свойство АИС

Анализ существующих взглядов на защищенность информации показывает, что основное внимание теоретических и практических разработок ориентировано на защищенность уже созданных законными пользователями легитимных данных. По понятным причинам пристальное внимание при проектировании современных АИС, особенно АИС специального назначения, уделяется вопросам подобного рода защиты информации, что нашло свое отражение в появлении теории защиты информации, а также понятия «защищенные информационные системы», наделенных своей системой свойств.

В соответствии с методологией системного анализа одним из основных этапов познания и проектирования сложных объектов является выделение и исследование их свойств. Свойство – это объективная особенность объекта, зависящая от его строения и характеризующая отдельную его сторону (аспект) [114]. В этом плане у АИС различного назначения также принято выделять как отдельные свойства, так и их совокупности, характеризующие качество АИС. Они могут меняться с течением времени, соответствуя переходам объекта из одного состояния в другое. Защищенность информации не является собственно только свойством определенного количества информации в отличие от, например, ценности, полноты и т. д., а зависит как от характеристик функционирования системы защиты, так и от характеристик функционирования системы нападения [58].

Однако, на наш взгляд, вопросы защиты информации часто рассматриваются однобоко, что отражается в неполноте общепринятой системы свойств АИС. Неполнота, по нашему мнению, состоит в недостаточном учете такого аспекта информации как доверие к ней. В настоящее время сложилась определенная система взглядов на свойство защищенности данных в автоматизированных информационных системах в ряду других свойств более высокого уровня, таких как: устойчивость, живучесть, безопасность, надежность и помехоустойчивость – рис. 1.1.

Традиционно под защищенной понимается АИС, в которой реализован комплекс средств защиты [123], обобщенная модель которой в условиях применения злоумышленником специальных организационно-технических мер программно-технических средств (информационного оружия) представлена на рис. 1.2.

Однако при подобном подходе вопросы возможности подлога, навязывания ложной информации (дезинформации), проверки

Рис. 1.1. Защищенность данных как свойство АИС

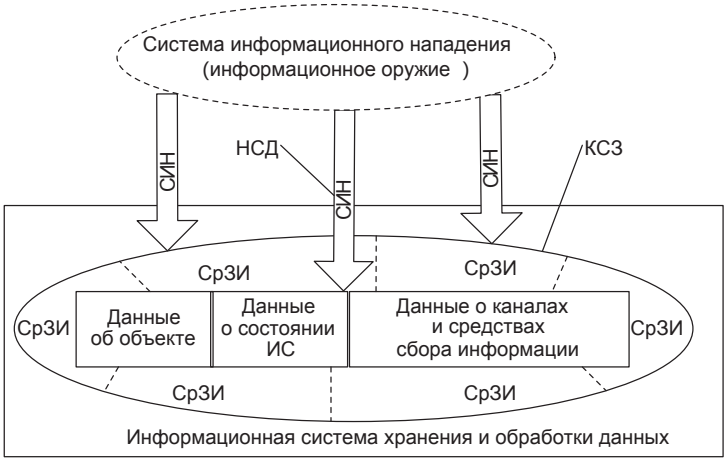

Рис. 1.2. Обобщенная модель защищенной АИС в условиях информационного противоборства: КСЗ – комплекс средств защиты; СрЗИ – средство защиты информации; СИН – средство информационного нападения; НСД – несанкционированный доступ

подлинности (целостности и авторства) создаваемых документов оставались до последнего времени без должного внимания. При этом понятно, что пользователь АИС доверяет (или хотел бы доверять) тем данным, которые им получены (присланы в его адрес), а также доверять и соответствующему источнику данных, каналу связи и т. д.

В подтверждение важности и злободневности поднимаемых вопросов доверия к информации можно привести ряд известных примеров и проблемных ситуаций:

– 17 июня 2007 года чешское телевидение вышло с сенсационным сообщением о ядерном взрыве, якобы происшедшем близ города Есеник в Северной Моравии. При этом на телеэкранах появились вполне реальные кадры атомного гриба – рис. 1.3;

– летом 2009 года сотрудники ГИБДД одной из территорий страны наблюдали не реальную картину с видеокамер, а их более раннюю запись, прокручиваемую фирмой, осуществлявшей техническое обслуживание видеокамер в период их временной неработоспособности;

– 14 января 2010 года в центре Москвы на Садовом кольце в районе Серпуховского тоннеля на рекламном видеоэкране в течение 18 минут крутился двухминутный ролик порнографического содержания;

– 3 февраля 2013 года Член Молодежной палаты муниципалитета Орехово-Борисово г. Москвы Ю. Урсу пожаловался на портале правительства Москвы «Наш город» на плохую уборку улиц от снега. На следующий день администрация сайта сообщила, что проблема решена и вывесила фото расчищенного участка. Однако Урсу обнаружил [134], что изображение откорректировано при помощи графического редактора – рис. 1.4;

– чтобы быть юридически признаваемым документом фотоснимки, аудиозаписи и т. п. электронные документы нуждаются в защите от подделки, а также в защите авторства, для чего часто используются так называемые цифровые водяные знаки (ЦВЗ), которые могут быть как видимыми, так и невидимыми на защищаемом изображении – рис. 1.5;

– в 2001 году согласно выводам международного авиационного комитета во время учений украинскими военными был произведен пуск ракет зенитно-ракетной системы С-200 по учебным целям. В результате «рокового стечения обстоятельств» одна из зенитных ракет ошибочно захватила не учебную цель, а пассажирский самолет Ту-154М авиакомпании «Сибирь». Все 78 пассажиров и члены экипажа, находившиеся на борту, погибли. В системном плане это событие можно трактовать как пример того, что средства системы опознавания «свой-чужой» (рис. 1.6), разработанные на научно-технических решениях симметричного шифрования середины прошлого века, нуждаются в дальнейшем совершенствовании и применении новых подходов как с целью расширения множества опознаваемых объектов и средств опознавания, так и с целью установления соответствия сетецентрической организации современных боевых действий [98].

Поднятый здесь аспект информационной безопасности – в отличие от защищенности информации, назовем его защищенностью пользователей (от ложной (подложной) информации, от информационного мусора, шума и т. д.) – еще нуждается в самостоятельном научном изучении. В целом же теперь представляется возможным говорить о целесообразности введения еще одного свойства информационной безопасности – защищенности пользователя от неверной и ненужной информации, а также от «лишних» источников информации и пр. Иными словами, это свойство должно характеризовать реализуемую степень доверия пользователей АИС к, скажем, функционирующему электронному документообороту. Чтобы избежать путаницы с существующим понятием «защищенность данных», ориентированным прежде всего на их охрану от злоумышленников

Рис. 1.3. «Ядерный взрыв» на чешском телевидении

Рис. 1.4. Откорректированное в графическом редакторе и реальное изображение объекта приборки ЖКХ

Рис. 1.5. Пример внедренных видимых цифровых водяных знаков

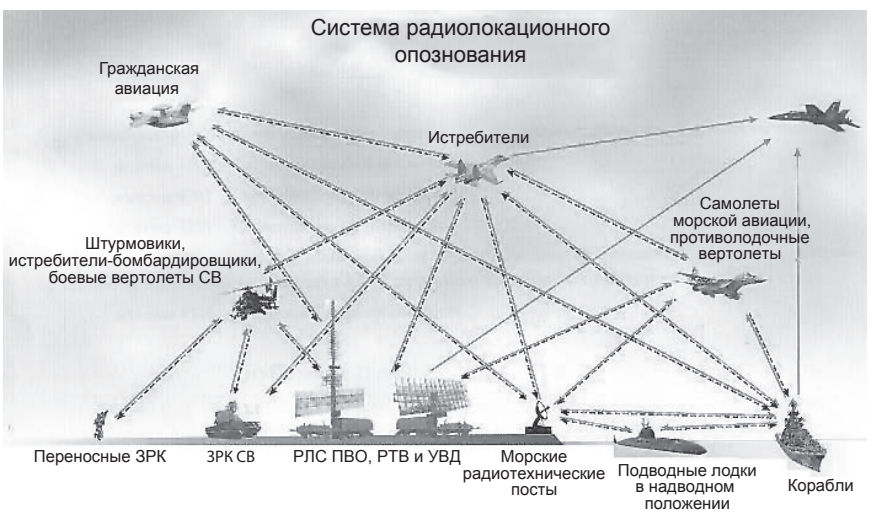

Рис. 1.6. Иллюстрация к существующей системе радиолокационного опознавания «свой-чужой»

и отказов (сбоев) технических средств, ниже будет введено понятие **«доверительность»**, которое может иметь отношение к данным, АИС в целом, принимаемым организационно-техническим решениям и т. д. и существовать на нескольких иерархических уровнях. Дополнив систему свойств АИС новым свойством, получим следующее его иерархическое положение в общей системе свойств АИС – рис. 1.7.

Сформулируем в самом общем виде определение доверительности как свойства АИС, характеризующего ее способность к организации обмена данными между пользователями, обеспечивающего однозначную и надежную идентифицируемость авторов (источников данных), аутентификацию потребителей (получателей) и подтверждение неискажаемости содержания информации (*примечание: сами данные могут быть изменены, например, кодированы*).

Следует понимать, что по существу говорится здесь об удостоверении подлинности происхождения информации (сведений, данных, документов и т. д.), которое гарантирует не ее достоверность,

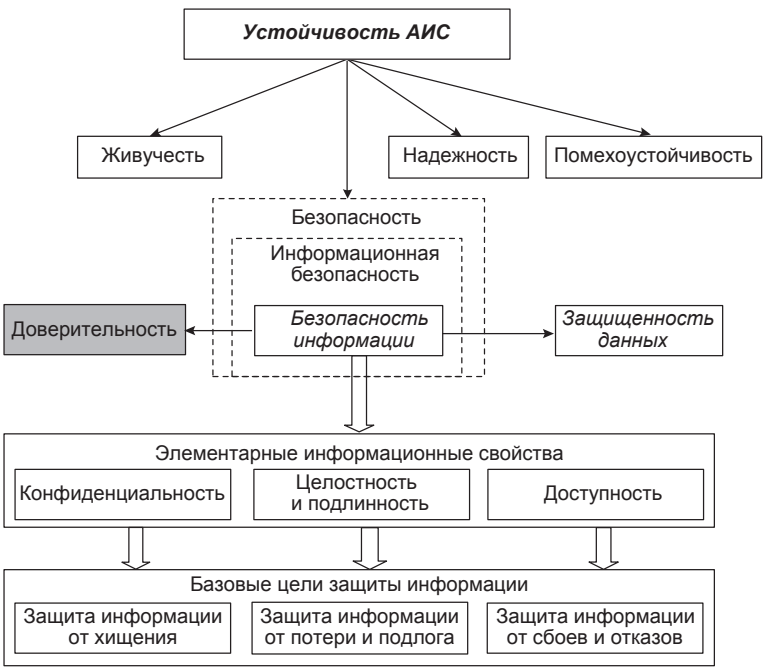

Рис. 1.7. Дополненная «доверительностью» система свойств АИС

а лишь факт того, что данная информация порождена (передана) конкретным источником и, возможно, не нарушены ее конфиденциальность и целостность. То есть достоверность информации отнюдь не обеспечивается удостоверением (свидетельствованием) ее подлинности – подобно тому, как нотариус заверяет подлинность копии представленному документу, не вникая в его существо и правдивость.

Таким образом, следует различать функции защиты данных и функции удостоверения подлинности циркулирующих документов. Между ними может быть некоторое сходство в механизмах реализации, но назначение – различным. Именно наличие подобной функции свидетельствования, в первую очередь, должно отличать системы доверенного электронного документооборота от просто защищенных информационных систем.

Другими словами, одним из составляющих свойств качества информации предлагается полагать (см. подраздел 1.4) подлинность происхождения, которая лежит в основе доверительности информационного обмена и которое может складываться из некоторых элементарных свойств и обеспечиваться функционированием ряда специальных механизмов АИС.

В совокупности это все позволяет говорить о введении в теорию и практику защиты информации новой научной категории – доверенные автоматизированные системы, которые и будут являться далее объектом исследования настоящего издания.

1.3. Классификация АИС и подлинность происхождения как показатель качества информации

С целью последующего формирования единого тезауруса (понятийного аппарата) следует заметить, что в настоящее время параллельно используются два термина – автоматизированная система («гостированный» термин) и информационная система (научно-популярный).

Автоматизированная система (АС) представляет собой [120] «систему, состоящую из персонала и комплекса средств автоматизации его деятельности, реализующую информационную технологию выполнения установленных функций, то есть организационно-техническую систему, обеспечивающую выработку решений на основе автоматизации информационных процессов в различных сферах деятельности или их сочетаниях».

Автоматизированные системы реализуют информационный процесс как определенную последовательность информационно

связанных функций, задач или процедур, выполняемых в автоматизированном (интерактивном) или автоматическом режимах. В зависимости от сферы автоматизируемой деятельности АС разделяют на [120]:

– автоматизированные системы управления (АСУ);
– АС обработки и передачи информации;
– системы автоматизированного проектирования (САПР);
– АС научных исследований;
– АС технологической подготовки производства;
– АС контроля и испытаний;
– АС, автоматизирующие сочетания различных видов деятельности.

Когда хотят подчеркнуть именно информационный аспект АС, то используют термин «автоматизированная информационная система» (иногда: информационно-вычислительная система). Тогда в общем виде под этим термином понимают системы сбора, накопления, хранения, поиска, передачи, обработки информации с использованием вычислительной техники, компьютерных информационных сетей, средств и каналов связи.

Собственно информационные системы также можно классифицировать по ряду признаков. В основу примененной (взятой за основу совокупности существовавших [120, 122] и дополненной) классификации положены наиболее существенные признаки, определяющие функциональные возможности и особенности построения современных систем:

• По типу хранимых данных ИС делятся на фактографические и документальные. *Фактографические системы* предназначены для хранения и обработки структурированных данных в виде чисел и текстов. Над такими данными можно выполнять различные операции. *В документальных системах* информация представлена в виде документов, состоящих из наименований, описаний, рефератов и текстов. Поиск по неструктурированным данным осуществляется с использованием семантических признаков. Отобранные документы предоставляются пользователю, а обработка данных в таких системах практически не производится.

• По степени автоматизации информационных процессов системы делятся на ручные, автоматические и автоматизированные. *Ручные ИС* характеризуются отсутствием современных технических средств переработки информации и выполнением всех операций человеком. *В автоматических ИС* все операции по переработке информации выполняются без участия человека. *Автоматизирован-*

ные ИС предполагают участие в процессе обработки информации и человека, и технических средств, причем главная роль в выполнении рутинных операций обработки данных отводится компьютеру. Именно этот класс систем соответствует современному представлению понятия «информационная система».

• По характеру обработки данных ИС предлагается разделить на информационно-поисковые, информационно-решающие, информационно-аналитические и информационного взаимодействия. *Информационно-поисковые системы* (иногда: информационно-справочные) производят ввод, систематизацию, хранение, выдачу информации по запросу пользователя без сложных преобразований данных (например, ИС библиотечного обслуживания, резервирования и продажи билетов на транспорте, бронирования мест в гостиницах и пр.). *Информационно-решающие* системы осуществляют, кроме того, операции по переработке информации по определенному алгоритму. По характеру использования выходной информации такие системы принято делить на управляющие и советующие. Результирующая информация управляющих ИС непосредственно трансформируется в принимаемые человеком решения. Для этих систем характерны задачи расчетного характера и обработка больших объемов данных (например, ИС планирования производства или заказов, бухгалтерского учета). Советующие ИС вырабатывают информацию, которая принимается человеком к сведению и учитывается при формировании управленческих решений, а не инициирует конкретные действия. Эти системы имитируют интеллектуальные процессы обработки знаний, а не данных (например, экспертные системы). *Информационно-аналитические системы* осуществляют в интересах семантического анализа различные виды обработки информации и данных, начиная от статистической обработки данных, заканчивая поиском закономерностей, зависимостей, например, используя процедуры дата-майнинга, визуализации обстановки и т. д. *Системы информационного взаимодействия* ориентированы на организацию и поддержание информационного взаимодействия пользователей, то есть обмена различного рода информацией. При этом системы связи и передачи данных выступают здесь лишь в качестве транспортной подсистемы, окруженной рядом других подсистем, например, делопроизводства, сбора данных, представления информации и др. В свою очередь, системы информационного взаимодействия можно разделить на системы обмена информацией и системы распределения информации (информационные агентства, порталы и т. п.). Среди систем обмена информа-

цией целесообразно выделить как отдельный класс системы обмена документами.

Отсюда следует, что можно выделить некоторый класс автоматизированных информационных систем, сочетающих признаки систем документального типа, автоматизированных, информационного взаимодействия, ориентированных на обмен документами в электронном виде, или *систем электронного документооборота* – специализированных АИС, которые обеспечивают строго регламентированное и формально контролируемое движение документов внутри и вне организации на основе информационных и коммуникационных технологий.

Примечание 1. Здесь следует упомянуть, что близкие по звучанию системы делопроизводства и документооборота – это не одно и то же. Технологии электронного делопроизводства и электронного документооборота являются разными типами систем, поддерживающих и автоматизирующих работу с документоориентированной информацией [126].

Системы электронного делопроизводства обеспечивают работу с электронными версиями документов и реквизитами регистрационно-контрольных форм в соответствии с принятыми в стране правилами и стандартами делопроизводства.

Если основным назначением систем делопроизводства является документальная регистрация тех или иных свершившихся действий и событий (например, «Документ принят к исполнению», «Документ передан на исполнение конкретному сотруднику», «На документ дан соответствующий ответ» и т. д.) в соответствии с принятыми правилами, то системы документооборота не только регистрируют действия и события, но и поддерживают сами процессы работы над документами.

С точки зрения пользователей систем автоматизации можно сказать, что пользователями систем автоматизации делопроизводства являются сотрудники таких структурных подразделений компании, как управление делами, секретариаты, канцелярии, общие отделы, экспедиции (10–15% сотрудников организации). Пользователями систем, автоматизирующих деловые процессы, связанные с документами (например, работа с «обращениями граждан», договорами, подготовка заседаний и др.), являются отдельные сотрудники многих подразделений, вовлеченных в общий деловой процесс (40–50% сотрудников организации). Пользователями систем электронного документооборота являются прак-

тически все сотрудники из разных подразделений организации (до 80% сотрудников компании) [104, 126].

Примечание 2. Здесь следует отметить, что понятия «электронный документ» и «документ в электронном виде» до настоящего времени строго не определены.

Ключевое место в АС занимает конечный пользователь – должностное лицо, решающее функциональные, то есть конечные, целевые задачи и вырабатывающее (принимающее) необходимые решения. Задачи, решаемые в автоматизированной системе с целью обеспечения выполнения функциональных задач, называются обеспечивающими или вспомогательными. Они решаются программирующими пользователями, или эксплуатационным персоналом АС. Традиционно к ним относят: [121, 77]:

– сбор данных – получение по каналам связи информации от оконечных устройств, датчиков и т. д.;

– накопление данных на материальных носителях. Процесс формирования первичного, несистематизированного массива информации называется ее накоплением;

– хранение данных – процесс переформирования исходной информации и поддержания его в виде, обеспечивающем выдачу данных по запросам пользователей в установленные сроки;

– обработка данных по специальным алгоритмам, обеспечивающая выполнение вспомогательных или функциональных задач, например, автоматизированная подготовка технических отчетов за сутки;

– выдача данных по запросам пользователей в виде, удобном для их анализа или интерпретации;

– управление средствами и системами АС, представляющее собой процессы администрирования в сетях передачи информации и вычислительных сетях, эксплуатации технических и программных средств АС, защиты информации и т. д.;

– организация и поддержание в работоспособном состоянии каналов связи, позволяющих передавать необходимые объемы управляющей, аналитической и другой информации с требуемыми достоверностью, своевременностью, надежностью и т. д.

Представляется необходимым подчеркнуть, что потребитель предъявляет особые требования к *качеству информации*, под которым следует понимать совокупность свойств информации, характеризующих степень ее соответствия потребностям (целям, ценностям) пользователей (средств автоматизации, персонала АС и др.).