

ОБЕСПЕЧЕНИЕ ГАРАНТИЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

В статье рассматриваются вопросы обеспечения комплексной безопасности информационных систем в соответствии с общими критериями безопасности информационных технологий.

назначенное для автоматизации решения прикладных задач или технологических процессов;

2. Программно-техническую инфраструктуру (серверное оборудование, система телекоммуникаций, автоматизированные рабо-

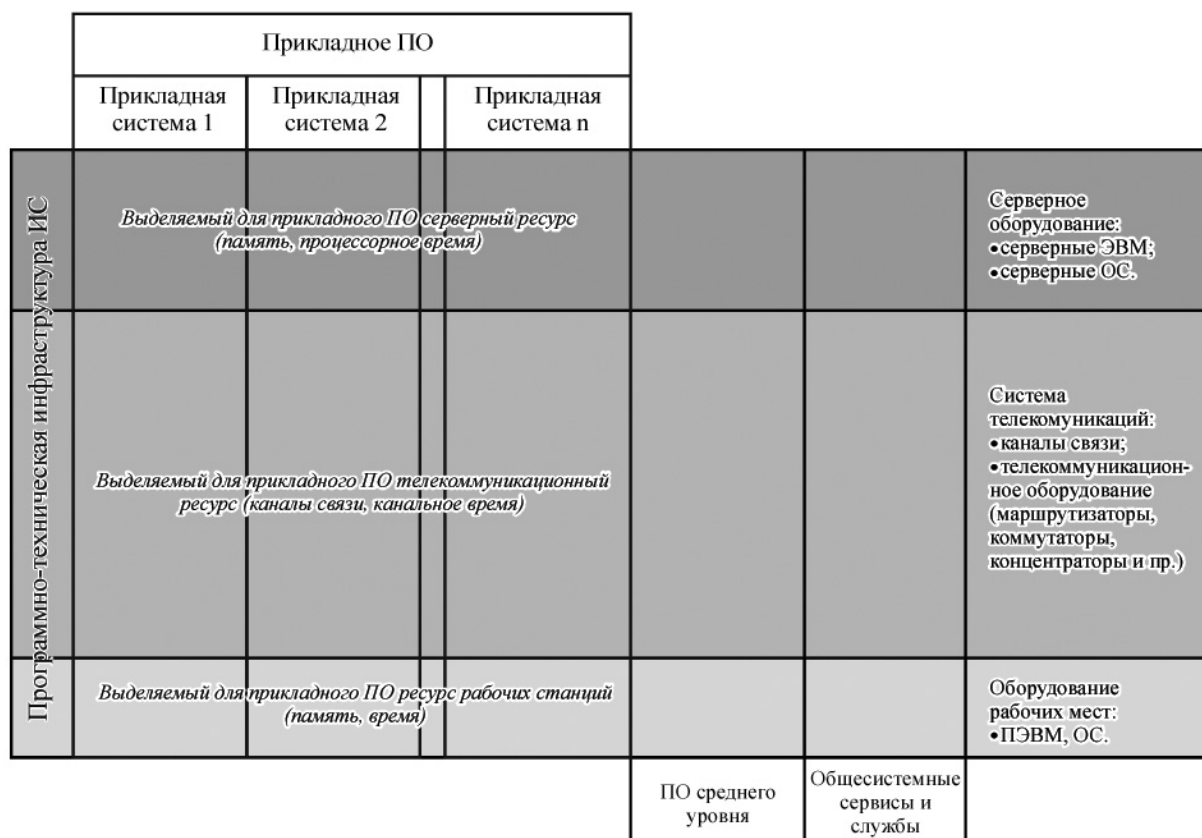


Рис. 1 Обобщенная модель ИС ресурсного типа.

В информационной системе (ИС) целесообразно выделять две составляющих:

1. Прикладное ПО, пред-

чисе места, системные сервисы и службы, ПО среднего уровня), которая предоставляет необходимые ресурсы (вычислительные, коммуникационные, сервисные и пр.) для функциони-



рования прикладного ПО и взаимодействия с ним пользователей.

Обобщенная модель ИС ресурсного типа представлена на рис. 1.

Объектом защиты в ИС являются как ресурсы и системные данные инфраструктуры, так и прикладное ПО и обрабатываемая им информация (данные), которые в совокупности составляют активы ИС.

Безопасность ИС, как объекта информационных технологий (ОИТ), характеризуется доступностью, целостностью и конфиденциальностью активов [2,3].

Доступность есть свойство, характеризующие возможности системы предоставлять необходимые ресурсы (вычислительные, коммуникационные, информационные, функциональные) авторизованным субъектам (пользователям, процессам) в требуемое им время. Доступность активов ИС является основой обеспечения непрерывности процессов деятельности, автоматизированных с использованием данной ИС.

Целостность данных является свойством, характеризующим, что данные не изменены неавторизованным образом в процессе их обработки, передачи и хранения в системе.

Системная целостность характеризует способность ИС выполнять предназначенные ей функции неизменным образом, отсутствие неавторизованных изменений в системе.

Конфиденциальность характеризует возможности по предоставлению доступа к активам системы только авторизованным субъектам.

Перечисленные выше свойства безопасности ИС достигаются использованием различных механизмов и средств безопасности.

Постоянная доступность ресурсов ИС достигается применением целого комплекса организационных и технических мер, предусмотренных на случаи возникновения сбоев и отказов оборудования, ошибок в функционировании ПО, нарушений в системе энергоснабжения, актов вандализма и т.д. Эти меры направлены на поддержание непрерывности функционирования системы в критических ситуациях и/или на обеспечение восстановления работоспособности системы и вычислительных процессов за время, приемлемое для деятельности пользователей системы. Как правило, для обеспечения необходимого уровня доступности ресурсов ИС широко используют различные способы организации избыточности ресур-

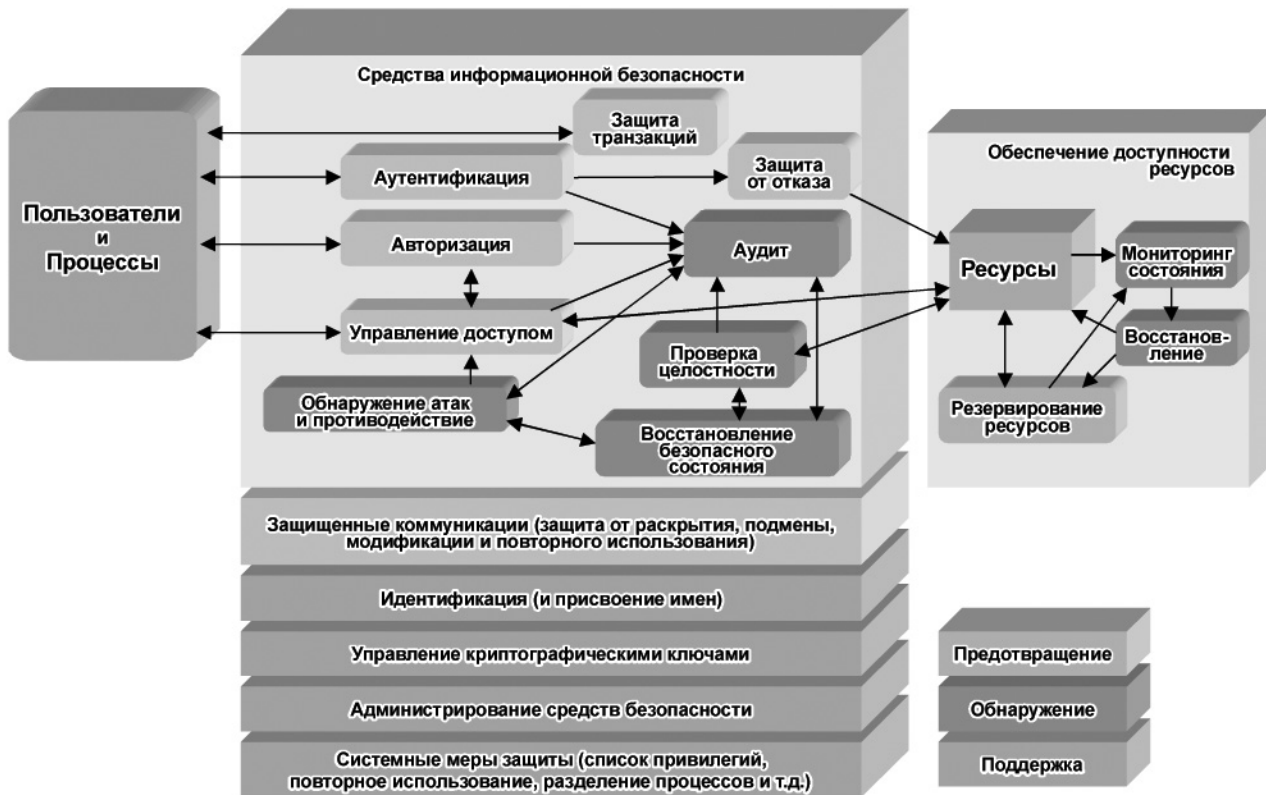
сов путем резервирования наиболее критичных ее компонентов. В наиболее критичных ИС, например, создаются резервные вычислительные центры, которые обеспечивают непрерывность функционирования ИС даже в катастрофических ситуациях. На случай возникновения критических ситуаций в системе заблаговременно должен разрабатываться план восстановления доступности ресурсов ИС, предусматривающий как организационные мероприятия по восстановлению, так и технические меры поддержки возможности восстановления оборудования, баз данных и вычислительных процессов.

Обеспечение целостности данных достигается применением различных программных, программно-аппаратных и аппаратных средств защиты целостности данных, в том числе криптографическими методами, в процессе их хранения, передачи и обработки.

Обеспечение системной целостности ИС достигается применением комплекса организационных мер и технических средств, препятствующих несанкционированному изменению в системе и режимов ее функционирования. К подобным средствам, например, могут быть отнесены такие средства управления ресурсами информационной системы как Tivoli. Для поддержки целостности системы должны быть также выработаны соответствующие организационные политики безопасности.

Для обеспечения необходимого уровня конфиденциальности активов ИС используются как организационные меры, так и технические средства. Среди технических средств защиты ресурсов ИС используются средства защиты от несанкционированного доступа (средства идентификации и аутентификации субъектов, средства управления доступом и пр.), а для защиты конфиденциальности данных используются, кроме того, и криптографические средства. Защита конфиденциальности активов должна поддерживаться соответствующими организационными политиками безопасности.

В ИС должен вестись учет всех ее активов, а также операций, выполняемых авторизованными субъектами с активами. Это позволяет контролировать выполнение субъектами установленных в организации политик безопасности. Средствами ведения такого учета могут быть записи аудита. Записи аудита должны регулярно анализироваться уполномоченным лицом (лицами) с целью своевременного обнаружения нару-



шений безопасности или попыток их осуществления таких нарушений.

Общая структура системы безопасности и ее составляющие представлены на рисунке 2 [3]. Все средства безопасности разделяются на три основные группы: средства предотвращения нарушений безопасности; средства обнаружения нарушений безопасности и ликвидации последствий в случаях, когда нарушение не было предотвращено; средства общей поддержки безопасности. В целом обеспечение безопасности ИС должно носить комплексный характер и сочетать программно-технические средства безопасности инфраструктуры ИС и прикладных систем с организационными мерами безопасности.

Как правило, средства обеспечения безопасности ИС распределены по всем компонентам инфраструктуры ИС. Во многих случаях прикладное ПО также имеет встроенные средства обеспечения безопасности. Кроме того, в инфраструктуре ИС могут присутствовать отдельные компоненты, предназначенные только для решения определенных задач безопасности (например, анализаторы атак). В целом система безопасности ИС имеет достаточно сложную,

многослойную, распределенную по всем компонентам ИС структуру. Основные составляющие многоуровневой системы безопасности ИС представлены на рисунке 3 [3]. Кроме разветвления и использования в ИС собственно средств безопасности в системе должны поддерживаться также и меры гарантии безопасности. Эти меры являются основой для доверия системе безопасности ИС со стороны пользователей ИС и владельцев активов ИС.

Можно ли рассматривать множество средств обеспечения безопасности, распределенных по инфраструктуре и прикладному ПО ИС, как самостоятельную подсистему (систему) ИС – систему безопасности ИС? С точки зрения системотехники [4] система должна обладать структурой и функционалом. Структура характеризуется множеством компонент и отношений (связей) между ними. Функционал характеризует решаемую системой задачу (ее функцию). При этом функционал системы не есть сумма функций (функционалов) компонент ее структуры, а есть новая функция более высокого уровня. В качестве функционала для системы безопасности ИС могут рассматриваться цели и задачи безопасности, установленные для ИС как объекта информационных технологий. Если же говорить о структуре си-

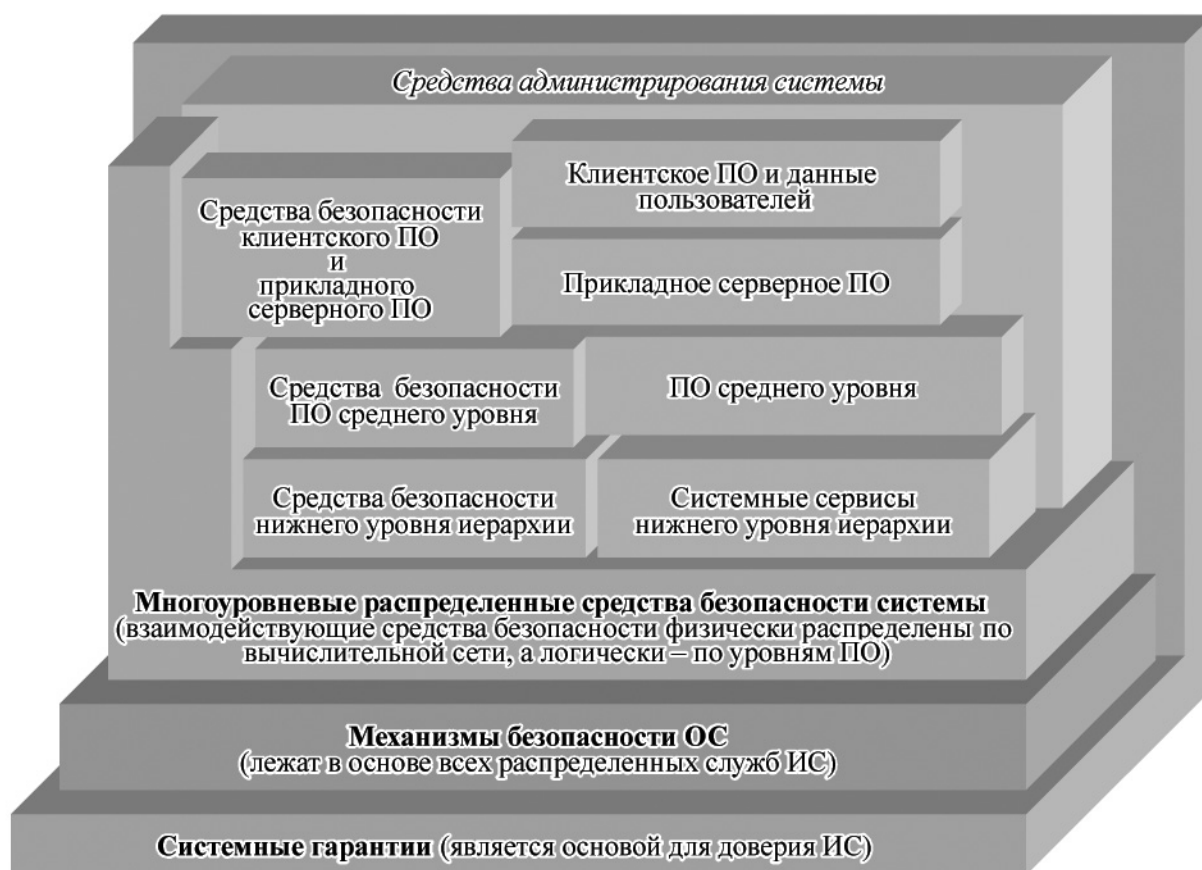


Рис. 3. Распределенная система безопасности ИС

стемы безопасности ИС, то большинство средств безопасности ИС распределены по всем компонентам инфраструктуры ИС и прикладному ПО в виде встроенных сервисов (средств) безопасности соответствующих компонентов ИС. Следует учитывать, что встроенные средства безопасности некоторого компонента инфраструктуры ИС или прикладного ПО создавались не для решения задач безопасности ИС в целом, а для решения задач безопасности именно данного конкретного компонента инфраструктуры или прикладного ПО. Таким образом, совокупность встроенных средств безопасности компонентов инфраструктуры и прикладного ПО ИС еще не образуют систему безопасности ИС – они не объединены в рамках ИС некоторой структурной организацией (т.е. не организованы как система) и не обеспечивают в общем случае решения задач безопасности для ИС. Необходимо также учитывать, что система безопасности ИС кроме чисто технических аспектов имеет и организационно-правовые аспекты обеспечения безопасности.

Независимо от того, рассматривается уже существующая ИС или разрабатывается новая,

необходимо, чтобы система безопасности ИС соответствовала критериям безопасности информационных технологий, определяемых соответствующими нормативными документами, например [1]. При строгом следовании рекомендациям общих критериев оценки безопасности информационных технологий [1] могут быть предоставлены гарантии пользователям и владельцам активов в том, что в ИС обеспечивается и поддерживается требуемый уровень защиты активов от потенциальных угроз. Однако выполнение рекомендаций Общих критериев по обеспечению безопасности ИС в целом является далеко не тривиальной задачей. Основная проблема, очевидно, будет заключаться в корректной декомпозиции ИС на подсистемы для последующей их аттестации по требованиям безопасности. Например, если разбить ИС на подсистемы по функциональному признаку, т.е. выделить в ИС прикладные функциональные подсистемы (например, делопроизводства, документооборота, бухгалтерского учета, электронную почту и т.д.) и для каждой из них в отдельности решать задачи безопаснос-

ти, то окажется, что достаточно сложно и экономически неоправданно для каждой из подсистем создавать собственную систему защиты от всех потенциальных угроз. В то же время для большинства из прикладных систем могут быть использованы общие средства и механизмы обеспечения безопасности, особенно в случае ИС ресурсного типа. В связи с этим представляется целесообразным при разработке комплексной системы безопасности ИС рассматривать в качестве самостоятельных объектов защиты следующие подсистемы ИС:

1) программно техническую инфраструктуру ИС (ПТИ), в которой должна обеспечиваться преимущественно защита ресурсов ИС от потенциальных угроз, а также реализоваться общие для функциональных систем средства и механизмы защиты;

2) функциональные подсистемы, в которых преимущественно должны реализоваться механизмы защиты от несанкционированного доступа к средствам и данным функциональных систем.

При этом ПТИ ИС может рассматриваться в качестве среды эксплуатации функциональных подсистем, в которой решается часть задач по обеспечению безопасности активов функциональных систем.

Для обеспечения гарантий безопасности ПТИ и функциональных подсистем ИС как объектов информационных технологий (ОИТ) в соответствии с рекомендациями Общих критериев безопасности информационных технологий [1] необходимо:

1. Определить цели, задачи и требований по обеспечению безопасности исходя из потенциальных угроз активам ОИТ и допустимых для организации рисков (с этой целью должен разрабатываться специальный документ – задание по обеспечению безопасности ОИТ);

2. Разработать и реализовать комплекс средств обеспечения безопасности ОИТ, обеспечивающий выполнение требований по безопасности. При этом должна быть разработана функциональная спецификация средств обеспечения безопасности, описана архитектура и принципы построения и функционирования ОИТ, разработаны необходимые руководства администратора и пользователей, другая необходимая для оценки безопасности документация, проведено тестирование средств безопасности разработчиком;

3. Провести независимую

оценку комплекса средств обеспечения безопасности ОИТ на соответствие требованиям по безопасности (выполняется экспертами независимой испытательной лабораторией с выдачей соответствующего протокола и технического отчета испытаний);

4. Поддерживать меры гарантии безопасности в процессе эксплуатации ОИТ (проводится периодический аудит безопасности ОИТ, анализируются потенциальные угрозы и связанные с ними риски безопасности, принимаются меры по поддержанию требуемого уровня безопасности, при необходимости проводится тестирование средств безопасности).

При этом, задачи безопасности как для ПТИ, так и для функциональных подсистем должны быть увязаны с задачами безопасности для ИС в целом. Основным документом, который устанавливает задачи безопасности для ИС и показывает их выполнение с помощью комплексов средств безопасности ПТИ и функциональных систем, должно быть задание по обеспечению безопасности ИС. По форме это задание должно соответствовать требованиям стандарта [1, часть 1].

В разделе *Описание объекта* должна быть описана архитектура ИС с указанием и описанием основных подсистем (ПТИ и функциональных) и решаемых ими задач.

В разделе *Среда безопасности объекта* должны быть указаны предположения об общих условиях эксплуатации ИС, определены существенные для процессов деятельности организации активы ИС, определены и идентифицированы потенциальные угрозы активам в пределах ИС и среды ее эксплуатации, установлены политики безопасности организации, являющиеся основой для определения задач безопасности ИС.

В разделе *Задачи безопасности* должны быть сформулированы общие задачи безопасности для ИС и среды эксплуатации, обеспечивающие защиту активов в пределах ИС и среды ее эксплуатации от потенциальных угроз. При этом задачи безопасности должны охватывать такие аспекты безопасности, как обеспечение доступности, целостности и конфиденциальности активов ИС.

В разделе *Требования безопасности* при формулировке функциональных требований безопасности для ИС может оказаться проблематичным использование нотаций, рекомендуемых [1, часть 2], так как они представляют собой во многих случаях достаточно сильную



конкретизацию требований безопасности для ОИТ. В связи с этим представляется возможным в данном разделе формулировать более общие требования безопасности для ИС, и не обязательно в нотации [1, часть2], тем более что данный стандарт допускает иную формулировку требований. Гарантийные требования безопасности должны быть сформулированы в соответствии с [1, часть3].

В разделе *Общая спецификация* при описании комплекса средств безопасности ИС следует представить декомпозицию средств безопасности по подсистемам ИС, выделенным при описании объекта оценки. При этом для каждой подсистемы необходимо дать только общую характеристику ее средств безопасности.

Меры гарантии безопасности ИС должны предусматривать предварительную оценку безопасности подсистем ИС.

В *Обосновании* должно быть показано, что средства безопасности подсистем ИС обеспечивают достижения установленных для ИС целей и задач безопасности.

В целом предлагаемый подход обеспечивает возможность рассмотрения средств безопасности различных подсистем ИС как единой системы безопасности ИС, а также последующую оценку как ИС в целом, так и ее отдельных подсистем на соответствие критериям безопасности ИТ.

Несмотря на то, что многие организации, владельцы ИС корпоративного уровня, пытаются решать задачи безопасности ИС, а следовательно и безопасности своей деятельности, собственными силами, все же к комплексному решению проблем безопасности ИС должны привлекаться организации, имеющие соответствующую квалификацию, опыт и ресурсы для выполнению подобных работ. СП ЗАО “Международный деловой альянс” имеет квалифицированных специалистов с опытом проведения работ в области построения систем безопасности различных ИС, что позволяет предоставлять следующие услуги заказчикам по обеспечению безопасности их ИС:

- разработка задания по обеспечению безопасности ИС Заказчика и подсистем ИС;
- определение структуры системы безопасности ИС или ее отдельных подсистем, отвечающей установленным требованиям;
- поставка и инсталляция необходимых средства безопасности для ИС и ее отдельных подсистем, в том числе средств обеспечения отказоустойчивости компонентов ИС и восстановления вычислительных процессов;
- проведение тестирования средств безопасности ИС и анализ уязвимостей ИС;
- оказание помощи в подготовке документации, необходимой для аттестации ИС по безопасности;
- проведение независимой оценки ИС и ее подсистем на соответствие критериям безопасности ИТ.

Для предоставления услуг по оценке безопасности ИС в СП ЗАО “Международный деловой альянс” создана испытательная лаборатория информационных систем, которая аттестована на независимость и техническую компетентность в системе аккредитации Республики Беларусь. Областью аккредитации лаборатории является оценка информационных систем и программных продуктов на соответствие критериям безопасности ИТ, устанавливаемых стандартами [1].

Литература

1. СТБ 34.101.(1-2)-2001 (ИСО/МЭК 15408-(1-3)-99) Информационная технология. Методы и средства безопасности. Критерии оценки безопасности информационных технологий. Части 1,2 и3.
2. ISO/IEC 17799 Information technology – Code of practice for information security management.
3. EP-ITS (Engineering Principles for IT Security). NIST, draft 10/23/00.
4. Николаев В.И., Брук В.М. Системотехника: методы и приложения. – Л.:Машиностроение, 1985 – 199 с.