УДК 681.3

СИСТЕМНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ РАСПРЕДЕЛЕННОГО ТИПА

© 2003 А.Ю. Родичев, Ю.А. Родичев[1]

Развитие компьютерных сетей и информационных технологий обусловило актуальность задач обеспечения информационной безопасности и защиты информационных систем от несанкционированного доступа. В работе построена модель защиты информации для информационных систем распределенного типа. Модель позволяет построить эффективную систему защиты информации, применить адекватные средства и методы обеспечения безопасности на всех уровнях информационных процессов.

Наблюдающийся в последние годы процесс бурного развития глобального информационного обмена поставил ряд серьезных правовых вопросов. Мировое сообщество, и в частности Россия, явно отстает от процесса разработки соответствующих правовых норм, регулирующих отношения в сфере информационных технологий [1, 2, 3]. В связи с этим одной из задач по построению информационного общества является создание нормативно-правовой базы в области информационных технологий, в том числе информационной безопасности и защите авторских прав на электронные средства информации.

Процесс формирования глобального информационного общества привел не только к качественному изменению способов хранения и обработки информации, но и сделал ее одним из ценнейших товаров. В настоящее время информация представляет собой стратегический ресурс, лежащий в основе национального богатства стран с развитыми информационными технологиями. Именно "интеллектуалоемкость" информационных технологий позволяет государствам, не обладающим достаточными природными ресурсами, поставлять на мировой рынок информационные услуги, продукты, технологии. С другой стороны, развитие компьютерных сетей и информационных технологий вызвало резкое увеличение нарушений авторских прав владельцев информации. В связи с этим проблема обеспечения информационной

[1]Родичев Александр Юрьевич (roal@ssu.samara.ru), Родичев Юрий Андреевич (rodichev@ssu.samara.ru), информационно-вычислительный центр Самарского государственного университета, 443011, г. Самара, ул. Акад. Павлова, 1.

безопасности и защита информационных систем от несанкционированного доступа приобрела в настоящее время особую актуальность.

В соответствии со статьей 20 Федерального закона "Об информации, информатизации и защите информации" целями защиты в области информационных процессов являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращения несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Понятие информационной безопасности в российской юридической терминологии не является до сих пор устоявшимся по причине отсутствия единого методологического основания, на базе которого могут быть определены его сущность, степень необходимости использования и границы применения [4]. С методологической точки зрения при анализе проблем информационной безопасности необходимо выявить субъекты информационных отношений и их интересы, связанные с использованием информационных систем, определить задачи по защите информации, основные угрозы безопасности и возможные средства защиты от них. Таким образом, необходима многомерная модель информационной безопасности.

Проблемы информационной безопасности существенно зависят от типа информационных систем и сферы их применения. В локальных системах малого масштаба систему защиты построить гораздо проще, чем в системах распределенного типа [5]. Это объясняется особенностями информационных систем распределенного типа, основными из которых являются: территориальная разнесенность компонентов системы и как следствие наличие обмена информацией между ними; широкий спектр способов представления, хранения и передачи информации; одновременное участие в процессах обработки информации большого количества пользователей с разными правами доступа; использование разнородных программно-технических средств обработки и систем телекоммуникаций.

Структурная модель информационной безопасности систем распределенного типа представима в виде схемы, представленной на рис. 1. Решение проблемы безопасности в информационных системах распределенного типа заключается в анализе следующих основных компонент: определении основных задач защиты информации, выявлении субъектов информацион-

ных процессов, классификации основных возможных угроз безопасности, определении уровней уязвимости информационных систем.

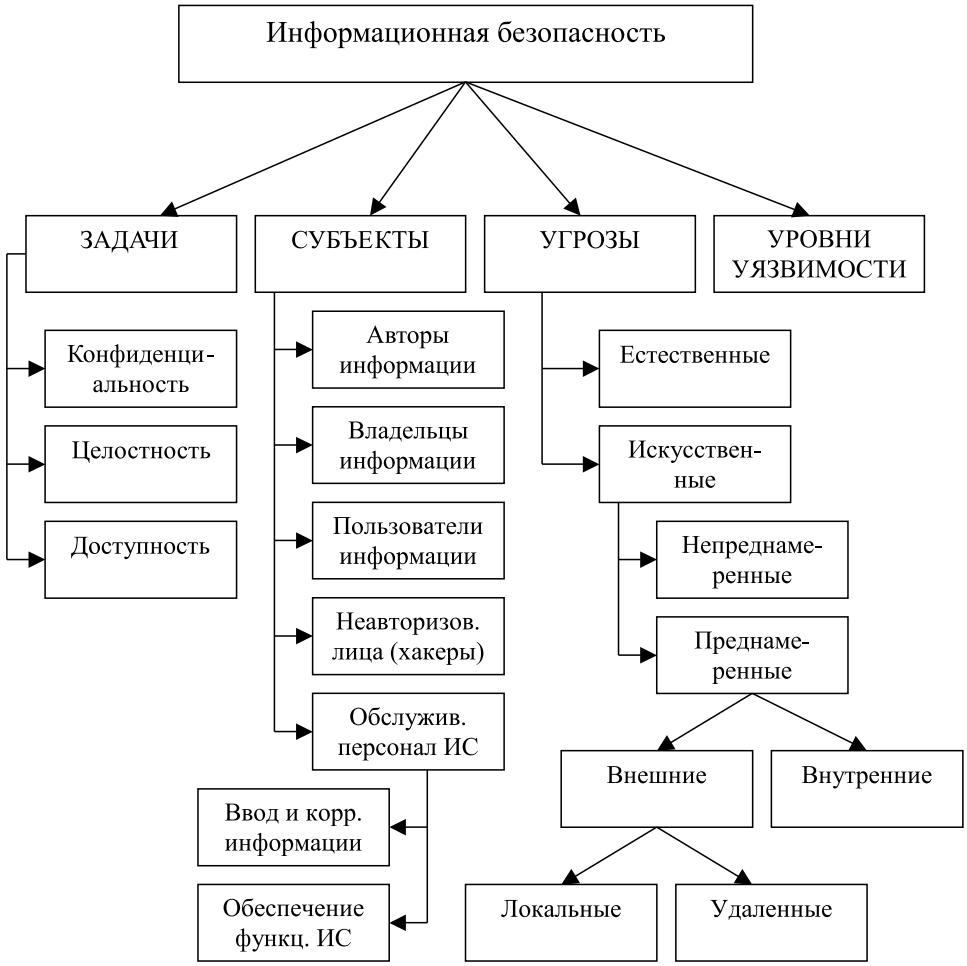

Рис. 1. Модель информационной безопасности

Обеспечение безопасности информации состоит в решении трех взаимосвязанных задач: конфиденциальность, целостность и доступность. Задача по обеспечению конфиденциальности состоит в защите информации в процессе ее создания, хранения, обработки и обмена от ознакомления с ней лицами, не имеющими права доступа к ней. Каждый пользователь системы должен иметь доступ только к той части информации, на которую он имеет разрешение. Для обеспечения конфиденциальности могут быть эффективно применимы методы криптографии.

Задача по обеспечению целостности состоит в защите от преднамеренного или непреднамеренного изменения информации и алгоритмов ее обработки лицами, не имеющими на то права. Наиболее эффективными средствами обеспечения целостности информации являются аутентификация (проверка подлинности по содержанию, источнику, времени создания и т.п.) и иден-

тификации (проверки подлинности сторон в процессе информационного обмена).

Обеспечение доступности состоит в предоставлении пользователям всей имеющейся в системе информации в соответствии с установленными им правами.

Основными субъектами в информационных процессах являются: авторы и владельцы информации, авторизованные пользователи информации, неавторизованные лица (лица, пытающиеся получить самовольный доступ к информации — "хакеры"), отдельные сотрудники или коллективы, участвующие в разработке, обеспечении работоспособности программно-технических средств информационных систем и наполнении системы информацией. Системы защиты должны обеспечивать защиту прав авторов и владельцев информации и одновременно предоставлять доступ к информации пользователям в соответствии с их правами. Кроме того, возможны каналы утечки информации, заложенные разработчиками информационной системы и известными только им. Персонал, занимающийся сопровождением программно-технических средств и информационным наполнением, также представляет определенную угрозу несанкционированных утечек. В этом случае система защиты должна располагать соответствующими законодательными и нормативно-правовыми актами на уровне государства и организационными мероприятиями на уровне учреждения.

Под угрозой безопасности информационным системам понимается потенциально возможное действие, событие или процесс, которое посредством воздействия на информацию и другие компоненты системы может нанести ущерб интересам субъектов. Угрозы безопасности на первом уровне классификации могут быть разделены на естественные и искусственные. Естественными угрозами безопасности являются, например, стихийные бедствия, аварии, внезапные отключения электропитания, поломки технических средств и другие, не зависящие от человека. Искусственные угрозы вызваны действиями человека и подразделяются на непреднамеренные и преднамеренные. Основными непреднамеренными угрозами являются следующие: неквалифицированные действия обслуживающего персонала, повлекшие к разрушению аппаратно-программных средств и информационных ресурсов; неумышленная порча носителей информации; ошибки, допущенные в процессе проектирования системы; заражение рабочих станций вирусами; игнорирование персоналом организационно-технологических ограничений, повлекшее разглашение конфиденциальной информации и паролей; ввод ошибочной информации и другие.

Уровни защиты (уязвимости) информационных систем классифицируются в соответствии со схемой, представленной на рис. 2.

Физический уровень определяет на сколько эффективно защищены элементы, образующие техническую часть информационной системы: сервера, рабочие станции, активное сетевое оборудование и линии связи. Технологический уровень отражает, насколько эффективно обеспечена защита ап-

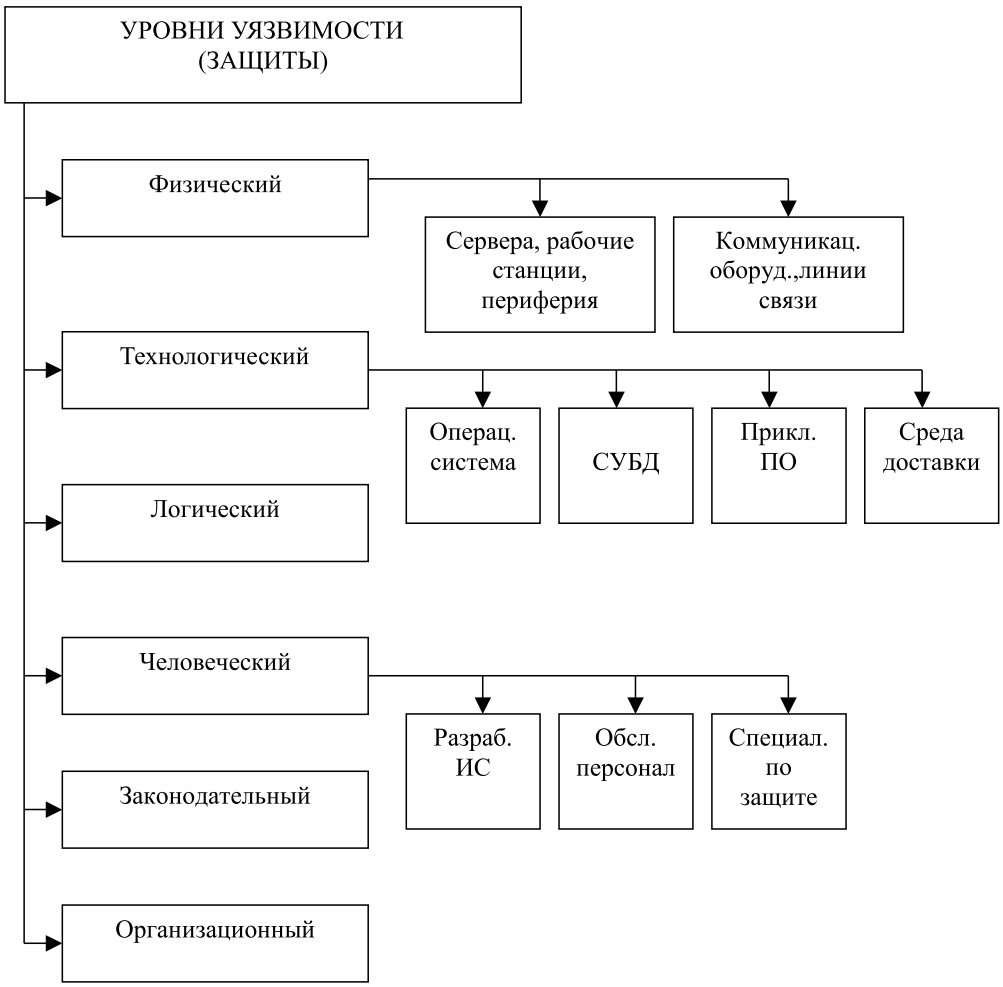

Рис. 2. Уровни защиты

паратно-программных процедур, обеспечивающих требуемую степень безопасности. Это касается выбора операционных систем, систем управления базами данных (СУБД), прикладного программного обеспечения, среды доставки информации.

Логический уровень характеризует адекватность логических основ механизма безопасности и организации хранения и кодирования информации. Человеческий уровень отражает степень квалификации и ответственности персонала на стадиях проектирования системы и ее эксплуатации (техническое и программное сопровождение, информационное наполнение, контроль за соблюдением требований безопасности).

Законодательный уровень определяет комплекс законодательных и нормативно-правовых актов, регулирующих отношения субъектов в процессах информационного обмена. Организационный уровень предусматривает комплекс организационных мероприятий, регламентирующий процессы эксплуатации системы.

Построенная модель защиты информации для информационных систем распределенного типа, позволяет определить основные задачи по обеспечению безопасности, выявить субъекты в информационных процессах, определить типы угроз и уровней уязвимости. В конечном счете она позволяет построить эффективную систему защиты информации, применить адекватные средства и методы безопасности на всех уровнях информационных процессов.

Литература

[1] Минков А.М. Международная охрана интеллектуальной собственности. СПб: Питер, 2001. 720 с.

[2] Правовые аспекты использования Интернет-технологий // Под ред. А.С. Кемрадж, Д.В. Головерова. М.: Книжный мир, 2002. 410 с.

[3] Шамраев А.В. Правовое регулирование информационных технологий (анализ проблем и основные документы). Версия 1.0. М.: Статут, Интертех, БДЦ-пресс, 2003. 1013 с.

[4] Городов О.А. Основы информационного права России: Учебное пособие. СПб.: Юридический центр Пресс, 2003. 305 с.

[5] Морозов А.В., Родичев Ю.А. Сохранность ресурсов автоматизированных информационных финансово-экономических и бухгалтерских систем // Междунар. науч.-техн. конф. "Измерение, контроль, информатизация" ИКИ-2000. Тезисы доклада. Барнаул, 2000. С. 148–151.

Поступила в редакцию 23/*XII*/2003;
в окончательном варианте — 23/*XII*/2003.

A SYSTEM MODEL OF INFORMATION SECURITY OF DISTRIBUTED INFORMATION SYSTEMS

© 2003 A.Y. Rodichev, Y.A. Rodichev[2]

The computer networks development and progress in information technologies cause the increasing importance of providing information systems protection. In the paper the information security model of a distributed type is proposed. The model affords the effective security system and gives appropriate tools and methods of providing information security.

Paper received 23/*XII*/2003;
Paper accepted 23/*XII*/2003.

[2]Rodichev Alexander Yurievich (roal@ssu.samara.ru), Rodichev Yuri Andreyevich (rodichev@ssu.samara.ru), Center of Computational Science and Technology, Samara State University, Samara, 443011, Russia.