С. А. Охрименко, Г. А. Черней

# Угрозы безопасности автоматизированным информационным системам (программные злоупотребления)

*Излагаются основы новой классификации угроз безопасности автоматизированным информационным системам с выделением самостоятельного класса — программных злоупотреблений. Рассматриваются их характеристики, тактические и стратегические цели.*

Событие, которое может вызвать нарушение функционирования автоматизированной информационной системы (АИС), включая, искажение, уничтожение или несанкционированное использование обрабатываемой в ней информации, называется *угрозой.* Возможность реализации угроз зависит от наличия в АИС уязвимых мест, количество и специфика которых определяется видом решаемых задач, характером обрабатываемой информации, аппаратно-программными особенностями системы, наличием средств защиты и их характеристиками.

Основываясь на анализе результатов научных исследований [1, 2, 3, 4] и практических разработок [5, 6, 7, 8, 9, 10, II, 12, 13, 14 и др.], следует выделить два типа угроз:

*непреднамеренные или случайные действия,* выражающиеся в неадекватной поддержке механизмов защиты и ошибками в управлении;

*преднамеренные угрозы* — несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами и самими системами.

Выделение двух типов угроз является недостаточным и требует детализации.

Множество непреднамеренных угроз, связанных с внешними (по отношению к АИС) факторами, обусловлено влиянием воздействий, неподдающихся предсказанию. К ним относят угрозы, связанные со стихийными бедствиями, техногенными, политическими, экономическими, социальными факторами, развитием информационных и коммуникационных технологий, другими внешними воздействиями.

К внутренним непреднамеренным относят угрозы, связанные с отказами вычислительной и коммуникационной техники, ошибками программного обеспечения, персонала, другими внутренними непреднамеренными воздействиями, которые

могут быть источниками угроз нормальной работе ЛИС.

К распространенным преднамеренным информационным нарушениям относят [15, 16, 17 и др.]:

- несанкционированный доступ к информации, хранящейся в памяти компьютера и системы, с целью несанкционированного использования;
- разработку специального программного обеспечения, используемого для осуществления несанкционированных доступа или других действий;
- отрицание действий, связанных с манипулированием информацией и другие несанкционированные действия;
- ввод в программные продукты и проекты "логических бомб", которые срабатывают при выполнении определенных условий или по истечении определенного периода времени, частично или полностью выводят из строя компьютерную систему;
- разработку и распространение компьютерных вирусов;

• небрежность в разработке, поддержке и эксплуатации программного обеспечения, приводящие к краху компьютерной системы',

• изменение компьютерной информации и подделку электронных подписей;

• хищение информации с последующей маскировкой (например, использование идентификатора, не принадлежащего пользователю, для получения доступа к ресурсам системы);

• манипуляцию данными (например, несанкционированная модификация, приводящая к нарушению целостности данных);

• перехват (например, нарушение конфиденциальности данных II сообщений);

• отрицание действий или услуги (отрицание существования утерянной информации);

• отказ в предоставлении услуги (комплекс нарушений, вызванных системными ошибками, несовместимостью компонент и ошибками в управлении).

Заслуживает внимания подход автора [18], который разделяет преднамеренные угрозы безопасности на:

• **физические,** к которым относят хищения, разбойные нападения, уничтожение собственности, террористические акции, другие чрезвычайные обстоятельства;

• технические, к которым относят перехват информации, радиоразведку связи и управления, искажение, уничтожение и ввод ложной информации;

• интеллектуальные — уклонение от обязательств, мошеннические операции, агентурная разведка, скрытое наблюдение, психологическое воздействие.

Для получения доступа к ресурсам АИС злоумышленнику необходимо реализовать следующие действия:

• отключение или видоизменение защитных механизмов;

• использование недоработок системы защиты для входа в систему;

• вход в систему под именем и с полномочиями реального пользователя.

В первом случае злоумышленник должен видоизменить защитные механизмы (например, отключить программу запроса паролей пользователей), во втором — исследовать систему безопасности информации на предмет наличия недокументированных возможностей или недоработанных 'механизмов защиты и в третьем — выяснить или с помощью набора действий подделать идентификатор реального пользователя (например, подсмотреть пароль, вводимый с клавиатуры). • -

Анализируя источники угроз, следует отметить классификацию нарушителей, приведенную в [19]:

первая группа — так называемые хакеры;

вторая группа — преступники, преследующие цели обогащения путем непосредственного внедрения в финансовые системы или получения коммерческой и другой информации для организации действий уголовного характера;

третья группа — террористы и другие экстремистские группы, использующие внедрение в, информационные системы для совершения устрашающих действий, шантажа. Следует особо отметить, что с развитием компьютерных, сетей Internet создается дополнительное киберпространство, где могут производиться различные несанкционированные действия, которые могут остаться нераскрытыми;

четвертая группа — различные коммерческие: организации и структуры, стремящиеся

вести промышленный шпионаж и борьбу с конкурентами путем добычи или искажения конфиденциальной, финансовой, технологической, проектной, рекламной и другой информации.

Таким образом можно отметить, что рыночные отношения стимулируют совершенствование методов скрытого проникновения в информационные системы конкурирующих фирм.

Рассматривая комплекс угроз, которые получили распространение на сегодняшний день 'и исследованы в различных публикациях, следует отметить, что в отечественной и зарубежной литературе, посвященной проблеме безопасности АИС, преднамеренные воздействия рассматриваются с различных точек зрения и используются различные категории.

С. Мафтик при рассмотрении механизмов защиты в сетях ЭВМ выделяет только программы 'типа "троянский конь" [20]. В свою очередь, С.Недков, использует термин "программы проникновения в вычислительные системы" [21].

С появлением компьютерных вирусов получила распространение новая классификация компьютерных злоупотреблений. Н. Н. Безруков в [22,23 и др.] рассматривает предшественников компьютерных вирусов — программы вандалы и троянские кони, с выделением в составе последних логических мин (logic bomb), мин с часовым механизмом (time bomb) и программных люков (trap doors).

:С. И. Расторгуев использует термин "средства скрытого информационного воздействия (ССИВ)", понимая под ними вирусы и программные закладки [24]. В [2] предложен термин "разрушающие программные средства" (РПС), под которыми понимаются программно-реализуемые средства нарушения целостности обработки и хранения информации в компьютерных системах. При этом выделяются три класса: компьютерные вирусы; средства несанкционированного доступа; программные закладки.

Авторы [7], описывая комплекс защиты для АИС *с* использованием баз данных, в качестве средств несанкционированного доступа выделяют специально разработанное программное обеспечение — *программы- шпионы.* В данной работе **ис**пользуется термин "программные злоупотребление", который наиболее полно с содержательной и функциональной точки зрения отражает природу подобного вида угроз [5].

Интересным является подход к классификации угроз безопасности АИС, представленный в [25]. . Автор классифицирует угрозы следующим образом:

а) по признаку области поражения: угрозы для информационной среды, ее подсистем и элементов; угрозы для предметных областей информационного обеспечения — субъектов и объектов пользования; угрозы для всей социальной системы, исходящие от информационной среды;

6) по признаку их связи с информационной средой определенной социальной системы: внешние; внутренние — идущие от социальной системы и ее элементов; внутрисистемные — исходящие от самой информационной среды;

в) по силе воздействия на область поражения выделяются: разрушительные; дестабилизирующие; парализующие и стимулирующие угрозы;

г) по организационной форме выражения и степени социальной опасности: коллизии, конфликты, проступки, преступления, аварии и катастрофы.

Рассмотренная система классификации угроз реализована с точки зрения информационной безопасности общества и информационных процессов, происходящих в нем. Следует отметить ее функциональную наполненность и емкость.

Наиболее полная классификация угроз безопасности АИС представлена в [17].

Авторы монографии предлагают классификацию угроз по:

цели реализации угрозы: нарушение конфиденциальности, нарушение целостности, нарушение доступности;

принципу воздействия: с использованием доступа, с использованием скрытых каналов;

характеру воздействия: активные, пассивные;

причине появления используемой ошибки защиты: неадекватность политики безопасности, ошибкой управления системой защиты, ошибки проектирования системы защиты) ошибки кодирования;

способу воздействия на объект атаки: непосредственное воздействие на объект атаки, воздействие на систему разрешений, опосредованное воздействие;

способу воздействия: в интерактивном и пакетном режимах;

объекту атаки: на АИС в целом, на объекты АИС, на субъекты АИС, на каналы передачи данных;

используемым средствам атаки: с использованием штатного программного обеспечения, с использованием разработанного программного обеспечения;

состоянию объекта атаки: при хранении объекта, при передаче объекта, при обработке объекта.

Таким образом, в настоящее время отсутствует единый подход к классификации программных злоупотреблений (ПЗ), поскольку они лишь недавно стали объектом пристального внимания и исследования. Кроме того, многообразие форм проявлений, различия во внутренней организации, жизненный цикл и среда обитания — все это существенно усложняет создание единого классификатора.

Представляется необходимым дополнить рассмотренные подходы к классификации угроз безопасности АИС, концентрируя внимание на преднамеренных угрозах — программных злоупотреблениях. Считаем возможным предложить новую классификацию, приведенную на рис. 1 и призванную дополнить и расширить предложенные в [17, 25] основы классификации.

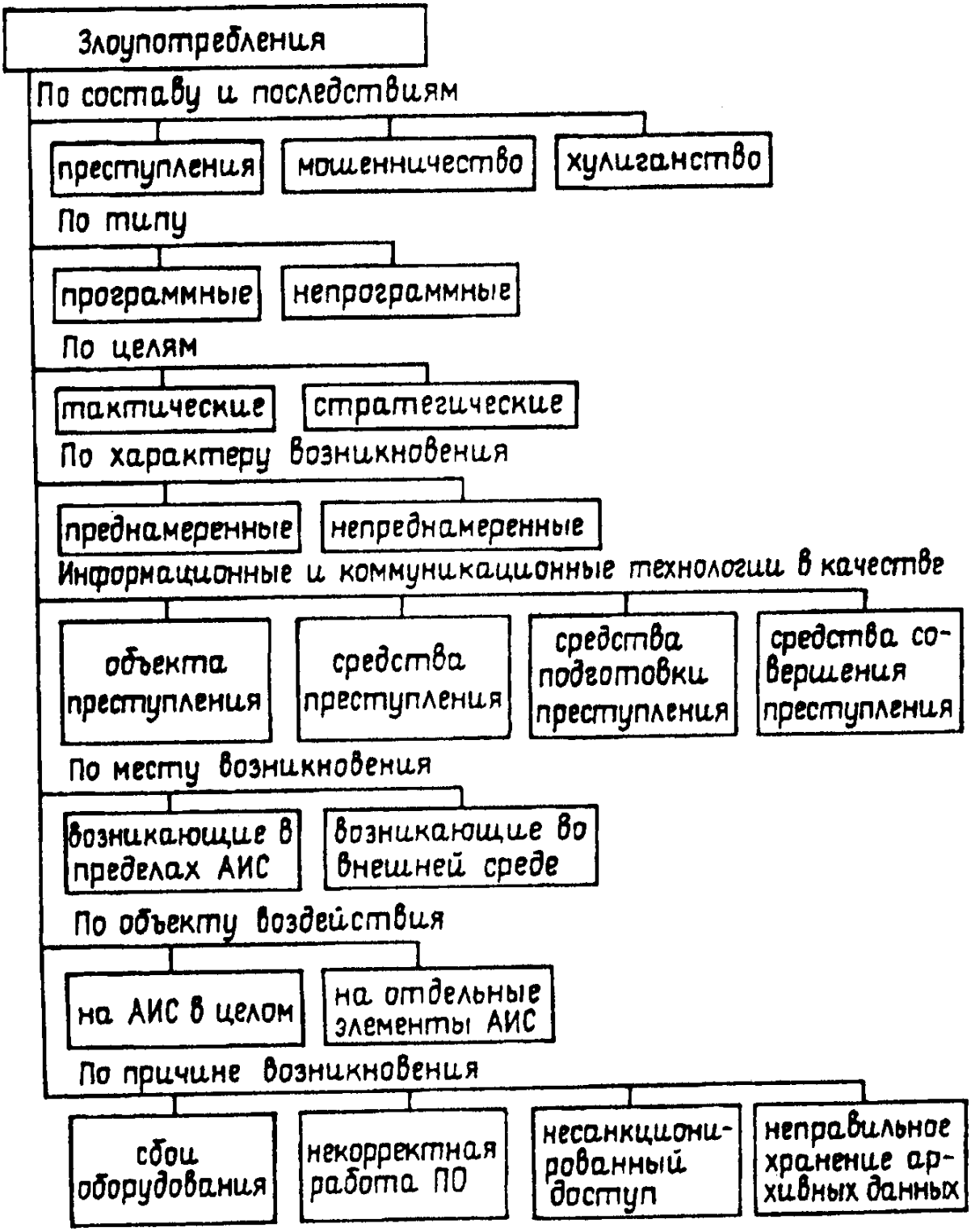


Рис. 1. Классификация угроз информационной безопасности АИС

*По составу и последствиям* следует выделять *преступления, мошенничество* и *хулиганство.*

Под компьютерным преступлением (КП) следует понимать комплекс противоправных действий, направленных на несанкционированный доступ, получение и распространение информации, выполненный с использованием средств вычислительной техники, коммуникаций и программного обеспечения.

Группа экспертов из Организации экономического сотрудничества и развития в 1983 г. определила, что под термином "компьютерная преступность" (или "связанная с компьютерами преступность") трактуются любые незаконные, неэтичные или неправомерные действия, связанные с автоматической обработкой данных и/или их передачей [26]. В той же работе определены основные виды компьютерной преступности:

1) связанные с компьютерами экономические преступления, среди которых можно различать шесть основных видов:

махинации путем компьютерного манипулирования АИС с целью получения финансовой выгоды;

компьютерный шпионаж и кража программного обеспечения; компьютерные диверсии;

кража услуг (времени), неправомерное использование АИС;

неправомерный доступ к АИС и их "взламывание";

традиционные преступления в сфере бизнеса (экономики), совершаемые с помощью АИС.

2) нарушение личных прав. К такого вида нарушениям можно отнести следующие действия:

составление и использование некорректных данных;

незаконное раскрытие данных или их использование не по назначению (данное действие частично входит в сферу традиционных преступлений, связанных с производственными секретами); незаконный сбор и хранение данных; нарушение формальных обязанностей и информационного права в соответствии с законами о частной тайне.

3) компьютерные преступления против "индивидуальных" интересов, таких, как преступления против национальной безопасности, трансграничного потока данных, неприкосновенности компьютерных процедур и сетей передачи данных и другие.

В последнее время получила широкое распространение разновидность компьютерных преступлений — компьютерное мошенничество и хулиганство.

Компьютерное мошенничество — вид компьютерных нарушений, целью которого является незаконное обогащение нарушителя.

Компьютерное хулиганство на первый взгляд, является безобидной демонстрацией интеллектуальных способностей. По последствия подобных действий могут быть весьма серьезными, поскольку выражаются в потере доверия пользователей к вычислительной системе, а также краже данных, характеризующих личную или коммерческую информацию.

Следует отметить, что представленная классификация является условной и дальнейшее уточнение должно проводиться в рамках существующих правовых актов.

*По типу реализации* можно различать *программные* и *непрограммные* злоупотребления. К программным относят злоупотребления, которые реализованы в виде отдельного программного модуля или модуля в составе программного обеспечения. К непрограммным относят злоупотребления, в основе которых лежит использование технических средств АИС для подготовки и реализации компьютерных преступлений (например, несанкционированное подключение к коммуникационным сетям, съем информации с помощью специальной аппаратуры и др.).

Компьютерные злоумышленники преследуют различные цели и для их реализации

используют широкий набор программных средств. Исходя из этого, представляется возможным объединение программных злоупотреблений в две группы: *тактические* и *стратегические.* К тактическим относят злоупотребления, которые преследуют достижение ближайшей цели (например, получение пароля, уничтожение данных и др.). К группе стратегических относятся злоупотребления, реализация которых обеспечивает возможность получения контроля за технологическими операциями преобразования информации, влияние на функционирование компонентов АИС (например, мониторинг системы, вывод из строя аппаратной и программной среды и др.).

*По характеру возникновения* различают *непреднамеренные* и *преднамеренные.* Непреднамеренные угрозы связаны со стихийными бедствиями и другими неподдающимися предсказанию факторами, сбоями и ошибками вычислительной техники и программного обеспечения, а также ошибками персонала. Преднамеренные угрозы обусловлены действиями людей и ориентированы на несанкционированное нарушение конфиденциальности, целостности и/ или доступности информации, а также использование ресурсов в своих целях.

При реализации угроз информационные и коммуникационные технологии могут выступать в качестве объекта преступления, средства преступления, средства подготовки преступления или среды совершения преступления [15].

*По месту возникновения* угроз безопасности АИС можно различать угрозы, возникающие в пределах АИС и угрозы, возникающие во внешней среде.

*По объекту воздействия* следует выделять угрозы, воздействующие на АИС в целом, и угрозы, воздействующие на отдельные ее элементы.

*По причине возникновения* различают сбой оборудования, некорректную работу операционных Систем и программного обеспечения, несанкционированный доступ и неправильное хранение архивных данных, вследствие чего они могут быть утеряны (уничтожены).

Анализируя совокупность несанкционированных манипуляций с информацией и ресурсами АИС, можно различать следующие основные группы:

*утрата информации* — неосторожные действия владельца информации, представленной в АИС на различных носителях и в файлах, или лица, которому была доверена информация в силу его официальных обязанностей в рамках АИС, в результате чего информация была потеряна и стала достоянием посторонних лиц;

*раскрытие информации* — умышленные или неосторожные действия, в результате которых содержание информации, представленной на различных носителях и в файлах, стало известным или 'доступным для посторонних лиц;

*порча информации* — умышленные или Неосторожные действия, приводящие к полному или частичному уничтожению информации, представленной ни различных носителях и в файлах;

*кража информации* — умышленные действия, направленные на несанкционированное изъятие информации из системы ее обработки как посредством кражи носителей информации, так и посредством дублирования информации, представленной в виде файлов АИС;

*подделка информации* — умышленные или неосторожные действия, в результате которых нарушается целостность информации, находящейся на различных носителях и в файлах АИС;

*блокирование информации* — умышленные или неосторожные действия, приводящие к недоступности информации в системе ее обработки;

*покушение работы системы обработки информации* — умышленные или неосторожные действие, приводящие к частичному или полному отказу системы обработки или создающие благоприятный условия для выполнения вышеперечисленных действий.

Рассмотрим существующие к настоящему времени программные средства, используемые для получения несанкционированного доступа и нанесения ущерба АИС.

Потенциальными программными злоупотреблениями можно считать программные средства, которые обладают следующими функциональными возможностями [6,27]:

сокрытие признаков своего присутствия в программной среде ЭВМ;

обладание способностью к самодублированию, ассоциированию себя с другими программами и/или переносу своих фрагментов в иные области оперативной или внешней памяти;

разрушение (искажение произвольным образом) кодов программ в оперативной памяти;

сохранение фрагментов информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

искажение произвольным образом, блокирование и/или подмена выводимого во внешнюю память или в канал связи массива информации, образовавшегося в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

В соответствии с предложенной классификацией программные злоупотребления могут быть разделены по своему назначению на два больших класса: тактические и стратегические (рис. 2) [28]. Тактические программные злоупотребления предназначаются для достижения ближайших целей: получения паролей, несанкционированного доступа, разрушения информации и других действий. Тактические программные злоупотребления обычно используются для подготовки и реализации стратегических злоупотреблений. Стратегические программные злоупотребления направлены на реализацию далеко идущих целей и связаны с большими финансовыми потерями для АИС и объекта управления.

Среди самых распространенных программных злоупотреблений следует выделить: программы поручения паролей, "люки", логические бомбы, троянские кони, репликаторы, компьютерные вирусы, программные закладки и др.

1. *Программы получения паролей* — это две большие группы программ, которые предназначены для получения идентификаторов и паролей пользователей. В [17] с данным злоупотреблением связывается термин "взлом системы".

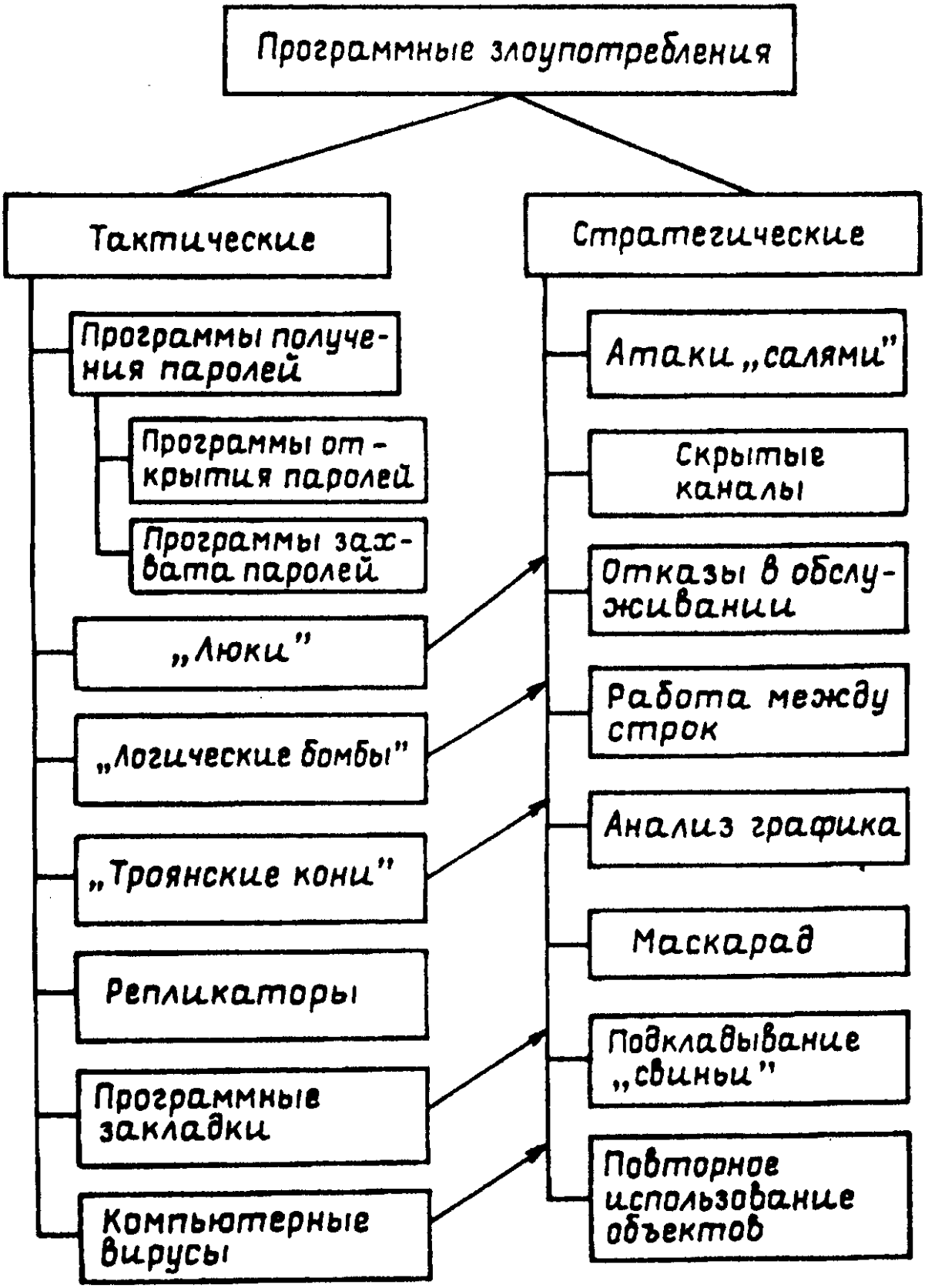


Рис. 2. Классификация программных злоупотреблений

Программы открытия паролей последовательно генерируют все возможные варианты пароля и выдают их системе до тех пор, пока не будет определен необходимый пароль [29]. Пароли являются основным средством идентификации пользователей в

многопользовательских компьютерных системах и открытие пароля и входного **имени** пользователя позволяет организовать доступ к конкретной информации.

Программы захвата паролей имитируют системный сбой в работе компьютера (например, перезагрузку операционной системы, отключение сети и др.), и запрашивают у пользователя идентификатор и пароль, после чего передают управление рабочей программе, операционной системе или другим программам [17, 30 и др.].

2. *"Люки"* или "trap door" — не описанные в документации возможности работы с программным продуктом [17, 29 и др.]. В [29] автор приравнивает программы открытия паролей к так называемым "люкам", которые на сегодняшний день формируются в самостоятельную группу злоупотреблений.

Сущность использования люков состоит в том, что при реализации пользователем не описанных в документации действий, он получает доступ к ресурсам и данным, которые в обычных условиях для него закрыты (в частности, вход в привилегированный режим обслуживания).

Люки могут появиться в программном продукте следующими путями:

**а) люки** чаще всего являются результатом забывчивости разработчиков. В процессе разработки программы создаются временные механизмы, облегчающие ведение отладки за счет прямого доступа к продукту.

Одним из примеров использования забытых люков является инцидент с вирусом Морриса [31]. Одной из причин обусловившей распространение этого вируса, являлась ошибка разработчика программы электронной почты, входящей в состав одной из версий ОС UNIX, приведшая к появлению малозаметного люка.

6) люки могут образоваться также в результате часто практикуемой технологии разработки программных продуктов "сверху—вниз". При этом программист приступает к написанию управляющей программы, заменяя предполагаемые в будущем подпрограммы так называемыми "заглушками" — группами команд, имитирующими или обозначающими место присоединения будущих подпрограмм. В процессе работы эти заглушки заменяются реальными подпрограммами.

На момент замены последней заглушки реальной подпрограммой, программа считается законченной. Но на практике подобная замена выполняется не всегда. Во-первых, из-за нарушения сроков разработки и сдачи в эксплуатацию и, во-вторых, из-за невостребованности данной подпрограммы. Таким образом, заглушка остается, представляя собой слабое место системы с точки зрения информационной безопасности.

в) программист пишет программу, которой можно управлять с помощью определенных команд, или, например, путем ввода "Y" ("Да") или "N" ("Нет"). А что произойдет, если в ответ на запрос будет вводиться "A" или "B" и т. д.? Если программа написана правильно, то на экране должно появиться сообщение типа "Неправильный ввод" и повтор запроса. Однако может быть ситуация, когда программа не учитывает такое, предполагая, что пользователь будет действовать правильно. В таком случае реакция программы на неопределенный ввод может быть непредсказуемой. Такую ситуацию в программе можно специально создать для того, чтобы получить доступ к определенным ресурсам и данным.

Таким образом, люк может присутствовать в программном продукте вследствие умышленных или неумышленных действий со стороны программиста для обеспечения:

тестирования и отладки программного продукта;

окончательной сборки конечной программы; скрытого средства доступа к программному продукту и данным.

В первом случае люк — это неумышленная, но серьезная брешь в безопасности

системы. Во втором — серьезная экспозиция безопасности системы. В третьем случае — первый шаг к атаке системы.

Такие виды нарушений называются trap doors или back doors (в литературе за данными программными злоупотреблениями закрепилось название "задние ворота"). Пример встроенного люка в операционную систему MS-DOS приводится в [32].

3. *Логические бомбы* (logic bomb) — программный код, который является безвредным до выполнения определенного условия, после которого реализуется логический механизм [29]. Логические бомбы, в которых срабатывание скрытого модуля определяется временем (текущий датой), называют бомбами с часовым механизмом (time bomb). Подобные программы, реализующие свой механизм после конкретного числа исполнении, при наличии или, наоборот, отсутствии определенного файла, а также соответствующей записи в файле, получили название логической бомбы (logic bomb).

В связи с тем, что подобные программы имеют ограниченный доступ к ресурсам системы, разрушительный эффект остается достаточно низким. Опасность может значительно увеличиться, если логическая бомба будет встроена в системное программное обеспечение, что приведет к уничтожению файлов, переформатированию машинных носителей или к другим разрушающим последствиям. Основной целью функционирования программ типа логической бомбы следует считать нарушение нормальной работы компьютерной системы.

4. *"Троянский конь"* — программа, которая кроме своей основной деятельности выполняет некоторые дополнительные (разрушительные), Не описанные в документации функции, о чем пользователь не подозревает [17, 29 и др.].

Реализация дополнительных функций выполняется скрытым от пользователя модулем, который может встраиваться в системное и прикладное программное обеспечение. При реализации пораженной программы троянский конь получает доступ' к ресурсам вместе с пользователем.

Троянские кони значительно опаснее ПЗ, рассмотренных ранее, поскольку чаще всего они встраиваются в хорошо зарекомендовавшие себя программные продукты — инструментальные средства, пакеты прикладных программ, текстовые редакторы, компьютерные игры и т. д., и выступают в качестве средства несанкционированного доступа к содержащейся в системе информации. В некоторых случаях термином "троянские программы" ошибочно называли программы, содержащие ошибки или плохо спроектированный интерфейс с пользователем.

Компьютерные системы, использующий дескрипторные методы управления доступом (и том числе такие, как полномочия, списки управления доступом и др.), становятся практически беззащитными против программ типа троянский конь.

5. *Репликаторы*— могут создавать одну, или более своих копий в компьютерной системе. Это приводит к быстрому переполнению памяти компьютера, но данные действия могут быть обнаружены опытным пользователем и достаточно легко устранены. Устранение программы репликатора усложняется в тех случаях, когда репликация выполняется с модификацией исходного текста: программы, что затрудняет распознавание ее новых копий. Репликаторные программы становятся особенно опасными, когда к функции размножения будут добавлены другие разрушающие воздействие.

6. *Программные закладки* — программы, которые сохраняют вводимую с клавиатуры информацию (в том числе и пароли) в некоторой зарезервированной для этого области.

Данный тип программных злоупотреблений включает [33, 40]:

- закладки, ассоциируемые с программно-аппаратной средой (BIOS);

- закладки, ассоциируемые с программами первичной загрузки, находящимися в Master Boot Record или Root секторов активных разделов;
- закладки, ассоциируемые с загрузкой драйверов DOS, командного интерпретатора, сетевых драйверов;
- закладки, ассоциируемые с прикладным программным обеспечением общего назначения (встроенные в клавиатурные или экранные драйверы, программы тестирования, утилиты и оболочки типа Norton Commander);
- исполняемые модули, содержащие только код закладки (как правило, внедряемые в пакетные файлы типа BAT);
- *м*одули-имитаторы, совпадающие по внешнему: виду с программами, требующими ввода конфиденциальной информации;
- Закладки, маскируемые под ПС оптимизационного назначения (архиваторы, ускорители и т.д.);
- закладки, маскируемые под ПС игрового и развлекательного назначения (как правило, используются для первичного внедрения закладок типа: "исследователь").

7. *Атаки "салями"* — характерны для финансовыми банковских информационных систем, где ежедневно проводятся тысячи операций, связанных с безналичными расчетами, переводами сумм, начислениями и т. д. [17, 30, 34]. При реализации расчетов вычисляются различного рода доли, которые округляются в большую или меньшую сторону. Атака "салями" состоит в накоплении на *от*дельном счете этих долей денежной единицы. Практика доказала, что эксплуатация такой программы обеспечивает накопление значительных сумм.

8. *Скрытые каналы* — это программы, передающие информацию лицам, которые в обычных условиях эту информацию получать не долж-нн1 [17]. Злоумышленник не всегда имеет непосредственный доступ к компьютерной системе. Для с.кры5гой передачи информации используют различные элементы, форматы "безобидных" отчетов, например, разную длину строк, пропуски между строками, наличие или отсутствие служебных заголовков, управляемый вывод незначащих цифр в выводимых величинах, количество пробелов или других символов в определенных местах отчета и т.д.;

При использовании скрытых каналов для получения относительно небольших объемов информации захватчик вынужден проделать достаточно большую работу. Поэтому скрытые каналы более приемлемы в ситуациях, когда нарушителя интересует не сама информация, а факт ее наличия.

Может возникнуть ситуация, когда скрытый канал сообщает о наличии в системе определенной информации, что в свою очередь служит признаком работы в системе определенного процесса, позволяющего провести атаку иного типа.

*9. Компьютерные вирусы* (КВ) — представляют собой программные разработки, способные проникать в среду компьютерных систем и наносить разного рода повреждения [17,21,22,29,35,36,37 и др.].

Вирусы представляют собой наиболее полно исследованный класс программных злоупотреблений превосходящий по разрушающим возможностям все другие.

Интересным является определение компьютерного вируса в законодательстве штата Техас (США) [38], как посторонняя (нежелательная) компьютерная программа или другой набор инструкций, внесенных в память компьютера, операционную систему или программу, при разработке которых они были специально снабжены способностью к воспроизведению или к воздействию на другие программы и файлы, находящиеся в компьютере, путем присоединения дубликата такой посторонней (нежелательной) программы к одной или более

компьютерным программам или файлам.

С развитием технологий обработки информации получили распространение и другие виды злоупотреблений. Самыми распространенными можно считать:

*"Отказы в обслуживании"* — несанкционированное использование компьютерной системы в своих целях (например, для бесплатного решения своих задач), либо блокирование системы для отказа в обслуживании другим пользователям. Для реализации такого злоупотребления используются так называемые "жадные программы" — программы, способные захватить монопольно определенный ресурс системы (причем необязательно центральный процессор). Следует отметить, что отказ в обслуживании пользователю, обладающему действительными правами доступа, может явиться одним из результатов функционирования таких программ, как "троянские кони", "люки" и другие.

*Работа между строк* (between lines) — подключение к линиям связи и внедрение в компьютерную систему с использованием промежутков в действиях законного пользователя [16, 28 и др.]. При интерактивной работе пользователя образуются своеобразные "окна" (например, отклик системы опережает действия пользователя, которому необходимо время для обдумывания последующих действий). Эти "окна" вполне могут быть использованы нарушителем для работы с системой под маской пользователя.

*Анализ трафика* (trafic analysis) — захватчик анализирует частоту и методы контактов пользователей в системе [16, 28 и др.]. При этом можно выяснить правила вступления в связь, после чего производится попытка вступить в контакт подвидом законного пользователя.

*Маскарад* (masquerade) — захватчик использует для входа в систему ставшую ему известной идентификацию законного пользователя [17, 28 и ДР.].

*"Подкладывание свиньи"* (piggback) — нарушитель подключается к линиям связи и имитирует работу системы с целью осуществления незаконных манипуляций. Например, он может имитировать сеанс связи и получить данные под видом легального пользователя. Пользователь, не подозревая об этом, передает информацию и/или получает ее. Таким образом, может осуществляться не только шпионаж, но и Дезинформация, что также отрицательно сказывается на работе АИС и объекта управления в целом.

*Повторное использование объектов* (object reutilization) — состоит в восстановлении и повторном использовании удаленных объектов системы.

Примером реализации подобного злоупотребления служит удаление файлов операционной системой. Когда ОС выдает сообщение, что, некоторый файл удален, то это не означает, что информация, содержащаяся в данном файле уничтожена в прямом смысле слова. Данное сообщение означает, что система пометила блоки памяти, ранее составлявшие содержимое файла, специальным флажком, говорящим о том, что данный блок не входит в состав какого-либо файла и может быть использован для размещения в нем другой информации. Но информация, которая была в данном блоке, никуда не исчезает до момента записи на это место другой информации. Таким образом, если прочесть содержание блока, можно получить доступ к "удаленной" информации (даже средствами ОС). Одной из разновидностей повторного использования объектов является работа с компьютерным "мусором". Компьютерным "мусором" являются данные, оставшиеся в памяти компьютера после завершения работы. Осуществляя сбор компьютерного "мусора" с помощью специальных программных средств, нарушитель имеет возможность проанализировать содержание информационной деятельности пользователей.

*Запуск "воздушного змея".* Для реализации подобного программного злоупотребления/используется такая последовательность действий. В двух или более банках открываются счета. Денежные средства переводятся из одного банка в другой с повышающимися размерами. Суть злоупотребления заключается в том, чтобы замаскировать

необеспеченный денежными средствами перевод. Данный цикл повторяется многократно, пока на конкретном счете не осядет значительная сумма [39]. После этого денежные средства снимаются и операции прекращаются. Следует отметить, что данное злоупотребление требует точного расчета и синхронизации последовательности действий нарушителей.

Несмотря на то, что данное злоупотребление не относится к "чисто" компьютерным, оно подготавливается и реализуется с помощью компьютера и программного обеспечения. В данном случае компоненты информационных и коммуникационных технологий используются в качестве средства подготовки и средства реализации преступления.

*"Раздеватели".* С развитием рынка "персональных" технологий, получило широкое распространение такое злоупотребление, как *нелегальное распространение, использование и/или изменение программных средств* [27, 40, 41 и др.].

Под *нелегальным распространением понимается продажа, обмен или бесплатное распространение программного продукта, авторские права на который принадлежат третьему лицу, без его Согласия.*

*Нелегальное использование* — это использование программного продукта без согласия владельца авторских прав.

*Нелегальное изменение* — это внесение в код программы или внешний вид (интерфейс) изменений, не оговоренных с владельцем авторских прав, с тем, чтобы измененный продукт не попадал под действие авторских прав.

Следует отметить, что проблема нелегального копирования и распространения программного обеспечения является актуальной. Это вызвано влиянием ряда объективных и субъективных факторов (социальных, экономических и др.). В условиях зарождения рынка сформировались группы специалистов, выполняющих работы по вскрытию средств защиты программных продуктов и нелегальному их распространению. Кроме того, некоторая часть программного обеспечения не обладает средствами защиты или они настолько слабы, что их устранение требует минимальных знаний в области информационных технологий.

С целью защиты программных продуктов от несанкционированного копирования (НСК), начали развиваться методы и средства защиты, основные из которых рассмотрены в (6, 41, 42, 43, 44].

Одновременно с этим на рынке появилось специальные средства для реализации НСК и "взлома" систем защиты [27, 33, 40 и др.].

Группа специальных средств, который предназначены для реализации НСК и снятия защиты в [41] названа "раздевателем". *Раздеватель* — комплекс специально разработанных программных средств, ориентированных на исследование Защитного механизма программного продукта от НСК и его преодоление. В данную группу входят следующие программные разработки, используемые для "вскрытия" защиты [42]:

• эмуляторы среды, предназначенные для подделки среды, в которой работает защищаемая программа;

• симулятор микропроцессора 8088;

• специальные отладчики для работы *в* защищенном режиме для 386-го микропроцессора.

Развитие средств связи и электронной почты выделило злоупотребление, которое относится к классу "компьютерного хулиганства" и в литературе получило название *"пинание"* (pinging) [28]. Суть данного злоупотребления заключается в том, что, используя стандартные или специально разработанные программные средства, злоумышленник; может вывести из строя электронный адрес, бомбардируя его многочисленными почтовыми сообщениями. Следствием "пинания" могут стать осложнения и возможность

непреднамеренного игнорирования полученной электронной почты.

Необходимо отметить, что при планировании и разработке злоупотреблений нарушителями могут создаваться новые, не приведенные в данной классификации, а также применяться любые сочетания описанных злоупотреблений.

СПИСОК ЛИТЕРАТУРЫ


1. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. М.:: Энергоатомиздат, 1994 .— Кн. 1, 2.
2. Зегжда П. Д., Матвеев .'В.' А.', Шмаков Э. М. Проблемы безопасности информационных технологий // Приборы и системы управления.—-1995 .—№ 6 . — С. 4-7.
3. Преснухин В. В., Пискова Г. К. Некоторые аспекты моделирования воспроизведения компьютерного вируса и совершенствования программных средств защиты // Информатика и вычислительная техника.—-1991 .—№4.— С. 52-58.
4. Автоматизированные информационные, ресурсы России. Состояние и тенденции развития (Национальный доклад) // Вестник Российского общества информатики и вычислительной техники.— 1994 - № 4-5 .— С. 7-66.
5. 5. Verdee N., Ohrimenco S., Paramonov D., Cernei Gh. Abuznri programate // Ciber. 1993 .—-№1-2. —С. 22-23.
6. Спесивцев А. В., Befrtep В. А., Крутков А. Ю., Серегин В. В., Сидоров В. А. 3aa9oiTk информации в персональных ЭВМ.— М.: *Радио и св*язь, "Веста", 1992.— 191 с.
7. Алексеев В. М., Андрианов В. В., Зефиров С. Л., Лупанов И. Ю. Комплекс защиты информации для автоматизированных информационных систем с использованием баз данных // Безопасность информационных технологий.— 1994 .— № 3-4 — 0,128-130.
8. Гарбарчук Д. А. "Группа МОСТ": Структура службы безопасности // Системы безопасности.— 1995- .-№5.— С. 54-55.
9. Смирнов В. Б. Системы охранного телевидения: Новый качественный уровень // Системы безопасности.— 1995 .—№5.—С. 48-49.
10. Вовченко В. В., Степанов И. О. Проблемы защиты информации от экономического шпионажа // Конфидент.— 1994 .— *№1*— С. 48-65.
11. Логинов А. Л., Елхимов Н. С. Общие принципы функционирования международных электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества // Конфидент.— 1995 .—№2.—С. 48-54.
12. Михайлов А. Г. Пластиковые карты с магнитя но6 полосой и защита систем электронных платежей // Конфидент— 1995 .—№2.—С. 43-47.
13. Андерсон Р. Чтобы системы на смарт-картах были Надежными // Конфидент.— 1995 .—№3.—С. 61-68.>.
14. Жаринов В. Ф., Киреев А. М., Синаев Д. В., Хмелев Л. С. К вопросу об использовании электронных идентификаторов Touch Memory в системах защиты конфиденциальной информации // Конфидент.— 1995 .—№3.—С. 26-31.
15. Курило А. П. О проблеме компьютерной преступности // НТИ. Сер. 1 — 1993 — №8— С. 6-9.

16. Давыдовский А. И., Дорошкевич П. В. Защита информации в вычислительных сетях // Зарубежная радиоэлектроника.— 1989 .—№12.—С. 60-70.

17. Гайкович В., Першин А. Безопасность электронных банковских систем.— М.: Изд-во компания "Единая Европа", 1993 .— 363 с.

18. Куранов А. И. Безопасность // Системы безопасности.— 1995 .—№4.—С. 38-41.

19. Домрачев А. А. Общие проблемы информационной безопасности и программа создания ИТКС // Конфидент.— 1995 .—№ 3.—С. 3-6.

20. Мафтик С. Механизмы защиты в сетях ЭЙМ— М.: Мир, 1993 — 216 с.

21. Недков С. Программи за проникване в **из**числителните системи // Автоматика изчислителна техника автоматизировани системи.— 1989 .— № 3.

22. Безруков Н. Н. Компьютерные вирусы.— М.: Наука, 1991 — 159 с.

23. Безруков Н. Н, Компьютерная вирусология.— Киев, УРЕ, 1991 — 416 с.

24. Расторгуев С. П. Исследование систем защиты информации // НТИ. Сер. 2 .— 1993 .— № 12.— С. 10-15.

25. Бачило И. Л. Методология решения правовых Проблем в области информационной безопасности// Информатика **и** вычислительная техника.— 1994. — № 2-3 — С. 21-25.

26. Давыдовский А. И. Методология построения безопасных процессов обработки информации // Безопасность информационных технологий.— 1994 .— №1.—С. 63-65.

27. Щербаков А. Разрушающие программные воздействия.— М.: Изд-во Эдель, 1993. — 64 с.

28. Охрименко С., Черней Г., Фотенко В., Руссу В. Система банковской безопасности. — Банковско-финансовый центр Республики Молдова, 1996 .— 79 с.

29. Охрименко С. А. Защита от компьютерных вирусов.— Кишинев: "Штиинца", 1991.— 101 с

30. Герасименко В. А. Проблемы защиты данных в системах их обработки // Зарубежная радиоэлектроника.— 1989 .—J^ 12.—С. 5-21.

31. Моисеенков И. Э. Суета вокруг Роберта или Моррис-сын и все, все, все... // КомпьютерПресс.— 1991 —№8.—С. 45-62; № 9. С. 7-20.

32. Касперский Е. "Дыры" в MS-DOS и программы защиты информации // КомпьютерПресс.— 1991.— № 10.

33. Щербаков А. Ю. Нетрадиционные методы проникновения к информации в компьютерных системах // Информатика и вычислительная техника.— 1994 .— № 2-3 .— С. 49-56.

34. Моисеенков И. Э. Основы безопасности компьютерных систем // КомпьютерПресс.— 1991 .— №10.—С. 19-24; №11.—С. 7-21; № 12 .— С. 57-'67.

35. Агеев А. С. "Компьютерные вирусы" и безопасность информации // Зарубежная радиоэлектроника.— 1989 .—№12.—С. 71-73.

36. Фигурнов В. Э. IBM PC для пользователя.— М.: Финансы и статистика, 1990 .— 240 с.

37. McAfee J. The virus cure // Datamaiton.— 1989 .— Vol. 35.—№4.

38. Никифоров И. Компьютерные преступления. Уголовные меры борьбы с

компьютерной преступностью // Конфидент.— 1995 .—№3.—С. 17-24.

39. Батурин Ю. М., Жиджитский А. М. Компьютерная преступность и компьютерная безопасность.— М: Юридическая литература, 1991 .— 162 с.
40. Щербаков А. Защита от копирования. Построение программных средств.— М.: Изд-во Эдель, 1992 .— 80 с.
41. Расторгуев С. П., Дмитриевский Н. Н. Искусство защиты и раздевания программ. — М.: Сов-маркет, 1991 .—94 с.
42. Расторгуев С. Купить или украсть? Оценка защиты // КомпьютерПресс.— 1992 .— №8.—С. 21-24.
43. Груздев С. 16 вариантов русской защиты // КомпьютерПресс, 1992 — №10.— С. 23-34.
44. Расторгуев С. П. Программные методы защиты информации в компьютерах и сетях.— М.: Изд-во агентства "Яхтсмен", 1993 .— 187 с.