и т. п.). Профессиональные знания, необходимые для повышения квалификации, можно получить на специальных факультетах или курсах повышения квалификации при высших учебных заведениях, в отраслевых или межотраслевых институтах повышения квалификации и их филиалах.

СПИСОК ЛИТЕРАТУРЫ:

1. *Зубков В. А., Осипов С. К.* Российская Федерация в международной системе противодействия легализации (отмыванию) преступных доходов и финансированию терроризма. М.: Издательский дом «Городец», 2006.
2. *Травин В. В., Дятлов В. А.* Основы кадрового менеджмента. М.: ЮНИТИ, 1995.
3. Управление персоналом организации. Учебник / Под ред. А. Я. Кибанова. М.: ИНФРА-М, 1997.
4. Управление персоналом. Учебно-практическое пособие для вузов / Под ред. А. Я. Кибанова. М., 1999.
5. *Шекшня С. В.* Управление персоналом современной организации. М.: ЗАО Бизнес-школа «Интел-синтез», 1998.
6. *Шкатулла В. И.* Настольная книга менеджера по кадрам. М.: Изд. группа «Норма-ИНФРА-М», 1998.

Л. А. Шивдяков

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЛЮЧЕВЫХ СИСТЕМАХ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ ОРГАНОВ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В КСИИ

(окончание)

Угрозы несанкционированного доступа к информации в вычислительной сети

К угрозам НСД к защищаемой информации в АС на базе АРМ относятся угрозы доступа к информации и программному обеспечению с нарушением установленных правил разграничения доступа. Для получения НСД используются штатные программные и аппаратные средства АС. Угрозы НСД, которые осуществляются с использованием дополнительных, специально создаваемых для этих целей программных (программно-аппаратных) средств, рассматриваются, вследствие специфики мероприятий по работе с ними, как самостоятельный класс угроз — угроз несанкционированных программно-математических воздействий (ПМВ) на защищаемую информацию и ресурсы АС.

При этом угрозы НСД (ПМВ) к информации обусловлены возможностями воздействия нарушителя на объективно существующие информационные потоки на отдельном АРМ оператора (отдельной ПЭВМ). При эксплуатации АС несколькими пользователями усложняется возможность установления факта НСД и истинного нарушителя, так как каждый из пользователей потенциально имеет доступ ко всем ресурсам АС.

Наиболее распространенными угрозами НСД (ПМВ) в АС являются:

— несанкционированное использование информационных ресурсов ЭВМ;

— хищение отчуждаемых (съемных) носителей информации;

— снятие неучтенной копии защищаемой информации с использованием дисковода, дисплея или принтера;

— программное копирование информации из ОЗУ и электронных носителей;

— несанкционированное использование оставшейся на носителях остаточной информации после ее обработки (в оперативной памяти, на ЖМД, ГМД и других носителях);

— подключение к устройствам ПЭВМ специальной аппаратуры, с помощью которой можно регистрировать информацию;

— изменение конфигурации ПЭВМ и вставка постороннего устройства;

— ввод в систему вредоносных ПС (ПМВ).

Субъектом НСД к информации может быть человек или инициализированный им процесс, действия которого нарушают регламентируемые на объекте правила разграничения доступа к информации.

НСД к информации на основе преодоления программных средств разграничения доступа к ресурсам компьютера может осуществляться за счет:

— проникновения в систему с несанкционированными параметрами входа — подбор пароля или обход защиты («взлом системы»). Подбор пароля может быть осуществлен различными способами. Так, например, вскрытие пароля возможно:

• простым перебором (который может выполнить специальная программа);

• используя системные файлы, в которых хранится информация о паролях;

• используя знания о типовых паролях, которые обычно применяются пользователями;

• используя программную закладку или вирус для «подсматривания» паролей. Обход парольной защиты можно осуществить, используя ошибки программы защиты или воздействуя на нее специальными программами;

— использования низкоуровневых процессов вычислительной системы, на которые не распространяется контроль средств защиты, например каналов обмена информацией между процессами в операционной системе («скрытые каналы»). В операционной системе (ОС) реализуются стандартные правила обмена информацией между устройствами и процессами, в связи с чем возможно осуществление контроля данной информации;

— использования скрытых, недокументированных разработчиками возможностей программного обеспечения («люков»). При разработке сложных программ многие их возможности не описываются в документации и могут быть неизвестны даже самим разработчикам данных программ;

— использования специальных ПМВ, осуществляемых вредоносными программами.

При эксплуатации ПЭВМ (АРМ) несколькими пользователями и наличии среди них возможного нарушителя опасность НСД возрастает, так как каждый из них имеет санкционированный доступ к средствам загрузки, ввода-вывода информации, что усложняет возможности по установлению факта НСД и истинного нарушителя.

Сетевые атаки в информационно-телекоммуникационных сетях общего пользования

Можно выделить шесть наиболее часто предпринимаемых в настоящее время типовых сетевых атак.

а) анализ сетевого трафика. Данная атака позволяет:

1) изучить логику работы сети — получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволит злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;

2) перехватить поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы — для извлечения секретной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т. п.;

б) сканирование сети. Сущность данной атаки заключается в передаче запросов сетевым службам хостов компьютерной сети и анализе ответов от них. Цель атаки — выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей;

в) подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.

Такая атака эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т. д. Под *доверенным объектом* будем понимать объект, легально подключенный к серверу. В более общем смысле «доверенная» система — это система, которая достигает специфического уровня контроля за доступом к информации, обеспечивая механизм предотвращения (или определения) неавторизованного доступа.

г) внедрение ложного объекта сети. Данная атака осуществляется двумя способами:

1) *навязыванием ложного маршрута* из-за недостатков, присущих алгоритмам маршрутизации (в частности, из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где с помощью определенных средств можно войти в операционную среду атакуемого компьютера;

2) *использованием недостатков алгоритмов удаленного поиска*. В случае, если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска (например, SAP в сетях Novell NetWare; ARP, DNS, WINS в сетях со стеком протоколов TCP/IP), заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата на атакующем объекте поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети. Эта атака позволяет проводить селекцию и сохранение потока информации, модифицировать информацию в передаваемых данных или в передаваемом коде, подменять информацию;

д) отказ в обслуживании. Атака заключается в передаче атакующим от имени легальных объектов большого количества запросов, адресованных сетевым службам. Эта атака может быть предпринята, если нет средств аутентификации адреса отправителя и с хоста на атакуемый хост можно передавать бесконечное число анонимных запросов на подключение от имени других хостов. Результатом осуществления данной атаки может стать нарушение работоспособности соответствующей службы, предоставление удаленного доступа на атакуемый хост, переполнение очереди запросов и, как следствие, невозможность обработки атакуемым хостом новых запросов на соединение;

е) удаленный запуск приложений. Атака заключается во внедрении и запуске на атакуемом хосте различных вредоносных программ:

1) программ-закладок;

2) вирусов;

3) «сетевых шпионов».

Основная цель перечисленных вредоносных программ — нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста.

Сопоставление представленных классов атак и основных схем их осуществления дано в таблице 1, а возможные последствия от реализации атак различных классов — в таблице 2.

Таблица 1. Классификация типовых удаленных атак

Признак типовой удаленной атаки	Характер воздействия		Цель воздействия			Условие начала осуществления воздействия			Наличие обратной связи с атакуемым объектом		Расположение субъекта атаки		Уровень модели OSI						
Класс атаки / схема атаки	1.1	1.2	2.1	2.2	2.3	3.1	3.2	3.3	4.1	4.2	5.1	5.2	6.1	6.2	6.3	6.4	6.5	6.6	6.7
1. Анализ сетевого трафика	+	-	+	-	-	-	-	+	-	+	+	-	-	+	-	-	-	-	-
2. Сканирование сети	+	-	+	-	-	-	-	+	-	+	+	-	-	+	-	-	-	-	-
3. Подмена доверенного объекта	-	+	+	+	-	-	+	-	+	+	+	+	-	-	+	+	-	-	-
4.1. Внедрение ложного объекта путем навязывания ложного маршрута	-	+	+	+	+	-	-	+	+	+	+	+	-	-	+	-	-	-	-
4.2. Внедрение ложного объекта путем использования недостатков алгоритмов удаленного поиска	-	+	+	+	-	+	-	+	+	-	+	+	-	+	+	+	-	-	-
5. Отказ в обслуживании	-	+	-	-	+	-	-	+	-	+	+	+	-	+	+	+	+	+	+
6. Удаленный запуск приложений		+	+	+	+	+	+	+	+	+	+	+	-	+	+	+	+	+	+

Таблица 2. Возможные последствия атак различных классов

Тип атаки	Возможные последствия
1. Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
2. Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
3. Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации

4. Внедрение ложного объекта сети		Несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений
5.Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
	Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установления соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т. д.)
	Нарушение логической связности между объектами	Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т. п.
	Использование ошибок в программах	Нарушение работоспособности сетевых устройств
6. Удаленный запуск приложений	Рассылка файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
	Путем переполнения буфера серверного приложения	
	Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Угрозы программно-математического воздействия на информацию при подключении к международным информационным сетям

Компьютерные вирусы (программные вирусы) изменяют свойства системы и, как следствие этого, являются источниками угроз безопасности при подключении к международным информационным сетям.

Компьютерные вирусы могут иметь следующие свойства:

- способность скрытия признаков своего присутствия в программной среде ЭВМ;
- способность самодублирования (копирования), ассоциирования себя с другими программами и/или переноса своих фрагментов в области оперативной или внешней памяти;
- возможность разрушения, искажения или модификации кодов программ в оперативной памяти и других носителях информации;
- возможность копирования фрагментов информации из оперативной памяти во внешнюю память;
- искажение произвольным образом, блокирование и/или подмена выводимых во внешнюю память или в канал связи массивов информации, образовавшихся в результате работы прикладных программ или уже находящихся во внешней памяти.

Самодублирование программы с потенциально опасными последствиями — процесс воспроизведения своего собственного кода в оперативной или внешней памяти ЭВМ.

Ассоциирование с другой программой — интеграция своего кода либо его части в код другой программы таким образом, чтобы при некоторых условиях управление передавалось на код программы с потенциально опасными последствиями.

В настоящее время широкое развитие получили программные вирусы, новые виды которых появляются по нескольку десятков в неделю.

Программные вирусы можно разделить на классы по следующим основным признакам:

- среда обитания;
- класс «заражаемой» операционной системы;
- особенности алгоритма работы;
- деструктивные возможности;
- характер воздействия на систему.

По среде обитания вирусы подразделяются на файловые, загрузочные, макро-, сетевые.

Файловые вирусы либо различными способами внедряются в выполняемые файлы баз данных (наиболее распространенный тип вирусов), либо создают файлы-двойники (компаньон-вирусы), либо используют особенности организации файловой системы (link-вирусы).

Загрузочные вирусы записывают себя либо в загрузочный сектор диска (boot-сектор), либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record), либо меняют указатель на активный boot-сектор.

Макровирусы заражают файлы-документы и электронные таблицы нескольких популярных редакторов.

Сетевые вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

По особенностям алгоритма работы компьютерные вирусы подразделяются на следующие группы:

- резидентные;
- использующие стелс-алгоритмы;
- использующие самошифрование и полиморфность;
- использующие нестандартные приемы.

Резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения операционной системы к объектам заражения и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки операционной системы. Нерезидентные вирусы не заражают память компьютера и сохраняют активность ограниченное время. Некоторые вирусы оставляют в оперативной памяти небольшие резидентные программы, которые не распространяют вирус. Такие вирусы считаются нерезидентными.

Резидентными можно считать макровирусы, поскольку они постоянно присутствуют в памяти компьютера в течение всего времени работы зараженного редактора. При этом роль операционной системы берет на себя редактор, а понятие «перезагрузка операционной системы» трактуется как выход из редактора.

Самошифрование и полиморфность используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру детектирования вируса. Полиморфные вирусы (polymorphic) — это достаточно трудно обнаруживаемые вирусы, не имеющие постоянных сигнатур, т. е. не содержащие ни одного постоянного участка кода. В большинстве случаев два образца одного и того же полиморфного вируса не будут иметь ни одного совпадения. Это достигается шифрованием основного тела вируса и модификациями программы-расшифровщика.

По деструктивным возможностям программные вирусы подразделяются на следующие группы:

- безвредные, т. е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
- неопасные, влияние которых ограничивается уменьшением свободной памяти на диске и графическими, звуковыми и прочими эффектами;

- опасные вирусы, которые могут привести к серьезным сбоям в работе компьютера;

- очень опасные, в алгоритм работы которых заведомо заложены процедуры, которые могут привести к потере программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизмов — вводить в резонанс и разрушать головки некоторых типов винчестеров.

По характеру воздействия на систему программные вирусы классифицируются следующим образом:

а) вирусы, не воздействующие на файловую структуру операционной системы:

1) размножающиеся в ОЗУ;

2) воздействующие на оператора;

3) имитирующие неисправность аппаратуры;

4) формирующие сообщения на терминале;

5) формирующие звуковые эффекты;

6) переключающие режимы настройки;

7) сетевые «черви»;

б) вирусы, воздействующие на файлы:

1) повреждающие исходные тексты программ, выполняемые программы, библиотеки программ;

2) повреждающие базы данных, текстовые документы, графические изображения, электронные таблицы;

в) вирусы, воздействующие на файловую подсистему ОС:

1) повреждающие системные области жесткого диска;

2) модифицирующие логическую структуру файловой подсистемы ОС;

3) производящие форматирование носителей информации;

4) воздействующие на файлы ОС;

5) криптующие информацию;

г) вирусы, воздействующие на аппаратуру:

1) воздействующие на графическую подсистему ЭВМ;

2) воздействующие на микросхемы ЭВМ (в том числе и на флэш-память);

3) воздействующие на жесткие магнитные диски;

4) воздействующие на принтер;

5) воздействующие на другие периферийные устройства ЭВМ.

Важнейшей особенностью компьютерных вирусов является высокая трудоемкость их выявления. В настоящее время не существует эффективных способов обнаружения неизвестных видов компьютерных вирусов в программном обеспечении.

Угрозы программно-математического воздействия, осуществляемые программными закладками

Угрозы, создаваемые целевым образом в ходе проектирования и разработки аппаратного и программного обеспечения в виде недекларированных возможностей операционных систем, прикладного программного обеспечения, электронного оборудования и т. п., реализуются в виде специально встроенных устройств и/или программных закладок (ПЗ).

Программные закладки — внесенные в программное обеспечение функциональные объекты, которые при определенных условиях (входных данных) инициируют выполнение неописанных в документации функций программного обеспечения, позволяющих осуществлять несанкционированные воздействия на информацию.

Как правило, любое сложное программное обеспечение содержит необъявленные возможности, которые предусмотрены разработчиком программного продукта. Кроме того, зачастую программный продукт может иметь скрытые возможности, о которых может не знать разработчик и которые вскрываются в процессе эксплуатации программы. Более того, не существует четкой границы определения, умышленно или неумышленно была предусмотрена в программном продукте та или иная возможность, которая в конечном счете привела к НСД.

Наличие в системе таких закладок открывает скрытые каналы доступа к информации и позволяет злоумышленнику обходить или блокировать защитные механизмы, предусмотренные в системе, в том числе парольную и криптографическую защиту.

Программные закладки могут быть внесены в программное обеспечение как на этапе разработки, так и в ходе эксплуатации и сопровождения программного продукта.

По признаку «время пребывания в оперативной памяти» программные закладки подразделяются на **резидентные** и **нерезидентные**.

ПЗ резидентного типа находятся в памяти постоянно с некоторого момента времени до окончания сеанса работы ЭВМ (выключения питания или перезагрузки). ПЗ может быть загружена в память при начальной загрузке ЭВМ, загрузке ОС либо при запуске некоторой программы (которая по традиции называется вирусоносителем), а также запущена отдельно.

ПЗ нерезидентного типа начинают работу аналогичным образом, но заканчивают ее самостоятельно по истечении некоторого промежутка времени или некоторого события, при этом выгружая себя из памяти целиком.

По методу внедрения ПЗ подразделяются на следующие группы:

- закладки, ассоциированные с программно-аппаратной средой;
- загрузочные закладки, ассоциированные с программами первичной загрузки (драйверные закладки, ассоциированные с загрузкой драйверов ОС, сетевых драйверов, т. е. с загрузкой операционной среды);
- закладки, ассоциированные с прикладным программным обеспечением общего назначения (встроенные в клавиатурные и экранные драйверы, программы тестирования ЭВМ, утилиты и оболочки);
- закладки, ассоциированные с исполняемыми программными модулями, содержащие код этих закладок;
- закладки-имитаторы, интерфейс которых совпадает с интерфейсом некоторых служебных программ, требующих ввода конфиденциальной информации (ключей, паролей);
- закладки, маскируемые под программные средства игрового и развлекательного назначения.

Так же как и для компьютерных вирусов, проблема обнаружения программных закладок или недекларированных возможностей в программном обеспечении не имеет эффективных алгоритмов решения, что выводит эти угрозы в разряд наиболее опасных и требует постоянного отслеживания информации о выявляемых дефектах программного или аппаратного обеспечения и высокой квалификации сотрудников.

Угрозы специальных воздействий на технические средства обработки защищаемой информации и средства вычислительной техники сверхкороткоимпульсными электромагнитными полями

К источникам угроз специальных электромагнитных воздействий на ТСОИ и СВТ относятся:

— передатчики электромагнитных излучений;

— генераторы электрических импульсов;

— генераторы импульсов магнитного поля.

Носителями угроз данного типа являются непрерывные и импульсные электромагнитные излучения, электрические импульсы большой мощности, магнитные импульсные поля.

Результатом электромагнитных воздействий на элементы аппаратуры ТСОИ и СВТ является возникновение множества деструктивных для ТСОИ и АС действий, которые проявляются:

— в отказах аппаратуры ТСОИ и АС с полным нарушением их работоспособности (тепловой разогрев подзатворного диэлектрика, лавинный и туннельный пробои в полупроводниках);

— в значительных ухудшениях параметров и характеристик полупроводниковых элементов аппаратуры ТСОИ и АС с сохранением их относительной работоспособности (изменение режимов работы, смещение рабочих точек нелинейных элементов и др.);

— в обратимых сбоях (электрическое защелкивание, изометрическая неустойчивость тока, лавинное умножение носителей в полупроводниках) в работе технических средств;

— в возрастании времени обработки информации в АС, сбоях и «зависании» работы ПЭВМ и других элементов вычислительной сети (наведение ложных управляющих сигналов на межблочных и внутриблочных соединительных линиях, возникающих при воздействии помеховых излучений).

Выявление и нейтрализация данного типа воздействий на ТСОИ и СВТ АС требует наличия специальной аппаратуры и значительных финансовых затрат.

Существующее большое разнообразие угроз безопасности информации затрудняет типовой подход к их классификации. В результате в научной литературе и на практике фигурирует множество различных классификационных схем, как правило, предназначенных для различных практических целей. В нашей статье мы отошли от классификации угроз с помощью традиционной блок-схемы, а привели их описание в таком порядке, какой нам представляется правильным по степени их важности для построения адекватной системы защиты информации в ключевых системах информационной структуры.

Заключение

Россия как одно из ведущих государств мира с его огромным научным, экономическим и интеллектуальным потенциалом всегда будет объектом для информационного воздействия со стороны ряда государств, претендующих на мировое господство. Чем выше будет наш научно-технический потенциал, тем больше информационно-телекоммуникационных ресурсов государства попадет в число потенциальных целей: телекоммуникации и связь, энергосистемы, транспорт, финансы, органы государственного и военного управления, предприятия ОПК, автоматизированные системы управления силовых ведомств и др. Это поднимает вопросы технической защиты информационных ресурсов государства на новый уровень — от потенциальной ямы пассивной теории к созданию упреждающих систем защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 1996 г. № 149-ФЗ. Ст. 3, 9, 16.

2. Федеральный закон «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ. Ст. 9, 17.

3. Распоряжение Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 9 сентября 2000 г. № р-1895.

4. Указ Президента Российской Федерации «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» от 17 марта 2008 г. № 351.

5. Указ Президента Российской Федерации «Об утверждении Концепции национальной безопасности Российской Федерации» от 17 декабря 1997 г. № 1300. Разд. 2.

6. Постановление Совета Министров — Правительства Российской Федерации «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам» от 15 сентября 1993 г. № 912-51. Разд. 1 ст. 9, 10, разд. 2 ст. 7, разд. 3 ст. 24, 25.

7. *Громыко И. А., Оспищев Е. Я., Кильмаев С. Ю.* Будущее за упреждающими системами защиты // Вопросы защиты информации. 2007. № 2. С. 11—14.