УДК 681.3

АНАЛИЗ МЕТОДОВ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

© 2018 П. И. Русанов, Д. Н. Мирошник, Т. С. Гурьева

Воронежский институт высоких технологий (г. Воронеж, Россия)
ОАО концерн «Созвездие» (г. Воронеж, Россия)

Статья посвящена анализу основных подходов, связанных с защитой автоматизированных систем. Показано, каким образом можно в информационных системах скрывать данные.

Ключевые слова: автоматизированная информационная система, метод, защита информации.

Внедрение защищенных информационных технологий в процессы обработки информации является сложным многоэтапным процессом.

На начальном этапе основные усилия разработчиков были направлены на создание средств вычислительной техники (СВТ), ориентированных на удовлетворение потребностей отдельных должностных лиц (автоматизация простейших процессов, подготовка документов в однопользовательском режиме и др.).

Следующий этап направлен на автоматизацию деятельности органов управления, когда задачи, решаемые отдельными должностными лицами, являются составной частью сложных процессов коллективной обработки информации. Для этого было необходимо объединение отдельных средств вычислительной техники в автоматизированные системы (АС), что, в свою очередь, потребовало разработку дополнительных средств защиты информации.

Создание объектов автоматизации диктует необходимость проработки дополнительных вопросов, связанных с обеспечением защиты от утечек информации по техническим каналам, в том числе с использованием специализированных информационных технологий, основанных на использовании криптографических методов

В современном мире число распределенных вычислительных систем постоянно растет. По сути, любую сеть можно отнести к этой категории. Однако чаще всего термин «распределенная вычислительная система» применяют к разнесенным в пространстве компьютерам, связь между которыми физически происходит на основе сетевых соединений и программным способом на базе механизма сообщений. Под такое описание подходит практически любая система, использующая для обмена информацией Интернет: локальные сети компании, домашний компьютер, Web-сервер и т. д. Сама технология распределенных вычислительных систем содержит немало «узких» мест, которыми могут воспользоваться различные злоумышленники. Вследствие этого существуют многочисленные проблемы информационной безопасности от непреднамеренных ошибок пользователей и персонала, обслуживающего информационную систему, до направленных попыток получения несанкционированного доступа к защищаемым ресурсам.

Знание наиболее распространенных угроз, которым подвержены современные компьютерные системы, а также уязвимых мест информационной системы, позволит выбрать наиболее эффективные средства обеспечения безопасности конфиденциальной, персональной или другой критической информации. Несмотря на наличие большого количества средств обеспечения защиты информации, а также литературы, посвященной теме информационной безопасности, существующие угрозы продолжают наносить существенный ущерб функционированию информационных систем. Ежегодное обследование проблем ИТ-безопасности Global Information Security Survey 2004 предоставило следующие результаты: 60 % опрошенных отметили, что неправомерные действия работников определяют угрозы для нормального функционирования информационных систем. Такой показатель превысил следующие «большие» проблемы, как спам (56 %), атаки типа

Русанов Петр Игоревич – Воронежский институт высоких технологий, студент, vwb5@mail.ru.
Денис Николаевич Мирошник – Воронежский институт высоких технологий, аспирант, e-mail: lommekingvl2309@vivt.ru.
Гурьева Татьяна Сергеевна – ОАО концерн «Созвездие», специалист, Kommm3mm3321weristy@yandex.ru.

«отказ в обслуживании» (48 %), осуществление финансового мошенничества (45 %) и пробелы для систем безопасности ПО (39 %), было меньше только по угрозам со стороны вирусов и червей (77 %). В первую десятку попали также другие внутренние угрозы – осуществление утечек информации по клиентам и иные виды кражи по конфиденциальным данным.

Выделяют следующие средства защиты информации, такие как:

- приложения криптографической защиты информации;
- антивирусное программное обеспечение;
- средства выявления слабых мест системы безопасности (сканеры безопасности);
- средства обнаружения попыток несанкционированного проникновения (IDS);
- межсетевые экраны или брандмауэры;
- средства организации виртуальных частных сетей (VPN);
- приложения фильтрации информационных ресурсов Интернета и электронной почты.

Основными задачами исследования являются:

- поиск и систематизация материала, посвященного современным средствам защиты информации;
- выявление основных типов угроз (атак), представляющих опасность защищаемой информации;
- анализ средств защиты информации на основании выявленных угроз, систематизация средств защиты в классы по функциональному назначению;
- анализ технологий и механизмов, на которых основаны современные средства защиты информации, выделение необходимых критериев классификации;
- представление полученных результатов в виде классификации, сопоставляющей вероятные угрозы информации с соответствующими программными средствами защиты.

Классификация – это упорядочивание или распределение объектов (предметы, явления, процессы, понятия) по классам в соответствии с определенным признаком. Выбор оптимальной структуры классификации включает попытки создания многопараметрических классификаций. Правильный выбор критерия классификации (или критериев – в случае многопараметрических классификаций), а также продуманная структура позволяют избежать таких проблем, возникающих при построении классификаций, как:

- повышение точности классификаций приводит к более сложной и разветвленной структуре, при этом теряется упорядоченность;
- относительность любой классификации - один и тот же объект может быть классифицирован по разным признакам или критериям;
- конфликт отнесения объекта к разным классификационным группировкам в зависимости от выбранного критерия.

Для построения классификации мы выбрали иерархический метод.

Достоинствами данного метода являются простота построения, а также возможность применения независимых классификационных признаков по различным ветвям иерархических структур. Однако при использовании данной структуры представление объекта, который может быть одновременно классифицирован по различным классификационным признакам, затруднительно. Так как в ходе анализа найденного материала данный случай был наиболее распространен, то предпочтительной стала структура, в которой выделяются критерии, представляющие собой совокупность элементов классификации.

Данная структура построения классификации позволяет наглядно представить объекты, классифицируемые по различным признакам. Каждый критерий классификации разбивает предметную область на определенные зоны.

Целью данной классификации является систематизация программных средств защиты информации, вследствие чего дальнейшая классификация продолжается именно в этом направлении, а остальные средства защиты, такие как физические или организационные выходят за рамки рассмотрения. Следующим шагом построения классификации является выделение вероятных угроз, предоставляющих опасность для нормального функционирования информационных систем. В это множество попадают следующие угрозы: вредоносное программное обеспечение, удаленные сетевые атаки, нарушение конфиденциальности информации и нарушение доступа. Данные типы угроз наиболее распространены, вследствие чего они и составляют следующий уровень классификации с классификационным признаком «по типам угроз».

Дальнейшая классификация будет рассматривать конкретные средства и методы обеспечения безопасности информации или

защиты от возможных атак для каждой из выделенных ранее угроз соответственно. Данная классификация не приводит конкретные программные продукты или их версии. Такой подход не эффективен ввиду того, что рынок средств защиты информации динамичен из-за своей специфики, так как от эффективных средств защиты требуется всегда быть на шаг впереди от средств нападения и преодоления защиты. Поэтому новые продукты появляются достаточно часто, вследствие чего их классификация теряет актуальность в довольно короткий промежуток времени. Вместо этого используется другой подход к классификации, а именно делается упор на технологии, методы и способы, которые используются в современных средствах защиты, а также на их достоинства и недостатки, так как в отличие от конечных программных продуктов они имеют более долгий период жизни. Вследствие этого с помощью подобной классификации можно легко охарактеризовать тот или иной программный продукт, зная используемые методы и технологии, применяемые при его реализации, и оценить его возможности.

В категорию искусственных преднамеренных угроз попадают основные пути, связанные с умышленной дезорганизацией работ, выводом систем из строя, проникновением в системы и несанкционированным доступом к информации. Угрозы этой категории наиболее часто ассоциируются с понятием компьютерная атака. Поэтому дальнейший анализ будет производиться над угрозами именно из этой категории. В классификации выделяются следующие типы атак, которые принадлежат к классу искусственных преднамеренных угроз: сетевые атаки; вирусные атаки; нарушение конфиденциальности; нарушение доступа.

Средствами защиты от вирусной угрозы по функциональным возможностям являются: детектор - позволяет только обнаруживать присутствие вирусных программ, известных им; ревизор - позволяет производить контроль целостности хранящейся информации, запоминая текущее состояние и реагируя на последующие изменения в структуре каталогов и свойствах файлов; иммунизатор - программа, применение которой позволяет избежать конкретной угрозы; фаги и полифаги - наиболее функциональные прикладные пакеты. Содержат функции детектирования, устранения и восстановления против действий вирусов различных типов.

Однако наибольший интерес представляют используемые технологии обнаружения зловредного кода. В настоящее время существует и активно используется три технологии сканирования:

- сигнатурный анализ – предлагает быстрый способ идентификации вирусов, но его польза уменьшается или становится бесполезной при обнаружении нового вируса;

- эвристический анализ – заключается в поиске признаков кода, который может выполнять злонамеренные функции. В свою очередь по методу анализа подразделяется на статический и динамический эвристический анализ;

- анализ поведения программного обеспечения – анализатор интегрируется с операционными системами хостов и наблюдает работу разных программ по реальному времени, с точки зрения попыток ведения подозрительных действий. Существующие системы блокирования поведения можно разделить на две категории: системы блокирования на основе политики и на основе экспертизы.

Нарушение конфиденциальности информации заключается в использовании данной информации неавторизованными для этого лицами. Вот почему для гарантированной защиты от несанкционированного использования к секретным данным нужно применять более серьезные методы, особенно если речь идет о корпоративной информации.

Для предотвращения несанкционированного доступа можно хранить всю конфиденциальную информацию на съемных носителях – магнитных лентах, магнитооптических дисках и дискетах. Но у такого способа хранения имеются существенные недостатки:

- съемные носители имеют ограниченный объем, и для хранения на них большого объема секретной информации нужно заводить картотеки таких носителей – что и где записано;

- необходимость надежного физического хранения таких накопителей, например, в сейфах;

- необходимость контроля доступа к этим носителям – назначение администратора, который будет выдавать их под роспись сотрудникам, ведение специальных журналов учета и так далее;

- человеческий фактор – при необходимости частого доступа к такой информации все эти правила хранения могут попросту нарушаться: диски с секретными данными могут быть помещены в ящик рабочего сто-

ла, а секретная информация может быть скопирована на жесткий диск.

Более простой и надежной альтернативой является защита конфиденциальной информации с помощью шифрования. Существуют различные методы обеспечения конфиденциальности с помощью шифрования, отличающиеся степенью надежности сохраняемой информации. Это такие методы, как: архивация с паролем; использование прикладных шифрующих приложений; криптографические файловые системы.

Архивация отдельных файлов и каталогов с паролем является простейшим способом шифрования данных. Во многие архиваторы встроена функция шифрования, и эти программные средства всегда под рукой у пользователя. Неудобством их применения можно назвать необходимость ручных операций при создании архивов. Впрочем, современные архиваторы лишены и этого недостатка – с их помощью можно легко защитить архив паролем прямо из меню программы. Но основной и более значимой причиной, по которой нельзя рассматривать архивирование с паролем в качестве серьезного метода, является невысокая степень предоставляемой защиты данных.

Гораздо надежнее для шифрования отдельных файлов пользоваться специальными программами – шифровальными машинками. Для извлечения файла из архива нужен всего лишь пароль, который может быть подобран с помощью специальных утилит. Для доступа к зашифрованным файлам нужен не только пароль, но и шифр, без обладания которыми злоумышленник не сможет открыть эти файлы. Шифрование файлов дает практически стопроцентную гарантию их защиты при условии, что пользователь не разбрасывает свои пароли и шифры, а хранит их в защищенном месте.

Программы шифрования отдельных файлов требуют от пользователя особой внимательности. Важно не забывать после работы с расшифрованным файлом опять его зашифровать. Иначе, понятное дело, он будет доступен для просмотра всем, кто получит физический доступ к диску. Но самым главным недостатком описанного метода является то, что он не защищает от такой угрозы, как возможность простого удаления самого зашифрованного файла.

Отмеченных выше недостатков лишены средства шифрования информации, использующие иные принципы работы – программы шифрования «на лету». Такие программы встраиваются в качестве промежуточного звена в процесс обмена информацией между жестким диском и процессором. Программы контролируют этот процесс, зашифровывая или расшифровывая данные при их чтении и записи. Преобразование данных происходит в автоматическом режиме, что позволяет пользователю работать в привычном для него порядке, не обращая внимания на вмешательство программы.

Первые программные реализации идеи шифрования «на лету» имели один существенный недостаток: для хранения информации, подлежащей шифрованию, необходимо было зарезервировать определенный объем дискового пространства. Самые первые программы этого класса умели «прозрачно» шифровать один и даже несколько логических дисков. Немного позже появились программы, создающие для шифрованной информации один огромный файл и работающие с ним, как с отдельным логическим диском. В обоих случаях невозможно было предугадать точный объем конфиденциальной информации, которую нужно будет шифровать, поэтому, как правило, под зашифрованные диски отводилось мало места. Если эти секретные данные переставали помещаться на дисках, приходилось создавать новые логические диски.

Следующим шагом стала реализация той же идеи шифрования «на лету», но несколько иным способом. Теперь «прозрачному» шифрованию подвергаются не секторы жестких дисков, а объекты, расположенные на этих дисках. Различают шифрование томов, шифрование файловых систем и шифрование файлов. Закрытая информация хранится в так называемых криптозонах, доступ к которым можно получить только с помощью самой программы шифрования, естественно, зная пароли. Остальная, незашифрованная информация хранится на тех же дисках как обычно - в открытом виде. Такой подход к шифрованию позволяет отказаться от резервирования места на диске под хранение секретной информации, и ее объем зависит лишь от физического размера жесткого диска.

Шифрование томов определяет возможности кодирования по всем логическим разделам и является удобным и интуитивно понятно для применения конечными пользователями, хотя и не дает надежный контроль над доступом к отдельным директориям или файлам.

Шифрование файлов связано с уровнем приложений и дает возможности надежного

непрерывного кодирования файлов. Для того, чтобы придать определенную прозрачность для конечного файла пользователя приложения обычно слегка переписываются, чтобы поддержать шифр. Такой метод оправдан только для небольшого количества файлов, но не совсем пригоден для систем сохранения.

Метод шифрования файловых систем лишен данного недостатка и предоставляет прозрачное шифрование файлов на основании прав доступа как к файлу, так и к каталогу, используя единый ключ.

И все же с помощью программ шифрования нельзя достичь стопроцентной защиты. Их уязвимость заключается в том, что взаимодействие с программой шифрования осуществляется через стандартный интерфейс операционной системы, а значит, нельзя сбрасывать со счетов такие угрозы, как мониторинг устройств ввода-вывода, перехват информации при ее обмене с различными сетевыми устройствами, удаленную запись изображения с экрана монитора. Поэтому шифрование можно назвать хоть и действенной, но все-таки небольшой частью комплекса программно-технических мероприятий для обеспечения компьютерной безопасности.

Приведенные выше методы применяются, если необходимо обеспечение конфиденциальности локальной информации, которая используется и хранится на одном ПК, и не применимы в случае, когда требуется защита информации, передающейся по локальной или глобальной сети как между отдельными узлами, так и между сегментами сети. В этом случае применима технология виртуальных частных сетей (Virtual private network).

Можно выделить два возможных способа скрытия данных:

- шифрование передающейся по сети информации. Технология IPSec;

- разделение трафика в канале передачи.

Второй способ зависит от применения его в локальной или глобальной сети. В первом случае это всем известная технология, базирующаяся на виртуальных локальных сетях (VLAN), применяемая для того, чтобы структурировать современные локальные сети. Для глобальных сетей распространение имеет аналог VLAN – технология MPLS (Multiprotocol Label Switching), она также применяет метки для того, чтобы разделять трафик и образовывать виртуальные каналы в IP, ATM и других сетях. Однако у технологии MPLS есть один недостаток (с точки зрения безопасности) – она может применяться только для связи «сеть – сеть» и не применима для соединения с отдельными узлами. Есть и второй недостаток – данные разных пользователей хоть и не смешиваются, но все-таки к ним можно получить данные, прослушивая сетевой трафик. Кроме того, провайдер, предлагающий услуги MPLS, будет иметь доступ ко всей передаваемой информации.

Поэтому более надежной является технология шифрования трафика, основанная на защищенном протоколе IP – IPSec. Именно эта технология применяется многими разработчиками средств сетевой безопасности. Фактически протокол IPSec – это комплекс стандартов, протоколов, алгоритмов шифрования и методов хеширования, которые при необходимости могут быть объединены так, чтобы удовлетворять требованиям различных приложений. Применение этой технологии позволяет строить надежные и эффективные частные сети на основе выделенных и коммутируемых каналов доступа.

Можно выделить четыре основных варианта построения сети VPN:

- Intranet VPN – позволяет объединить в единую защищенную сеть несколько распределенных филиалов одной организации, взаимодействующих по открытым каналам связи;

- Remote Access VPN – позволяет реализовать защищенное взаимодействие между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который подключается к корпоративным ресурсам из дома (домашний пользователь) или через notebook (мобильный пользователь). Данный вариант отличается от первого тем, что удаленный пользователь, как правило, не имеет статического адреса, и он подключается к защищаемому ресурсу не через выделенное устройство VPN, а прямиком со своего собственного компьютера, на котором и устанавливается программное обеспечение, реализующее функции VPN. Компонент VPN для удаленного пользователя может быть выполнен как в программном, так и в программно-аппаратном виде. В первом случае программное обеспечение может быть как встроенным в операционную систему (например, в Windows 2000), так и разработанным специально. Во втором случае для реализации VPN применяются небольшие устройства класса SOHO (Small Office\Home Office), которые не требуют серьезной на-

стройки и могут быть использованы даже неквалифицированным персоналом:

- Client/Server VPN – обеспечивает защиту передаваемых данных между двумя узлами (не сетями) корпоративной сети. Особенность данного варианта в том, что VPN строится между узлами, находящимися, как правило, в одном сегменте сети, например, между рабочей станцией и сервером. Такая необходимость очень часто возникает в тех случаях, когда в одной физической сети необходимо создать несколько логических сетей. Например, когда надо разделить трафик между финансовым департаментом и отделом кадров, которые обращаются к серверам, находящимся в одном физическом сегменте. Этот вариант похож на технологию VLAN, описанную выше. Но вместо разделения трафика используется его шифрование;

- Extranet VPN – предназначен для тех сетей, к которым подключаются так называемые пользователи «со стороны» (партнеры, заказчики, клиенты и т. д.), уровень доверия к которым намного ниже, чем к своим сотрудникам. Хотя по статистике чаще всего именно сотрудники являются причиной компьютерных преступлений и злоупотреблений.

Средства построения VPN могут быть реализованы по-разному:

- в виде специализированного программно-аппаратного обеспечения, предназначенного именно для решения задач VPN. Основное преимущество таких устройств - их высокая производительность и более высокая, по сравнению с другими решениями, защищенность. Такие устройства могут применяться в тех случаях, когда необходимо обеспечить защищенный доступ большого числа абонентов. Недостаток таких решений состоит в том, что управляются они отдельно от других решений по безопасности, что усложняет задачу администрирования инфраструктуры безопасности. На первое место эта проблема выходит при построении крупной и территориально-распределенной сети, насчитывающей десятки устройств построения VPN;

- в виде программного решения, устанавливаемого на обычный компьютер, функционирующий, как правило, под управлением операционной системы Unix. Для ускорения обработки трафика могут быть использованы специальные аппаратные ускорители, заменяющие функции программного шифрования. Также в виде программного решения реализуются абонентские пункты, предназначенные для подключения к защищаемой сети удаленных и мобильных пользователей;

- интегрированные решения, в которых функции построения VPN реализуются наряду с функцией фильтрации сетевого трафика, обеспечения качества обслуживания или распределения полосы пропускания. Основное преимущество такого решения – централизованное управление всеми компонентами с единой консоли. Второе преимущество – более низкая стоимость в расчете на каждый компонент по сравнению с ситуацией, когда такие компоненты приобретаются отдельно.

Научная новизна: построенная классификация является обобщением существующих технологий современных средств защиты, их достоинств и недостатков, а также сфер применения и функциональных возможностей. В результате анализа выявлены наиболее типичные угрозы информационной системы, а также программные средства, технологии и методы их устранения. Практическая ценность: данная классификация, сопоставляющая вероятные угрозы информации с соответствующими программными средствами защиты, ориентирована на использование при формировании политики безопасности. Перспективным аспектом развития данной классификации является ее дальнейшее расширение, поиск и систематизация средств и методов защиты, выявление новых видов угроз.

Итак, система обеспечения информационной безопасности в современных организациях имеет сложную многокомпонентную, многоуровневую, территориально и логически распределенную архитектуру. Компоненты системы обеспечения информационной безопасности очень тесно интегрированы в информационную инфраструктуру организации. Помимо программных и технических средств обеспечения информационной безопасности, которые могут быть встроены в телекоммуникационное и компьютерное оборудование, операционные системы и приложения, а также специализированных (наложенных) средств защиты информации, архитектура системы обеспечения информационной безопасности включает в себя также систему организационных мероприятий и ИТ-процессов. Для построения системы обеспечения информационной безопасности требуются профессиональные знания, активная поддержка руководства организации и серьезное финансирование.

ЛИТЕРАТУРА

1. Научные ответы на вызовы современности: техника и технологии / Н. М. Агеева [и др.]; Книга 2. – Одесса, Издательство: Куприенко Сергей Васильевич (Одесса). – 2016. – 189 с.

2. Воронов А. А. Обеспечение системы управления рисками при возникновении угроз информационной безопасности / А. А. Воронов, И. Я. Львович, Ю. П. Преображенский, В. А. Воронов // Информация и безопасность. – 2006. – Т. 9. – № 2. – С. 8-11.

3. Гуськова Л. Б. О построении автоматизированного рабочего места менеджера / Л. Б. Гуськова // Успехи современного естествознания. – 2012. – № 6. – С. 106.

4. Зяблов Е. Л. Разработка лингвистических средств интеллектуальной поддержки на основе имитационно-семантического моделирования / Е. Л. Зяблов, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 024-026.

5. Львович И. Я. Особенности проектирования корпоративных компьютерных сетей / И. Я. Львович, А. П. Преображенский, О. Н. Чопоров // Оптимизация и моделирование в автоматизированных системах. Материалы всероссийской молодежной научной школы. Министерство образования и науки РФ, Воронежский государственный технический университет, Российский фонд фундаментальных исследований. – 2017. – С. 16-20.

6. Львович И. Я. Применение информационных технологий в медицинской сфере / И. Я. Львович, А. П. Преображенский, О. Н. Чопоров // Интеллектуальные информационные системы. Труды Материалы всероссийской конференции с международным участием. – 2017. – С. 164-165.

7. Львович И. Я. Разработка системы учета заявок на ремонт оборудования / И. Я. Львович, А. П. Преображенский, О. Н. Чопоров // Перспективные достижения современных ученых. Техника и технологии. – Одесса. – 2017. – С. 48-74.

8. Львович И. Я. Факторы угрозы экономической безопасности государства / И. Я. Львович, А. А. Воронов, Ю. П. Преображенский // Информация и безопасность. – 2006. – Т. 9. – № 1. – С. 36-39.

9. Максимов И. Б. Принципы формирования автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 130-135.

10. Максимов И. Б. Классификация автоматизированных рабочих мест / И. Б. Максимов // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 127-129.

11. Пеньков П. В. Экспертные методы улучшения систем управления / П. В. Пеньков // Вестник Воронежского института высоких технологий. – 2012. – № 9. – С. 108-110.

12. Преображенский А. П. Применение статистических методов при управлении предприятием / А. П. Преображенский, О. Н. Чопоров // Наука Красноярья. – 2017. – Т. 6. – № 1-2. – С. 273-278.

13. Преображенский А. П. Особенности работы малых предприятий / А. П. Преображенский, О. Н. Чопоров // Наука Красноярья. – 2017. – Т. 6. – № 3.3. – С. 178-182.

14. Преображенский Ю. П. Оценка эффективности применения системы интеллектуальной поддержки принятия решений / Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2009. – № 5. – С. 116-119.

15. Самойлова У. А. О некоторых характеристиках управления предприятием / У. А. Самойлова // Вестник Воронежского института высоких технологий. – 2014. – № 12. – С. 176-179.

16. Фомина Ю. А. Принципы индексации информации в поисковых системах / Ю. А. Фомина, Ю. П. Преображенский // Вестник Воронежского института высоких технологий. – 2010. – № 7. – С. 98-100.

ANALYSIS OF METHODS OF PROTECTION OF THE AUTOMATED SYSTEMS

© 2018 П. И. Русанов, D. N. Miroshnik, T. S. Guryeva

Voronezh Institute of High Technologies (Voronezh, Russia)
JSC concern «Sozvezdie» (Voronezh, Russia)

The paper is devoted to the analysis of the main approaches related to the protection of automated systems. It is shown how it is possible to hide data in information systems.

Key words: automated information system, method, information protection.