УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ

“БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ”

Кафедра защиты информации

**РЕФЕРАТ**

**На тему:**

**«**Противодействие техническим средствам разведки**»**

МИНСК, 2008

Противодействие техническим средствам разведки (ТСР) представляет собой совокупность согласованных мероприятий, предназначенных для исключения или существенного затруднения добывания охраняемых сведений с помощью технических средств.

Добывание информации предполагает наличие информационных потоков от физических носителей охраняемых сведений к системе управления. При использовании TCP такие информационные потоки образуются за счет перехвата и анализа сигналов и полей различной физической природы. Источниками информации для технической разведки являются содержащие охраняемые сведения объекты. Это позволяет непосредственно влиять на качество добываемой злоумышленником информации и в целом на эффективность его деятельности путем скрытия истинного положения и навязывания ложного представления об охраняемых сведениях.

Искажение или снижение качества получаемой информации непосредственно влияет на принимаемые злоумышленником решения и, через его систему управления, на способы и приемы исполнения решения. Непосредственный контакт принципиально необходим на этапах добывания информации и исполнения решения, причем добывание информации должно предшествовать принятию решения и его исполнению злоумышленником. Поэтому противодействие ТСР должно носить упреждающий характер и реализовываться заблаговременно.

Любая система технической разведки (рис. 1) содержит следующие основные элементы:

— технические средства разведки (TCP);

— каналы передачи информации (КПИ);

— центры сбора и обработки информации (ЦСОИ).

Технические средства разведки представляют собой совокупность разведывательной аппаратуры, предназначенной для обнаружения демаскирующих признаков, предварительной обработки, регистрации перехваченной информации и ее передачи через КПИ в ЦСОИ. В ЦСОИ информация от различных TCP накапливается, классифицируется, анализируется и предоставляется потребителям (автоматизированным системам управления или лицам, принимающим решения. Таким образом, в системе технической разведки реализуется обнаружение и анализ демаскирующих признаков (ДП).

|  |
| --- |
| Рис. 1. Упрощенная структурная схема системы технической разведки |

Обнаружение ДП по физической сути заключается в выполнении следующих операций:

— поиск и обнаружение энергии ДП в пространстве, во времени, по спектру и т.д.;

— выделение ДП из искусственных и естественных помех.

Физический смысл анализа ДП раскрывают следующие операции:

— разделение ДП различных объектов;

— оценка параметров ДП (определение их объективных характеристик);

— сокращение избыточности информации;

— регистрация, накопление и классификация ДП;

— нахождение местоположения источника ДП;

— распознавание смыслового содержания ДП;

— выявление охраняемых сведений.

В соответствии с приведенной классификацией главными направлениями снижения эффективности TCP является противодействие обнаружению ДП и противодействие их анализу.

При противодействии обнаружению ДП преследуется цель скрытия от TCP демаскирующих признаков. Соответственно все организационные и технические способы, предназначенные для исключения или существенного затруднения обнаружения ДП, составляют одно из главных направлений противодействия TCP — скрытие.

Другим основным направлением является техническая дезинформация, которая объединяет все организационно-технические меры противодействия, направленные на затруднение анализа ДП и навязывание противнику ложной информации.

Скрытие, обеспечивая противодействие обнаружению, всегда затрудняет или исключает возможность проведения анализа демаскирующего признака. Техническая дезинформация, наоборот, затрудняя анализ, как правило, не влияет на возможность обнаружения объекта разведки.

Некоторые ТСР предназначены для обеспечения активного воздействия на любые объекты, чьи сигналы оказываются в заданных диапазонах поиска и обнаружения. Техническая дезинформация в такой ситуации может оказаться неэффективной. Поэтому реализация стратегии скрытия объекта является более радикальным направлением противодействия TCP, чем техническая дезинформация.

Однако на практике часто встречаются ситуации, когда невозможно обеспечить при ограниченных ресурсах надежное скрытие объекта (например, крупного здания или сооружения) или отдельных демаскирующих признаков (таких, как мощные непрерывные электромагнитные излучения радиоэлектронных и оптических систем на открытой местности). В подобных ситуациях цели противодействия техническим средствам разведки могут достигаться только применением методов и средств технической дезинформации.

Кроме рассмотренных мер ПД TCP, предполагающих нормальное функционирование всех составных частей системы разведки, возможно проведение активных действий по выявлению и выведению из строя элементов системы разведки.

Основными функциями системы разграничения доступа (СРД) являются:

— реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;

— реализация ПРД субъектов и их процессов к устройствам создания твердых копий;

— изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;

— управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;

— реализация правил обмена данными между субъектами для автоматизированных систем (АС) и средств вычислительной техники, построенных по сетевым принципам.

Функционирование СРД опирается на выбранный способ разграничения доступа. Наиболее прямой способ гарантировать защиту данных — это предоставить каждому пользователю вычислительную систему как его собственную. В многопользовательской системе похожих результатов можно добиться использованием модели виртуальной ЭВМ.

При этом каждый пользователь имеет собственную копию операционной системы. Монитор виртуального персонального компьютера для каждой копии операционной системы будет создавать иллюзию, что никаких других копий нет и что объекты, к которым пользователь имеет доступ, являются только его объектами. Однако при разделении пользователей неэффективно используются ресурсы АС.

В АС, допускающих совместное использование объектов доступа, существует проблема распределения полномочий субъектов по отношению к объектам. Наиболее полной моделью распределения полномочий является матрица доступа. Матрица доступа является абстрактной моделью для описания системы предоставления полномочий.

Строки матрицы соответствуют субъектам, а столбцы — объектам; элементы матрицы характеризуют право доступа (читать, добавлять информацию, изменять информацию, выполнять программу и т.д.). Чтобы изменять права доступа, модель может, например, содержать специальные права владения и управления. Если субъект владеет объектом, он имеет право изменять права доступа других субъектов к этому объекту. Если некоторый субъект управляет другим субъектом, он может удалить права доступа этого субъекта или передать свои права доступа этому субъекту. Для того чтобы реализовать функцию управления, субъекты в матрице доступа должны быть также определены в качестве объектов.

Элементы матрицы установления полномочий (матрицы доступа) могут содержать указатели на специальные процедуры, которые должны выполняться при каждой попытке доступа данного субъекта к объекту и принимать решение о возможности доступа. Основами таких процедур могут служить следующие правила:

— решение о доступе основывается на истории доступов других объектов;

— решение о доступе основывается на динамике состояния системы (права доступа субъекта зависят от текущих прав других субъектов);

— решение о доступе основывается на значении определенных внутрисистемных переменных, например значений времени и т.п.

В наиболее важных АС целесообразно использование процедур, в которых решение принимается на основе значений внутрисистемных переменных (время доступа, номера терминалов и т.д.), так как эти процедуры сужают права доступа.

Матрицы доступа реализуются обычно двумя основными методами — либо в виде списков доступа, либо мандатных списков. Список доступа приписывается каждому объекту, и он идентичен столбцу матрицы доступа, соответствующей этому объекту. Списки доступа часто размещаются в словарях файлов. Мандатный список приписывается каждому субъекту, и он равносилен строке матрицы доступа, соответствующей этому субъекту. Когда субъект имеет права доступа по отношению к объекту, то пара (объект — права доступа) называется мандатом объекта.

На практике списки доступа используются при создании новых объектов и определении порядка их использования или изменении прав доступа к объектам. С другой стороны, мандатные списки объединяют все права доступа субъекта. Когда, например, выполняется программа, операционная система должна быть способна эффективно выявлять полномочия программы. В этом случае списки возможностей более удобны для реализации механизма предоставления полномочий.

Некоторые операционные системы поддерживают как списки доступа, так и мандатные списки. В начале работы, когда пользователь входит в сеть или начинает выполнение программы, используются только списки доступа. Когда субъект пытается получить доступ к объекту в первый раз, список доступа анализируется и проверяются права субъекта на доступ к объекту. Если права есть, то они приписываются в мандатный список субъекта и права доступа проверяются в дальнейшем проверкой этого списка.

При использовании обоих видов списков список доступа часто размещается в словаре файлов, а мандатный список — в оперативной памяти, когда субъект активен. С целью повышения эффективности в техническом обеспечении может использоваться регистр мандатов.

Третий метод реализации матрицы доступа — так называемый механизм замков и ключей. Каждому субъекту приписывается пара (А, К), где А— определенный тип доступа, а К— достаточно длинная последовательность символов, называемая замком. Каждому субъекту также предписывается последовательность символов, называемая ключом. Если субъект захочет получить доступ типа А к некоторому объекту, то необходимо проверить, что субъект владеет ключом к паре (А, К), приписываемой конкретному объекту.

К недостаткам применения матриц доступа со всеми субъектами и объектами доступа можно отнести большую размерность матриц. Для уменьшения размерности матриц установления полномочий применяют различные методы сжатия:

— установление групп пользователей, каждая из которых представляет собой группу пользователей с идентичными полномочиями;

— распределение терминалов по классам полномочий;

— группировка элементов защищаемых данных в некоторое число категорий с точки зрения безопасности информации (например, по уровням конфиденциальности).

По характеру управления доступом системы разграничения разделяют на дискреционные и мандатные.

Дискреционное управление доступом дает возможность контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам и т.п.). Например, владельцам объектов предоставляется право ограничивать доступ к этому объекту других пользователей. При таком управлении доступом для каждой пары (субъект—объект) должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта к данному объекту. Однако имеются и другие задачи управления доступом, которые не могут быть решены только дискреционным управлением. Одна из таких задач — позволить администратору АС контролировать формирование владельцами объектов списков управления доступом.

Мандатное управление доступом позволяет разделить информацию на некоторые классы и управлять потоками информации при пересечениях границ этих классов.

Во многих системах реализуется как мандатное, так и дискреционное управление доступом. При этом дискреционные правила разграничения доступа являются дополнением мандатных. Решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должны контролироваться не только единичный акт доступа, но и потоки информации.

Обеспечивающие средства для системы разграничения доступа выполняют следующие функции:

— идентификацию и опознавание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;

— регистрацию действий субъекта и его процесса;

— предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;

— реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление системы защиты после НСД;

— тестирование всех функций защиты информации специальными программными средствами;

— очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными путем двукратной произвольной записи;

— учет выходных печатных и графических форм и твердых копий в АС;

— контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Для каждого события должна регистрироваться следующая информация, дата и время; субъект, осуществляющий регистрируемое действие; тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа); успешно ли осуществилось событие (обслужен запрос на доступ или нет).

Выдача печатных документов должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе общего количества листов (страниц). Вместе с выдачей документа может автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа.

Автоматическому учету подлежат создаваемые защищаемые файлы, каталоги, тома, области оперативной памяти персонального компьютера, выделяемые для обработки защищаемых файлов, внешних устройств и каналов связи.

Такие средства, как защищаемые носители информации, должны учитываться документально, с использованием журналов или картотек, с регистрацией выдачи носителей. Кроме того, может проводиться несколько дублирующих видов учета.

Реакция на попытки НСД может иметь несколько вариантов действий:

— исключение субъекта НСД из работы АС при первой попытке нарушения ПРД или после превышения определенного числа разрешенных ошибок;

— работа субъекта НСД прекращается, а информация о несанкционированном действии поступает администратору АС и подключает к работе специальную программу работы с нарушителем, которая имитирует работу АС и позволяет администрации сети локализовать место попытки НСД.

Реализация системы разграничения доступа может осуществляться как программными, так и аппаратными методами или их сочетанием. В последнее время аппаратные методы защиты информации от НСД интенсивно развиваются благодаря тому, что: во-первых, интенсивно развивается элементная база, во-вторых, стоимость аппаратных средств постоянно снижается и, наконец, в-третьих, аппаратная реализация защиты эффективнее по быстродействию, чем программная.

**ЛИТЕРАТУРА**

1. Ярочкин В.И. Информационная безопасность: Учеб. для ВУЗов. Изд. 2. Минск: Академический проект, 2005. – 544 с.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие для подготовки экспертов системы Гостехкомиссии России. М.: Горячая линия - Телеком, 2005. – 416 с.
3. Деднев М.А. Защита информации в банковском деле и электронном бизнесе. М.: Кудиц-образ, 2004. – 512 с.
4. Конеев И.Р. Информационная безопасность предприятия. СПб.: БХВ‑Петербург, 2003. – 752 с.