УДК 002:004:056

ОСНОВЫ КЛАССИФИКАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ИЗМЕРИТЕЛЬНЫХ СИСТЕМ УДАЛЕННОЙ ОБРАБОТКИ ДАННЫХ

К.П. КУРЕЙЧИК, А.А. ТРУШКЕВИЧ

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6, Минск, 220013, Беларусь

Поступила в редакцию 26 апреля 2011

Даны определения основных терминов, относящихся к вопросам информационной безопасности, перечислены условия безопасности информационной системы, приведена схема общей классификации угроз информационной безопасности. В предлагаемой классификационной схеме угрозы информационной безопасности разделены на угрозы, характерные для программного обеспечения, направленные на систему коммуникаций и угрозы, касающиеся аппаратной части информационной системы. Угрозы, относящиеся к каждой из перечисленных категорий, разделены на группы по характерным признакам, сопровождены описаниями и примерами.

Ключевые слова: информационная безопасность, угроза, конфиденциальность, целостность, доступность.

Введение

Удаленная обработка различных по своей природе данных и управление технологическими процессами основано на использовании информационно-измерительных систем, архитектура которых включает аппаратную, программную и коммуникационную составляющие. В связи с этим одним из самых актуальных вопросов правильного функционирования является вопрос обеспечения информационной безопасности данных систем.

В современной классификации под информационной безопасностью понимается состояние защищенности информационной системы, при котором обеспечивается ее нормальное функционирование и развитие [1, 2].

В безопасной информационной системе должны выполняться условия доступности, целостности и конфиденциальности информации. Доступность – возможность за приемлемое для пользователя время и в требуемом объеме получить регламентированную информационную услугу [2]. Целостность – актуальность, корректность и непротиворечивость информации, ее защищенность от разрушения и искажения [1]. Конфиденциальность – защита от несанкционированного доступа, разграничение доступа к информации в соответствии с правами пользователя [2].

Возможность нарушения перечисленных условий информационной безопасности обусловлено так называемыми уязвимостями в информационной системе. Уязвимостью называется недостаток системы, позволяющий нарушить одно или несколько условий безопасности [2]. Потенциальная возможность нарушения одного или нескольких условий безопасности информационной системы называется угрозой [2]. Попытку реализации угрозы принято называть атакой [2]. В соответствии с характером действия, угрозы подразделяются на угрозы доступности, угрозы целостности и угрозы конфиденциальности информации.

Окно опасности – промежуток времени от момента, когда появляется возможность воспользоваться уязвимостью до ликвидации такой возможности [2].

Источником угрозы называется объект или процесс, предпринимающий атаку безопасности информационной системы.

Часть атак на безопасность информационной системы может осуществляться с помощью вредоносного программного обеспечения.

Вредоносное программное обеспечение (ВПО) – программа либо программный комплекс, созданный с целью организации окна опасности на целевой информационной системе. Исходя из определения, программы мониторинга ресурсов и удаленного администрирования не являются ВПО, но могут использоваться злоумышленником для атаки информационных систем.

По структурной ориентированности различают угрозы, характерные для аппаратной части, программного обеспечения или системы коммуникации.

Классификация угроз безопасности информации

Согласно условию безопасности информации, на нарушение которого направлена угроза, разделяют угрозы доступности, целостности и конфиденциальности информации. Дополняя таблицу угроз [3–8], можно предложить классификационную схему угроз информационной безопасности (см. рис. 1), согласно которой можно выделить угрозы, характерные для ПО; угрозы, характерные для системы коммуникаций и угрозы, связанные с аппаратной частью информационной системы.

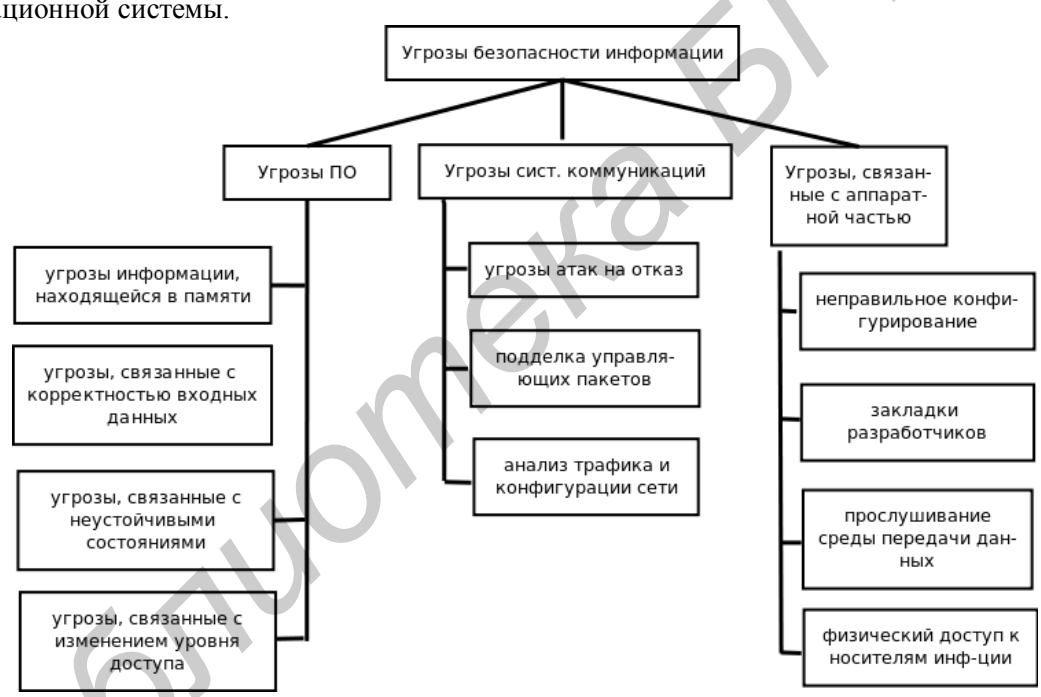

Рис. 1. Классификация угроз безопасности информации в информационных системах

Угрозы, характерные для программного обеспечения информационной системы

К угрозам данного класса относятся *угрозы, направленные на информацию, находящуюся в памяти.*

Переполнение буфера – явление, когда программа начинает записывать данные за пределами выделенного буфера, тем самым затирая данные за или перед границами выделенного буфера [3]. Нарушаются условия целостности информации, доступности (из-за возможности отказа программы или системы вследствие критической ошибки, вызванной затиранием информации, важной для обеспечения работоспособности), конфиденциальности (учитывая то, что языки высокого уровня используют механизм стекового кадра, размещая данные программы вместе с управляющими данными в стеке, злоумышленник может подменить точку возврата из подпрограммы и выполнить произвольный код [3]). Переполнение буфера обычно возни-

кает из-за неправильной работы с данными, полученными извне, и с памятью, при отсутствии жесткой защиты со стороны подсистемы программирования (компилятор или интерпретатор) или операционной системы [3].

«*Висящие указатели*» – явление, характерное для объектно-ориентированного программирования, представляющее собой ссылку (указатель) на объект, который был удален. Оперируя такой ссылкой, злоумышленник получает возможность обращения к участку памяти, которую занимал объект. Возможно нарушение условий целостности (т.к. освобожденная от объекта область памяти может быть выделена другим данным программы, которые могут быть перезаписаны злоумышленником), доступности (обращение к памяти, на которую указывает высящая ссылка, может вызвать завершение по ошибке или остановку системы).

Угрозы, связанные с корректностью входных данных.

Ошибка форматирующей строки, встречающаяся в программах, использующих вывод с помощью форматирующих строк, формируемых пользователем при отсутствии проверки вводимых параметров. Манипулируя параметрами форматирующей строки, злоумышленник может нарушить условия конфиденциальности (просмотр произвольного участка памяти), целостности и доступности (изменить произвольные данные, в т.ч. адреса возврата на стеке, передавая таким образом управление произвольному коду, размещенному в памяти, что может вызвать отказ системы или ее некорректную работу).

Угроза манипулирования метасимволами командной оболочки, характерная для систем, в которых не фильтруемые входные данные служат параметрами команды, предназначенной для выполнения командной оболочкой. Позволяет выполнять произвольные команды, поддерживаемые командной оболочкой. Спектр нарушаемых условий информационной безопасности зависит от возможностей командной оболочки. Обычно – нарушение конфиденциальности, целостности.

Угроза внедрения в запросы. Разновидностью данной угрозы является SQL-инъекция, характерная для баз данных, формирующих запросы из параметров, задаваемых пользователем без соответствующей проверки. Данный метод основан на внедрении в запрос произвольных команд (в частности SQL-кода). Возможно нарушение условий конфиденциальности (возможность запроса произвольных данных из базы) и целостности (возможность изменения произвольных данных в базе).

Открытый доступ к системным областям, встречающийся в системах с недостаточным контролем прав доступа к системным областям для приложений. Позволяет пользователю получить доступ к критическим для работоспособности системы областям. Возможно нарушение условий доступности (в случае вывода из строя программного обеспечения системы), целостности системного программного обеспечения. Может являться промежуточной стадией для реализации угрозы конфиденциальности.

Угроза манипуляций с пользовательскими скриптами, характерная для веб-ориентированных систем, в которых имеется возможность установки на сервере скриптов пользователя, выполняемых в клиентских программах других пользователей, подключающихся к данному серверу. Учитывая то, что набор операции, который может выполняться таким скриптом, зависит от возможностей, заложенных в клиентскую программу, могут быть нарушены условия целостности, доступности и конфиденциальности в пользовательской системе.

Угрозы, связанные с неустойчивыми состояниями (гонки).

Ошибки времени проверки ко времени использования, характерные для систем, в которых проверки контроля доступа не являются атомарными с защищаемыми действиями, что позволяет обойти контроль доступа [9]. Например, в системах, поддерживающих многопоточную обработку, программным обеспечением злоумышленника на вход модуля проверки посылается безобидный код, который проходит проверку и непосредственно перед исполнением заменяется на вредоносный.

Возможно нарушение целостности, доступности, конфиденциальности в зависимости от типа вредоносного кода.

Гонки файлов-семафоров, характерные для многозадачных систем, выполняющих синхронизацию по созданию специальных файлов-семафоров во временных каталогах. Злоумышленник может уничтожать либо изменять такие файлы и таким образом влиять на работу программного обеспечения атакуемой информационной системы. Например, сигналом для завер-

шения программы пользователя является наличие файла-семафора /tmp/stop.tmp. Создав данный файл, злоумышленник может вызвать завершение пользовательской программы в произвольный момент времени. При реализации данной угрозы возможно нарушение условий целостности и доступности.

Угрозы, связанные с изменением уровня доступа.

Эскалация привилегий, основанная на получении доступа к ресурсам, обычно недоступным для пользователя и приложений. Данная угроза характерна для операционных систем. Примером может служить прорыв в нулевое кольцо защиты в операционных системах Windows 9x – Windows XP методом установки своего callgate в таблицу GDT [10].

Результатом эскалации привилегий является выполнение действий в контексте другой учетной записи (системы, суперпользователя) либо более низкого кольца защиты. Угроза в случае реализации нарушает условия целостности, конфиденциальности, доступности.

Угроза атаки с помощью символических ссылок, основывающаяся на использовании возможности обращения к файлу через символическую ссылку.

Частным случаем реализации угрозы данного типа в Unix-подобных операционных системах является создание символических ссылок на системные файлы во временных каталогах. Если в системе используется скрипт для автоматической чистки временных каталогов, выполняющийся с привилегиями суперпользователя вида:

```
#!/bin/bash
DATE=`date+%s`
rm-f/tmp/backup.etc.$DATE.tgz
tar -cz /etc > /tmp/backup.etc.$DATE.tgz
. . .
```

то злоумышленник может создать множество символических ссылок вида /tmp/backup.etc.$DATE.tgz, указывающих на файл /etc/passwd. Первый запуск приведенного выше скрипта разрушает один из важнейших файлов системы. Если скрипт запускается хотя бы один раз в сутки, то достаточно создать 86400 ссылок, чтобы уничтожить систему со 100%-ой вероятностью [4]. При реализации данной угрозы нарушаются условия целостности и доступности.

Угрозы, характерные для системы коммуникации

К данному классу угроз информационной безопасности можно отнести *возможность проведения атак на отказ в обслуживании*, следующими разновидностями которой являются:

- *простая атака на отказ* (DoS, Denial of Service), являющаяся одним из самых распространенных видов атак в сети Интернет. Заключается в том, что атакуемой системе отправляются запросы, число которых превышает ее способность к обработке либо является критическим для данной пропускной способности канала. В результате атаки нарушается условие доступности.

В настоящее время известны пять видов DoS-атак: Smurf (ping-запросы ICMP (Internet Control Message Protocol) по адресу направленной широковещательной рассылки. Используемый в пакетах этого запроса фальшивый адрес источника в результате оказывается мишенью атаки. Системы, получившие направленный широковещательный ping-запрос, отвечают на него и «затапливают» сеть, в которой находится сервер-мишень), ICMP flood (атака, аналогичная Smurf, только без усиления, создаваемого запросами по направленному широковещательному адресу), UDP flood (отправка на адрес системы-мишени множества пакетов UDP (User Datagram Protocol), что приводит к «связыванию» сетевых ресурсов), TCP flood (отправка на адрес системы-мишени множества TCP-пакетов, что также приводит к «связыванию» сетевых ресурсов), TCP SYN flood (при проведении такого рода атаки выдается большое количество запросов на инициализацию TCP-соединений с узлом-мишенью, которому, в результате, приходится расходовать все свои ресурсы на то, чтобы отслеживать эти частично открытые соединения) [5];

- *распределенная атака на отказ* (DDoS, Distributed Denial of Service), являющаяся дальнейшим развитием DoS-атак. Характерным для нее является то, что целевая система атакуется большим количеством рабочих станций. Самым распространенным способом реализации

атаки данного типа является использование ботнета. В этом случае пользователи компьютеров, с которых направляются ложные запросы, могут даже не подозревать о том, что их машина используется хакерами. Программы, установленные злоумышленниками на этих компьютерах, принято называть «зомби». Известно множество путей «зомбирования» компьютеров – от проникновения в незащищенные сети до использования вредоносного программного обеспечения [6].

При реализации DDoS атаки происходит нарушение условия доступности информационной системы. Чаще всего злоумышленники при проведении DDoS-атак используют трехуровневую архитектуру, которую называют «кластер DDoS». Такая иерархическая структура содержит: управляющую консоль (их может быть несколько), т.е. именно тот компьютер, с которого злоумышленник подает сигнал о начале атаки; главные компьютеры – те машины, которые получают сигнал об атаке с управляющей консоли и передают его агентам – «зомби» (на одну управляющую консоль в зависимости от масштабности атаки может приходиться до нескольких сотен главных компьютеров); агенты – непосредственно сами «зомбированные» компьютеры, своими запросами атакующие узел-мишень [6].

Подделка пакетов управляющих сетевых устройств. Разновидностями данного вида угроз являются:

- *подмена доверенного объекта сети,* характерная для распределенных информационных систем с нестойкими алгоритмами идентификации распределенных объектов. Заключается в подделке идентификационных данных и передаче по каналу связи сообщений от произвольного объекта распределенной системы. Для адресации сетевых сообщений используется система уникальных адресов (на канальном уровне модели OSI – физический адрес сетевого адаптера, на сетевом уровне (для стека TCP/IP) – IP-адрес). В простейшем случае для идентификации распределенных объектов сети используются сетевые адреса, что недопустимо с точки зрения информационной безопасности, так как адрес может быть подделан злоумышленником [7]. Это касается также систем, использующих слабо защищенные протоколы идентификации и аутентификации. Данный тип угрозы нарушает условия целостности, доступности (в том случае, если злоумышленник подделает системные сообщения от управляющих объектов распределенной системы, он будет иметь возможность нарушить конфигурацию системы), конфиденциальности (злоумышленник может инициировать сеанс передачи данных с произвольным объектом распределенной системы от имени доверенного объекта);

- *навязывание ложного маршрута.* Реализация данной типовой удаленной атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации. Цель атаки состоит в том, чтобы изменить исходную маршрутизацию на объекте распределенной информационной системы так, чтобы новый маршрут проходил через ложный объект – хост атакующего. Для изменения маршрутизации атакующему необходимо послать по сети определенные данными протоколами управления сетью специальные служебные сообщения от имени сетевых управляющих устройств (например, маршрутизаторов). В результате успешного изменения маршрута атакующий получит полный контроль над потоком информации, которой обмениваются два объекта распределенной информационной системы, и атака перейдет во вторую стадию, связанную с приемом, анализом и передачей сообщений, получаемых от дезинформированных объектов компьютерной сети [7]. Данная атака нарушает условия целостности и конфиденциальности;

- *угроза атаки «человек посередине»* (Man in the middle, MitM-атака) означающая, ситуацию, когда злоумышленник может просматривать и модифицировать по своему усмотрению данные, которыми обмениваются два абонента. Для реализации данного типа атаки злоумышленнику должны быть известны параметры сеанса связи и адреса абонентов. Предположим, что абоненту А необходимо передать некоторую информацию абоненту В. Злоумышленник С перед началом сеанса связи идентифицирует себя абоненту А как В, а абоненту В как А. Таким образом, абонент А передает информацию С, полагая, что он передал ее абоненту В. Злоумышленник копирует либо изменяет полученную информацию и передает ее абоненту В [11]. Данная атака нарушает условия целостности и конфиденциальности информации.

Угрозы, связанные с анализом сетевого трафика и конфигурации сети:

- *угроза «Анализ сетевого трафика»* («сниффинг»), подразумевающая перехват и анализ злоумышленником информации, предназначенной другим абонентам. Во время «сниффин-

га» коммуникационное оборудование злоумышленника переводится в режим прослушивания, что позволяет просматривать транзитную информацию. Данный тип угрозы особенно актуален для беспроводных (Wi-Fi) сетей.

Разновидностью данной угрозы является активное прослушивание, заключающееся в атаке на канальном (подмена MAC-адреса), или сетевом (подмена IP) уровне, которая переводит трафик, предназначенный атакуемой системе, на систему злоумышленника, а затем возвращает его по назначению.

Еще одной разновидностью данной угрозы является выявление паролей по сети. В этом случае перехваченный трафик анализируется на наличие паролей в открытом виде (характерно для HTTP-сессий) либо в зашифрованном виде для их последующего восстановления. Анализ сетевого трафика приводит к нарушению условия конфиденциальности информации.

Угроза сканирования, реализуемая путем попыток последовательного подключения к сетевым портам атакуемой системы, что позволяет выявить активные сервисы. Данная информация может быть использована для поиска уязвимостей в сетевом программном обеспечении атакуемой системы. Технически процесс сканирования может быть осуществлен следующим образом. Для обнаружения открытого TCP-порта на атакуемой системе злоумышленник пытается установить соединение с этим портом методом посылки на него TCP SYN запроса. Если приходит ответ TCP SYN ACK, то порт открыт и TCP-угрозы аппаратной части соединение будет создано, если же по истечении некоторого времени ответ не получен, то это означает, что порт закрыт либо сканируемая система недоступна. После установления TCP-соединения между сканируемой системой и злоумышленником производится обмен командами для установления соединения на прикладном уровне, что в дальнейшем позволит идентифицировать приложение, обслуживающее данный TCP-порт приложение [7].

Данный тип угрозы формально не нарушает условий безопасности информационной системы, однако может являться подготовительным этапом для последующей атаки.

Угрозы, характерные для аппаратной части

К данному классу угроз относятся следующие.

Угроза неправильного конфигурирования аппаратных средств. Данный тип угрозы связан с предоставляемой низкоуровневым программным обеспечением (Firm Ware) возможностью конфигурирования аппаратных средств информационной системы. При недостаточной защищенности средств конфигурирования и отсутствии проверок на установку некорректных параметров аппаратная часть может быть настроена на неправильную работу, что может вызвать отказ аппаратных средств или их физическое повреждение. Примером может служить возможность «разгона» (т.е. задания более высоких, чем регламентированные тактовой частоты и других параметров), поддерживаемая модулем конфигурирования BIOS материнских плат персональных компьютеров.

Реализация данной угрозы приводит к нарушению условий доступности и целостности (в случае нарушения нормальной работы системы ввода-вывода) информации. Неправильное конфигурирование устройств управления коммуникацией (например, маршрутизаторов) может привести к нарушению условия конфиденциальности информации.

Угроза несанкционированного использования закладок разработчиков характерна для аппаратных устройств, в низкоуровневое программное обеспечение которых заложена возможность обхода процедуры аутентификации для получения доступа к инженерным функциям. Примером может служить наличие универсальных паролей для доступа к конфигурационному модулю материнских плат с некоторыми версиями BIOS. В случае использования информации по закладкам разработчиков злоумышленником могут быть нарушены условия целостности, доступности и конфиденциальности информации (в зависимости от возможностей заложенных инженерных функций).

Угроза аппаратного прослушивания среды передачи данных. Данная угроза характерна для распределенных систем, не использующих криптографической защиты передаваемой информации либо использующих алгоритмы шифрования с недостаточной криптостойкостью. При реализации угрозы злоумышленник производит физическое подключение к среде передачи данных либо осуществляет прослушивание среды передачи данных (для беспроводных се-

тей), что дает возможность перехвата сообщений, которыми обмениваются адресаты. Разновидностью данной угрозы является утечка информации по техническим каналам (за счет побочных электромагнитных излучений и наводок, высокочастотного навязывания в волоконно-оптических линиях).

Данный тип угрозы нарушает условия целостности и конфиденциальности.

Угроза физического доступа к носителям информации актуальна в том случае, когда информация хранится на носителях (например, на жестком диске) в открытом (незашифрованном виде). Получив прямой доступ к носителю, злоумышленник может скопировать, изменить либо уничтожить хранящуюся на нем информацию. Реализация угрозы данного типа нарушает условия целостности, доступности (при удалении информации) и конфиденциальности.

Заключение

Таким образом, развитая в данной работе классификация угроз информационной безопасности информационно-измерительных систем обработки удаленных данных дает возможность предпринимать меры по обеспечению их нормальной работы за счет разработки архитектуры и программного кода на разных уровнях программного и аппаратного плана.

BASICS CLASSIFICATION OF INFORMATION SECURITY THREATS IN REMOTE MEASUREMENT DATA PROCESSING SYSTEMS

K.P. KUREJCHIK, A.A. TRUSHKEVICH

Abstract

The article provides definitions of basic terms related to information security issues, conditions of the information system security are listed and a general classification scheme of information security threats is included.

In proposed classification scheme of information security threats all threats are divided on specific to software, communication system and threats, related to hardware of information system.

Threats related to each of the listed above categories are divided into groups according to characteristic features, accompanied by descriptions and examples.

Литература

1. *Ишмухаметов Ш.Т.* [Электронный ресурс] Режим доступа: http://www.ksu.ru/f9/bin_files/metod_tzis
2. *Галатенко В.А.* [Электронный ресурс] Режим доступа: http://www.intuit.ru/department/security
3. *Яремчук С.А.* [Электронный ресурс] Режим доступа: http://www.mirandaim.info/protectionspc/protection
4. [Электронный ресурс] Режим доступа: http://forum.artofhack.kz/index.php?showtopic=1881
5. *Лавникевич Д.И.* [Электронный ресурс] Режим доступа: http://web-support.ru/net-security/sec_18.shtml
6. *Малярчук В.И.* [Электронный ресурс] Режим доступа: http://www.compdoc.ru/secur/xacer/
7. *Медведовский И.Д., Семьянов П.В., Платонов В.В.* Атака через Internet. М., 2003.
8. *Дегтярев Д.А.* [Электронный ресурс] Режим доступа: http://wiki.auditory.ru
9. *Роберт Уотсон* [Электронный ресурс] Режим доступа: http://hidemefirst.com/news/
10. [Электронный ресурс] Режим доступа: http://www.codeproject.com/KB/threads
11. *Кондураке В.П.* [Электронный ресурс] Режим доступа: http://www.securrity.ru/terms