УДК 004.056

А. А. Муханова [1], **А. В. Ревнивых** [2, 3], **А. М. Федотов** [3, 4]

[1] Евразийский национальный университет им. Л. Н. Гумилева
ул. Мунайтпасова, 5, Астана, 010008, Казахстан

[2] Тюменский государственный нефтегазовый университет
ул. Володарского, 38, Тюмень,605000, Россия

[3] Новосибирский государственный университет
ул. Пирогова, 2, Новосибирск, 630090, Россия

[4] Институт вычислительных технологий СО РАН
пр. Акад. Лаврентьева, 6, Новосибирск, 630090, Россия

E-mail: ayagoz198302@mail.ru, alexchr@mail.ru, fedotov@nsu.ru

КЛАССИФИКАЦИЯ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КОРПОРАТИВНЫХ СИСТЕМАХ *

Работа посвящена описанию и анализу угроз и уязвимостей информационной безопасности в корпоративных системах. Решается задача классификации угроз и уязвимостей в соответствии с эталонной моделью взаимодействия открытых систем (RM ISO/OSI). В качестве примеров анализируются сетевые атаки на уровень, на котором реализуется угроза, использующая уязвимости протоколов сетевого взаимодействия.

Ключевые слова: информационная безопасность, классификация угроз, классификация уязвимостей, доступ к информации, распределенные информационные ресурсы.

Введение

Повсеместное распространение информационных систем (ИС) и неоправданно высокий коэффициент доверия к ним со стороны пользователей заставляют задумываться о рисках, которые связаны с таким обширным использованием ИС. Немаловажным аспектом является сетевое взаимодействие узлов распределенных ИС, а также разрозненных ИС. В рамках такого взаимодействия по сети передаются данные, идентификационные атрибуты и управляющие команды.

В данной работе предлагается классификация сетевых атак в соответствии с эталонной моделью взаимодействия открытых систем (RM ISO/OSI). Проведен анализ возможности сетевых атак, использующих уязвимости протоколов сетевого взаимодействия.

Потенциальная возможность взаимодействия с ИС, хранящими и обрабатывающими данные, в том числе стратегические и конфиденциальные, появилась у множества пользователей, среди которых неизбежно найдутся и злоумышленники. Кроме того, в результате существенной величины, сложности и гетерогенности современных распределенных ИС их надежность функционирования может оказаться под угрозой и без постороннего вмешательства злоумыш-

* Работа выполнена при финансовой поддержке Министерства образования и науки Российской Федерации (грант № 07.514.11.4130), а также при частичной поддержке РФФИ (проект № 12-07-00472).

Муханова А. А., Ревнивых А. В. , Федотов А. М. Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 2. С. 55–72.

ISSN 1818-7900. Вестник НГУ. Серия: Информационные технологии. 2013. Том 11, выпуск 2

ленников, а вследствие сугубо внутренних факторов или внешнего воздействия непредусмотренных природных катаклизмов.

Под информационной безопасностью (ИБ) понимается состояние защищенности информационных ресурсов (или ИС) и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, связанных с нарушением одного или нескольких критериев ИБ (конфиденциальность, доступность, актуальность / целостность) [1]. Нарушения ИБ обычно чреваты нанесением ущерба владельцам или пользователям информационных ресурсов [2].

В особой защите нуждаются такие привлекательные для злоумышленников элементы сетей, как серверы и активное сетевое оборудование. Первые – как концентраторы больших объемов информации, вторые – как элементы, в которых осуществляется преобразование данных (возможно через открытую, незашифрованную форму представления). При этом во многих случаях получить доступ к серверам и / или сетевому оборудованию организации злоумышленникам удается, именно предварительно получив доступ к рабочим станциям, которые подключены к тому же сегменту сети, что и целевые компоненты инфраструктуры.

Рассмотрим основные термины и понятия, относящиеся к ИБ, а также их взаимосвязи.

Риск – это вероятность реализации определенной угрозы ИБ (использующей некоторые уязвимости), а также величина возможного ущерба.

Отметим, что понятие риска является следствием взаимного соотношения логической цепочки понятий «актив» – «источник угрозы» – «уязвимость» – «угроза» (действие) – «последствия» (атака) – «ущерб» (см., например, [1; 3]):

- активы – ключевые компоненты инфраструктуры и значимая для собственника информация, обрабатываемая в информационной системе, имеющая определенную ценность;
- источник угрозы информационной безопасности – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации;
- уязвимость – это присущие объекту информатизации свойства, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные особенностями процесса функционирования объекта информатизации, свойствами архитектуры автоматизированной системы, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, а также условиями эксплуатации;
- угроза (действие) – это возможная опасность (потенциальная или реально существующая) совершения какого-либо деяния (действия или бездействия), направленного против объекта защиты (информационных ресурсов), наносящего ущерб собственнику, владельцу или пользователю, проявляющегося в опасности искажения, потери и утечки информации;
- последствия (атака) – это возможные последствия реализации угрозы (возможные действия) при взаимодействии источника угрозы через имеющиеся уязвимости;
- ущерб – затраты на восстановление системы в работоспособное состояние после возможного инцидента ИБ, а также на восстановление искаженной, утерянной информации или же нейтрализация последствий утечки конфиденциальной информации [3].

Уязвимости

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, особенностями протоколов обмена и интерфейсов, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения.

Источники угроз используют уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны действия источников угроз по активизации тех или иных уязвимостей, не связанные со злым умыслом.

Наиболее распространенными причинами возникновения уязвимостей являются:

- ошибки при проектировании, разработке и эксплуатации программно-аппаратного обеспечения;

- преднамеренные действия по внесению уязвимостей в ходе проектирования, разработки и эксплуатации программно-аппаратного обеспечения;
- неправильные настройки оборудования и ПО, недопустимое изменение режимов работы устройств и программ;
- несанкционированное внедрение и использование неучтенных программ с последующим необоснованным расходованием ресурсов (например, загрузка процессора, захват оперативной памяти, памяти на внешних носителях);
- внедрение вредоносных программ, создающих уязвимости в программном и программно-аппаратном обеспечении;
- несанкционированные неумышленные действия пользователей;
- сбои в работе оборудования и ПО (вызванные сбоями в электропитании, выходом из строя аппаратных элементов в результате старения и снижения надежности, внешними воздействиями электромагнитных полей технических устройств и др.).

Каждой угрозе могут быть сопоставлены различные уязвимости, устранение или существенное ослабление которых влияет на вероятность реализации угроз ИБ.

Общая классификация уязвимостей. Уязвимости ИБ можно разделить на объективные, субъективные и случайные.

Объективные уязвимости основываются на особенностях построения и технических характеристиках оборудования и ПО, применяемых на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз ИБ.

Субъективные уязвимости зависят от действий субъектов (например, разработчиков оборудования и ПО, системных администраторов и пользователей организации). Уязвимости данного типа в большинстве случаев устраняются организационными и программно-аппаратными методами.

Случайные уязвимости обуславливаются особенностями окружающей объект информатизации среды и непредвиденными обстоятельствами. Многие из факторов, обеспечивающих наличие таких уязвимостей ИС, в целом предсказуемы, но полное их устранение либо невозможно, либо затруднено и достижимо только при проведении целого комплекса организационных и инженерно-технических мероприятий.

Представим уязвимости в виде дерева рубрикатора.

0. Уязвимости.
0.1. Объективные уязвимости.
0.1.1. Сопутствующие техническим средствам излучения.
0.1.1.1. Электромагнитные (побочные излучения элементов технических средств, кабельных линий технических средств, излучения на частотах работы генераторов, на частотах самовозбуждения усилителей).
0.1.1.2. Электрические (наводки электромагнитных излучений на линии и проводники, просачивание сигналов в цепи электропитания, в цепи заземления, неравномерность потребления тока электропитания).
0.1.1.3. Звуковые (акустические, виброакустические).
0.1.2. Активизируемые.
0.1.2.1. Аппаратные закладки (устанавливаемые в линии связи, сети электропитания, помещения, аппаратное обеспечение и технические средства).
0.1.2.2. Программные закладки (вредоносные программы, технологические выходы из программ, нелегальные копии ПО).
0.1.2.3. Определяемые особенностями элементов.
0.1.2.4. Наличие элементов, работа которых связана с электроакустическими преобразованиями (телефонные аппараты, громкоговорители и микрофоны, катушки индуктивности, дроссели, трансформаторы и пр.).
0.1.2.5. Потенциальные уязвимости оборудования и ПО (например, сложность и несовершенство кода ПО, создающие предпосылки для успешных атак на отказ в обслуживании или «срыв» стека).

0.1.2.6. Наличие элементов, подверженных воздействию электромагнитного поля (магнитные носители, микросхемы, нелинейные элементы, потенциально подверженные высокочастотному навязыванию).

0.1.3. Определяемые особенностями защищаемого объекта.

0.1.3.1. Местоположение объекта (отсутствие контролируемой зоны, наличие прямой видимости объектов, удаленных и мобильных элементов объекта, вибрирующих отражающих поверхностей).

0.1.3.2. Организация каналов обмена информацией (использование радиоканалов, глобальных информационных сетей, арендуемых каналов, кабельных соединений, потенциально доступных снаружи охраняемого периметра).

0.2. Субъективные уязвимости.

0.2.1. Ошибки.

0.2.1.1. При разработке оборудования и ПО (например, логические и синтаксические ошибки при разработке алгоритмов и их реализации в ПО).

0.2.1.2. При подготовке и использовании ПО (при загрузке и инсталляции ПО, дальнейшей эксплуатации ПО, вводе данных).

0.2.1.3. При управлении сложными системами (при использовании возможностей самообучения систем, настройке сервисов систем, организации управления потоками информации).

0.2.1.4. При эксплуатации технических средств (при включении / выключении технических средств, использовании технических средств охраны, использовании средств обмена информацией).

0.2.2. Возможность нарушений.

0.2.2.1. Требований руководящих документов.

0.2.2.2. Установленных правил документирования событий.

0.2.2.3. Режима охраны и защиты (доступа на объект, доступа к техническим средствам).

0.2.2.4. Режима эксплуатации технических средств (энергообеспечения, жизнеобеспечения).

0.2.2.5. Режима использования информации (обработки и обмена информацией, хранения и уничтожения носителей информации, уничтожения производственных отходов и брака).

0.2.2.6. Режима конфиденциальности (сотрудниками в нерабочее время, уволенными сотрудниками).

0.3. Случайные уязвимости.

0.3.1. Потенциальная возможность сбоев и отказов.

0.3.1.1. Неисправности оборудования и технических средств (обрабатывающих информацию, обеспечивающих работоспособность средств обработки информации, обеспечивающих охрану и контроль доступа).

0.3.1.2. Старение и размагничивание носителей информации (дискет и съемных носителей, жестких дисков, элементов микросхем, кабелей и соединительных линий).

0.3.1.3. Неисправности ПО (ОС и СУБД, прикладных программ, сервисных программ, антивирусных программ и т. п.).

0.3.2. Возможность нарушения условий эксплуатации.

0.3.2.1. Нарушения обеспечивающих коммуникаций (электро-, водо-, газо-, теплоснабжения, канализации, кондиционирования и вентиляции).

0.3.2.2. Разрушение строительных и ограждающих конструкций (внешних ограждений территорий, стен и перекрытий зданий, корпусов технологического оборудования).

Уязвимости оборудования. Аппаратное обеспечение ИС подвержено уязвимостям всех трех типов. В целом уязвимость оборудования объясняется следующими факторами, представленными ниже в виде дерева рубрикатора.

0. Факторы, обуславливающие уязвимость оборудования.
0.1. Зависимость от физической среды эксплуатации.
0.1.1. Подверженность оборудования влажности, пыли, загрязнению.
0.1.2. Зависимость от температуры (плюс подверженность действию перепада температур) и давления.
0.1.3. Необходимость защиты от действия прямых солнечных лучей.
0.1.4. Подверженность оборудования вибрационным и ударным нагрузкам.
0.1.5. Необходимость электропитания (плюс подверженность флуктуациями электропитания).
0.2. Необходимость физической защиты от несанкционированного доступа.
0.2.1. Необходимость размещения инфраструктурного и клиентского оборудования в помещениях с ограниченным доступом.
0.2.2. Необходимость наличия документации, регламентирующей доступ к оборудованию и ответственность за несанкционированный доступ.
0.2.3. Зависимость от правомерности и адекватности использования механизмов контроля физического доступа .
0.2.4. Беззащитность инфраструктурного и клиентского оборудования по отношению к прямому физическому воздействию.
0.3. Неизбежные износ и старение элементов оборудования.
0.4. Необходимость обслуживания оборудования.
0.4.1. Необходимость наличия документации, регламентирующей обслуживание оборудования и ответственность за нарушение требований по обслуживанию.
0.4.2. Зависимость от адекватности мер по обслуживанию оборудования (исполнения указаний регламентирующих документов).
0.5. Неизбежная вероятность поломки элементов оборудования (современные технологии проектирования и изготовления технических средств не позволяют выпускать оборудование с точно предсказуемым сроком безотказной работы).
0.6. Ошибки и недоработки при проектировании, изготовлении, доставке, подключении, вводе в эксплуатацию, эксплуатации и обслуживании оборудования.
0.7. Возможность внедрения аппаратных «закладок» в оборудование.

Уязвимости программного обеспечения. ПО также подвержено уязвимостям всех трех типов. При этом стоит различать системное и прикладное ПО.

Системным ПО будем считать ОС, инфраструктурные системы управления базами данных (СУБД), драйверы устройств и протоколы сетевого взаимодействия. В некоторых случаях к системному ПО относят также микропрограммы, записанные в памяти элементов оборудования (например, прошивки материнских плат).

Прикладное ПО – это программы, рассчитанные на непосредственное взаимодействие с пользователем и предназначенные для выполнения определенных пользовательских задач.

Общая характеристика уязвимостей системного программного обеспечения. Уязвимости системного ПО необходимо рассматривать с привязкой к архитектуре построения вычислительных систем.

При этом возможны уязвимости:

- в микропрограммах, прошивках ПЗУ, ППЗУ;
- в средствах ОС, предназначенных для управления локальными ресурсами (обеспечивающих выполнение функций управления процессами, памятью, устройствами ввода / вывода, интерфейсом с пользователем и т. п.), драйверах, утилитах;
- в средствах ОС, предназначенных для выполнения вспомогательных функций – утилитах (архивирования, дефрагментации и др.), системных обрабатывающих программах

(компиляторах, компоновщиках, отладчиках и т. п.), программах предоставления пользователю дополнительных услуг (специальных вариантах интерфейса, калькуляторах, играх и т. п.), библиотеках процедур различного назначения (библиотеках математических функций, функций ввода / вывода и т. д.);

- в средствах коммуникационного взаимодействия (сетевых средствах) ОС.

Уязвимости в микропрограммах и в средствах ОС, предназначенных для управления локальными ресурсами и вспомогательными функциями, могут представлять собой:

- функции и процедуры, изменение параметров которых определенным образом позволяет использовать их для несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др.;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т. п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации.

Сетевая модель OSI. Бурное развитие информационных технологий (ИТ) началось с конца 1950-х гг. в основном за счет «гонки вооружений» между двумя существовавшими тогда «сверхдержавами» – СССР и США. Компьютеры и начинающие появляться сети передачи данных использовались, прежде всего, для создания новых видов оружия (в первую очередь ракетного) [4]. Разнообразие созданных программных сетевых протоколов обозначило проблему их несовместимости между собой. Возможным решением представлялся всеобщий переход на единый для всех стек сетевых протоколов, по возможности учитывающий достоинства и недостатки существующих в то время вариантов. Для этой цели в конце 1970-х гг. была начата разработка базовой эталонной модели для взаимодействия ИС (Open Systems Interconnection Basic Reference Model, OSI). В модели OSI средства взаимодействия делятся на семь уровней (табл. 1). Каждый уровень имеет дело с совершенно определенным аспектом взаимодействия сетевых устройств. Модель OSI описывает только системные средства взаимодействия, не касаясь приложений конечных пользователей. Приложения реализуют свои собственные протоколы взаимодействия, обращаясь к системным средствам. При этом приложение может взять на себя функции некоторых верхних уровней модели OSI. В таком случае при необходимости межсетевого обмена оно обращается напрямую к системным средствам, выполняющим функции нижних уровней модели OSI.

Таблица 1

Уровни модели OSI

Тип данных	Уровень (Layer)	Функции
Данные	7. Прикладной (application)	Работа прикладных сервисов
	6. Представительский (presentation)	Представление и шифрование данных
	5. Сеансовый (session)	Управление сеансом связи
Сегменты	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежность
Пакеты	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

В соответствии со стандартами модели OSI протоколы должны взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и / или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже – вертикальными. Протоколы в модели OSI не могут выполнять функций протоколов другого уровня. Отметим, что данное правило не выполняется в альтернативных вариантах моделей межсетевого взаимодействия.

В настоящее время основным используемым стеком протоколов является TCP/IP (Transmission Control Protocol / Internet Protocol), разработанный еще до принятия OSI в качестве эталонной модели и вне связи с ней. Этим объясняется неполное соответствие стека TCP/IP уровням модели OSI и некоторые противоречия между этими стандартами [5].

Стек протоколов TCP/IP. Общепринятым программным сетевым стеком протоколов, используемым в современных сетях передачи данных, стал TCP/IP. Данный стек изначально был разработан по инициативе Министерства обороны США в конце 1970-х гг. и предназначался для связи экспериментальной сети ARPAnet с другими сателлитными сетями. Он представляет набор общих протоколов для разрозненных вычислительных сред [6].

Большой вклад в развитие стека TCP/IP внес Калифорнийский университет в Беркли (University of California, Berkeley), реализовав данный набор протоколов в своей версии ОС – UNIX, которая оазалась весьма востребованной на развивающемся рынке ИТ, и ее широкое распространение привело к господству стека протоколов TCP/IP в области межсетевого взаимодействия. Именно на основе данной технологии заработала развивающаяся глобальная компьютерная сеть Internet.

В 1986 г. создан международный Инженерный совет Интернета (Internet Engineering Task Force, IETF), который по сей день вносит наиболее существенный вклад в развитие архитектуры и протоколов Internet. Содержание технических спецификаций и стандартов публикуется в виде «Рабочих предложений» (Request for Comments, RFC), по сути являющихся серией пронумерованных информационных документов, выпускаемых в настоящее время под эгидой IETF.

Как уже упоминалось, соответствие уровней стека TCP/IP уровням модели OSI достаточно условно (уровни TCP/IP можно поставить в соответствие четырем верхним уровням модели OSI).

Уязвимости протоколов сетевого взаимодействия связаны с особенностями их программной реализации и обусловлены ограничениями на размеры применяемого буфера, недостатками процедуры аутентификации, отсутствием проверок правильности служебной информации и др. [3].

Краткая характеристика уязвимостей нескольких протоколов верхних уровней модели OSI (на примере стека TCP/IP) приведена в табл. 2.

В табл. 2 перечислены уязвимости нескольких протоколов стека TCP/IP, обусловленные факторами «на уровне идеи». Необходимо отметить, что у этих же протоколов имеются и другие уязвимости, которые обусловлены ошибками и недоработками в их реализации, потенциальной возможностью наличия в них «закладок», вредоносных программ и т. д. Кроме того, с течением времени ПО, в котором реализована поддержка этих протоколов, обновляется, и соответственно каждая новая версия ПО может содержать в себе новые ошибки или «закладки».

Отметим также, что существуют протоколы с поддержкой шифрования процедуры авторизации, установленной сессии и передаваемых данных (например, SFTP, SSH). При этом и такие протоколы нельзя назвать полностью безопасными в силу неизбежных ошибок в их реализации, а также неидеальной криптографической составляющей.

Для систематизации описания множества уязвимостей программных сетевых протоколов и ПО используется единая база данных (БД) уязвимостей CVE (Common Vulnerabilities and Exposures), в разработке которой принимали участие специалисты многих известных компаний и организаций, таких как MITRE, ISS, Cisco, BindView, Axent, NFR, L-3, CyberSafe, CERT, Carnegie Mellon University, Институт SANS и т. д. Эта БД постоянно пополняется и используется при разработке многочисленных программных средств анализа защищенности и, прежде всего, средств мониторинга сетей.

Таблица 2

Уязвимости отдельных протоколов стека протоколов TCP/IP (v4)

Наименование протокола	Соответствие уровню OSI	Характеристика уязвимости	Содержание нарушения безопасности информации
FTP (File Transfer Protocol) – протокол передачи файлов по сети	Прикладной, представительный, сеансовый	1. Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде). 2. Доступ по умолчанию. 3. Наличие двух открытых портов	Возможность перехвата данных учетной записи (имен зарегистрированных пользователей, паролей). Получение удаленного доступа к хостам
Telnet – протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе открытого текста (пароли пересылаются в незашифрованном виде)	Возможность перехвата данных учетной записи пользователя. Получение удаленного доступа к хостам
UDP – протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера. Отсутствие проверки доставки пакетов адресату	Возможность реализации UDP-шторма. В результате обмена пакетами происходит существенное снижение производительности сервера. Вероятность потери информации в процессе передачи
ARP – протокол преобразования IP-адреса в физический адрес	Сетевой	Аутентификация на базе открытого текста (информация пересылается в незашифрованном виде)	Возможность перехвата трафика злоумышленником
RIP – протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута	Возможность перенаправления трафика через хост злоумышленника
TCP – протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP
DNS – протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	Фальсификация ответа DNS-сервера
IGMP – протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Возможность подделки маршрута. Приводит к остановке операционных систем Win9x / WinNT
SMTP – протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса отправителя сообщения
SNMP – протокол управления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность достижения максимальной пропускной способности сети

Общая характеристика уязвимостей прикладного программного обеспечения. К прикладному ПО относятся прикладные программы общего назначения и специальные прикладные программы.

Прикладные программы общего назначения – текстовые и графические редакторы, медиапрограммы (аудио- и видеопроигрыватели, программные средства приема телевизионных программ и т. п.), системы управления базами данных, программные платформы общего пользования для разработки программных продуктов (типа «Delphi», «Visual Basic»), средства защиты информации общего пользования и т. п.

Специальные прикладные программы – это программы, которые разрабатываются в интересах решения конкретных прикладных задач в данной ИС (в том числе программные средства защиты информации, разработанные для конкретной ИС). Специальное ПО может представлять собой инфраструктурные сервисы ОС. Например, «Internet Explorer» относится к специальному прикладному ПО и при этом является неотъемлемой частью некоторых версий ОС «Windows».

В контексте предмета изучения данной работы прикладными программами также будем считать программы, работающие на прикладном уровне эталонной модели.

Уязвимости прикладного ПО могут представлять собой:

- функции и процедуры, относящиеся к разным прикладным программам и несовместимые между собой (не функционирующие в одной операционной среде) из-за конфликтов, связанных с распределением ресурсов системы;
- функции и процедуры, некоторое изменение параметров которых позволяет использовать их для проникновения в операционную среду ИС и вызова штатных функций ОС, выполнения несанкционированного доступа без обнаружения таких изменений ОС;
- фрагменты кода программ («дыры», «люки»), введенные разработчиком, позволяющие обходить процедуры идентификации, аутентификации, проверки целостности и др., предусмотренные в ОС;
- отсутствие необходимых средств защиты (аутентификации, проверки целостности, проверки форматов сообщений, блокирования несанкционированно модифицированных функций и т. п.);
- ошибки в программах (в объявлении переменных, функций и процедур, в кодах программ), которые при определенных условиях (например, при выполнении логических переходов) приводят к сбоям, в том числе к сбоям функционирования средств и систем защиты информации, к возможности несанкционированного доступа к информации.

Классификация уязвимостей программного обеспечения. В целом уязвимость ПО ИС объясняется следующими факторами, представленными ниже в виде дерева рубрикатора.

0. Факторы, обуславливающие уязвимость ПО.
0.1. Ошибки кода ПО.
0.1.1. Логические .
0.1.2. Синтаксические.
0.1.3. Ошибки уровней доступа.
0.1.3.1. Учетные записи, наделенные определенными полномочиями, введенные разработчиками в код, например, для тестирования ПО и потом забытые.
0.2. Заложенные к код уязвимости.
0.2.1. «Закладки».
0.2.2. Мануфактурные входы (отладочные входы).
0.2.3. «Дыры» (когда ошибка есть, но ПО работает).
0.2.4. «Бананы» (когда из-за ошибки ПО работать перестает).
0.2.5. Учетные записи, наделенные определенными полномочиями, введенные разработчиками в код для дальнейшего несанкционированного доступа к системам пользователей этого ПО.

0.3. Недостаток или отсутствие необходимых средств защиты (аутентификации, проверки целостности).
0.4. Внедрение вредоносных программ.
0.5. Наличие в коде ПО функций, потенциально позволяющих выполнять деструктивные действия.
0.6. Отсутствие или недостатки проверки корректности входных данных.

Угрозы

Угроза ИБ реализуется в результате образования канала реализации угроз между источником угрозы и носителем, что создает условия для нарушения одного или нескольких критериев ИБ.

Основными элементами канала реализации угроз ИБ являются:

- источник угроз ИБ – субъект, материальный объект или физическое явление, создающие угрозы;
- среда (путь) распространения информации или воздействий, в которой физическое поле, сигнал, данные или программы могут распространяться и воздействовать на защищаемые свойства (конфиденциальность, актуальность, целостность и доступность) информации;
- носитель – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Общая классификация угроз. Угрозы ИБ классифицируются в соответствии со следующими признаками:

- по источнику угроз ИБ;
- по способу реализации угроз ИБ;
- по виду нарушаемого свойства ИБ (виду несанкционированных действий, осуществляемых с информацией);
- по типу используемой уязвимости;
- по объекту воздействия;
- по виду активов, подверженным угрозам ИБ.

Классификация по источнику угроз. Носителями угроз ИБ являются источники угроз, в качестве которых могут выступать как субъекты (личность), так и объективные проявления. Причем источники угроз могут находиться как внутри защищаемой организации – внутренние источники, так и вне ее – внешние источники.

Все источники угроз ИБ можно разделить на группы: антропогенные; технические; стихийные (природные).

Антропогенные угрозы. Источниками угроз ИБ могут выступать субъекты, действия (либо бездействие) которых могут быть квалифицированы как умышленное или случайное причинение ущерба. Действия (либо бездействие) субъекта не всегда можно спрогнозировать и объективно оценить.

В качестве источника угроз можно рассматривать субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта. Субъекты (источники), действия которых могут привести к нарушению ИБ, подразделяются на как *внешние* и *внутренние*.

Внешние источники могут быть случайными или преднамеренными и иметь разный уровень квалификации. К ним относятся:

- криминальные структуры;
- потенциальные преступники и злоумышленники;
- недобросовестные партнеры;
- конкуренты (конкурирующие организации);

- представители надзорных организаций и аварийных служб;
- представители силовых структур;
- представители провайдеров услуг связи;
- в некоторых случаях – обычные пользователи ИС [7].

Внешний нарушитель потенциально может осуществлять несанкционированный доступ:

- к каналам связи, выходящим за пределы служебных помещений;
- через автоматизированные рабочие места, подключенные к сетям связи общего пользования;
- к информации с использованием специальных программных воздействий посредством вредоносных программ, алгоритмических или программных закладок;
- через элементы информационной инфраструктуры, которые в процессе своего жизненного цикла (модернизации, сопровождения, ремонта, утилизации) оказываются за пределами контролируемой зоны.

Необходимо отметить, что воздействия со стороны внешних нарушителей совершенно необязательно будут иметь преднамеренный характер. В соответствии с техническими или организационными особенностями строения ИС действия (или бездействие) внешних субъектов могут приводить к нарушениям критериев ИБ в процессе нормальной эксплуатации системы с использованием внешних интерфейсов доступа к ней. Кроме того, перечисленные выше внешние субъекты при определенных условиях могут перейти в группу внутренних (например, представители аварийных организаций и надзорных служб по служебной необходимости могут получить возможность доступа к системе через ее внутренние интерфейсы).

Внутренние субъекты (источники) могут представлять собой как высококвалифицированных специалистов в области разработки и эксплуатации ПО и технических средств (и быть знакомыми со спецификой решаемых задач, структурой, основными функциями и принципами работы программно-аппаратных средств защиты информации), так и малограмотными в области ИТ пользователями. К ним относятся:

- основной персонал;
- административно-управленческий персонал;
- вспомогательный персонал (бухгалтеры, юристы, программисты, системные администраторы);
- технический персонал (слесари, уборщики, охрана).

Необходимо учитывать также, что особую группу внутренних источников составляют лица с нарушенной психикой, а также специально внедренные и завербованные агенты. Данная группа рассматривается в составе перечисленных выше источников угроз, но методы парирования угрозам для этой группы могут иметь свои отличия.

Технические угрозы определяются технократической деятельностью человека и развитием цивилизации. Однако последствия, вызванные такой деятельностью, отчасти вышли из-под контроля человека и существуют сами по себе. Эти источники угроз более прогнозируемые, напрямую зависят от свойств техники. Данный класс источников угроз ИБ особенно актуален в современных условиях. Эксперты ожидают резкого роста числа техногенных катастроф, вызванных физическим и моральным устареванием используемых ИС и ИТ.

При этом новые поколения ИС также содержат множество уязвимостей. В первую очередь, это связано со значительно возрастающей с каждым годом сложностью и функциональностью ИС при постоянной необходимости сокращать продолжительность циклов их разработки и изготовления.

Технические средства, являющиеся источниками потенциальных угроз ИБ, также могут быть *внешними* (средства связи, сети инженерных коммуникаций (водоснабжения, канализации), транспорт) и *внутренними* (технические и программные средства обработки информации, вспомогательные средства (охраны, сигнализации, телефонии), другие технические средства, применяемые в учреждении).

Существуют угрозы, источниками которых являются несанкционированные программно-аппаратные средства. К таким угрозам можно отнести, например, внедрение в систему троянов: кейлоггеров (англ. – *keylogger*), снифферов (англ. – *sniffer*) и др. Кейлоггер – это программный продукт (модуль) или аппаратное устройство, регистрирующее нажатия клавиш на клавиатуре компьютера, а затем, как правило, отправляющее протокол нажатий на некоторый внешний ресурс, к которому имеет доступ злоумышленник. Сниффер – это программно-аппаратный комплекс, предназначенный для перехвата сетевого траффика с целью его последующего анализа. Как правило, установка кейлоггеров и снифферов производится для выявления учетных записей и механизмов аутентификации доступа к тем или иным ресурсам ИС [8].

По положению источника выделяют:

- угрозы, источник которых расположен вне контролируемой зоны. Примеры таких угроз – перехват побочных электромагнитных излучений (ПЭМИН) или перехват данных, передаваемых по каналам связи; дистанционная фото- и видеосъемка; перехват акустической информации;
- угрозы, источник которых расположен в пределах контролируемой зоны. Примерами подобных угроз могут служить применение подслушивающих устройствили хищение носителей, содержащих конфиденциальную информацию [9].

Классификация по способам реализации угроз ИБ включает следующие группы:

- утечки информации по техническим каналам;
- социальная инженерия (метод несанкционированного доступа к информации или системам хранения информации без использования технических средств, когда в качестве объекта атаки выступает не сама машина, а человек-оператор);
- специальные воздействия на ИС (в том числе внедрение вредоносных программ, эксплуатация уязвимостей программного и аппаратного обеспечения и т. д.) [10].

Существует вероятность реализации угроз ИБ путем использования протоколов межсетевого взаимодействия. При этом может обеспечиваться несанкционированный доступ к информации или реализовываться угроза отказа в обслуживании [11].

По характеру все угрозы можно разделить на пассивные и активные [12]. Пассивная угроза – это угроза, при реализации которой не оказывается непосредственное влияние на работу ИС, но могут быть нарушены установленные правила разграничения доступа к информации или сетевым ресурсам. Примером таких угроз является угроза «Анализ сетевого трафика», направленная на прослушивание каналов связи и перехват передаваемой информации.

Активная угроза – это угроза, связанная с воздействием на ресурсы ИС, при реализации которой оказывается непосредственное влияние на работу системы (изменение конфигурации, нарушение работоспособности и т. д.) с нарушением установленных правил разграничения доступа к информации или сетевым ресурсам. Примерами таких угроз являются атаки типа «PING flood», «SYN flood» и др., успешная реализация которых может закончиться для пользователей ИС отказом в обслуживании всей системой или ее частью.

Надо отметить, что в целом реализация угроз пассивного типа обычно предназначена для получения неких результатов, которые в дальнейшем позволяют с большей вероятностью успешно реализовать активные угрозы.

Реализация угрозы может быть направлена на нарушение конфиденциальности, актуальности, целостности и доступности информации (в том числе на нарушение работоспособности ИС или ее элементов). Процесс реализации угрозы в общем случае состоит из четырех этапов:

- сбор информации;
- вторжение (проникновение в операционную среду);
- осуществление несанкционированного доступа;
- ликвидация следов несанкционированного доступа (см. рисунок).

Процесс реализации угрозы с применением межсетевого взаимодействия

На этапе сбора информации нарушителя могут интересовать различные сведения об ИС, в том числе:

- о топологии сети, в которой функционирует система. При этом может исследоваться область вокруг сети (например, нарушителя могут интересовать адреса доверенных, но менее защищенных хостов);
- о типе ОС, развернутых в ИС;
- о функционирующих на хостах сервисах, версиях прикладного ПО. Определение сервисов, исполняемых на хостах, может осуществляться удаленно методом выявления «открытых портов»;
- о субъектах ИС (пользователях, администраторах), их полномочиях, морально-этических принципах и т. д.;
- о политиках, связанных с ИБ, применяемых в исследуемой организации (например, о политиках управления доступом, резервного копирования и т. п.) [7].

Указанная выше информация собирается с целью исследования наличия типовых уязвимостей в системных сервисах или особенностей в администрировании системы, которые в дальнейшем можно будет использовать на этапе вторжения.

На этапе вторжения эксплуатируются ранее выявленные типовые уязвимости и особенности администрирования системы. Успешным результатом использования уязвимостей обычно является получение процессом нарушителя привилегированного режима выполнения (доступа к привилегированному режиму выполнения командного процессора), несанкционированное внесение в систему учетной записи злоумышленника, получение списка учетных записей, существующих в системе санкционированных пользователей, или нарушение работоспособности атакуемого элемента системы.

Этот этап развития угрозы, как правило, является многофазным. К фазам процесса реализации угрозы могут относиться, например:

- установление связи с хостом, относительно которого реализуется угроза;
- выявление уязвимостей целевого хоста;
- внедрение вредоносной программы в интересах расширения прав и др.

Угрозы, реализуемые на этапе вторжения, подразделяются по уровням стека протоколов TCP/IP, поскольку формируются на сетевом, транспортном или прикладном уровне в зависимости от используемого механизма вторжения.

К типовым угрозам, реализуемым на сетевом и транспортном уровнях, относятся угрозы, направленные на:

- подмену доверенного объекта;
- создание в сети ложного маршрута;
- ложного объекта с использованием недостатков алгоритмов удаленного поиска;
- а также угрозы типа «отказ в обслуживании», основанные на IP-дефрагментации, формировании некорректных ICMP-запросов (например, атака «Ping of Death» и «Smurf») и некорректных TCP-запросов (атака «Land»), на создании «шторма» пакетов с запросами на соединение (атаки «PING flood» и «SYN flood») и др.

К типовым угрозам, реализуемым на прикладном уровне, относятся угрозы, направленные на несанкционированный запуск приложений, угрозы, реализация которых связана с внедрением программных закладок (типа «троянский конь»), с выявлением паролей доступа к ресурсам ИС и т. д.

Если реализация угрозы не принесла нарушителю наивысших прав доступа в системе, возможны попытки расширения (эскалации) этих прав до максимально возможного уровня. Для этого могут использоваться уязвимости не только сетевых сервисов, но и уязвимости системного и прикладного ПО хостов ИС, а также уязвимости применяемого оборудования.

На этапе реализации несанкционированного доступа осуществляется собственно достижение цели реализации угрозы:

- нарушение конфиденциальности (копирование, неправомерное распространение);
- нарушение актуальности и целостности (изменение, частичное удаление или подмена);
- нарушение доступности (уничтожение, блокирование).

На этом же этапе, после указанных действий, как правило, формируется так называемый «черный вход» в виде одного из сервисов (демонов), обслуживающих некоторый порт и выполняющих команды нарушителя. «Черный вход» оставляется в системе в интересах обеспечения возможности получить доступ к хосту [1]:

- даже если администратор устранит использованную для успешной реализации угрозы уязвимость;
- как можно более скрытно;
- быстро (не повторяя заново процесс реализации угрозы).

«Черный вход» позволяет нарушителю внедрить в сеть или на определенный хост вредоносную программу, например, «анализатор паролей» (password sniffer) – программу, выделяющую пользовательские идентификаторы и пароли из сетевого трафика при работе протоколов высокого уровня (ftp, telnet, rlogin и т. д.). Объектами внедрения вредоносных программ могут быть программы аутентификации и идентификации, сетевые сервисы, ядро ОС, файловая система, библиотеки и т. д.

Наконец, на этапе ликвидации следов реализации угрозы осуществляется попытка уничтожения следов действий нарушителя. При этом удаляются соответствующие записи из всех возможных журналов аудита, в том числе записи о факте сбора информации.

В настоящее время можно выделить несколько наиболее распространенных угроз, реализуемых на различных уровнях модели ISO / OSI с эксплуатацией уязвимостей протоколов сетевого взаимодействия.

---

[1] Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена заместителем директора ФСТЭК России 15 февраля 2008 г.

Анализ сетевого трафика с целью выявления полезной информации (например, администраторских или пользовательских идентификаторов и паролей к ним). Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, которые интересуют злоумышленника (например, пакеты, в которых передаются идентификатор пользователя и его пароль). В ходе реализации угрозы нарушитель изучает логику работы сети, т. е. стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. Последствиями реализации такой угрозы может быть исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей.

Такого рода атаки реализуются на канальном уровне (непосредственного внедрения в ОС компьютеров не требуется). Особенно эффективным данный вид атак стал в связи с широким внедрением оптических каналов связи: можно поставить рядом с оптическим кабелем аппарат, который будет производить съем информации без потери качества ее передачи, – с медными каналами связи это было сложнее.

Сканирование сети. Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИС и анализе ответов от них. Последствиями реализации такой угрозы могут быть определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей.

Сканирование сети производится на прикладном уровне и может осуществляться как снаружи сети, так и изнутри ее периметра (в этом случае обычно сначала захватывается управление одним из пользовательских компьютеров, находящихся внутри сети).

Угроза подбора или перехвата пароля. Цель реализации угрозы состоит в получении несанкционированного доступа путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, сканирование файлов кэша браузера и файлов виртуальной памяти ОС, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ к хосту путем последовательного подбора паролей. В случае успеха злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа. Последствия – выполнение любого деструктивного действия, связанного с получением несанкционированного доступа. Необходимо также отметить, что компрометация идентификаторов и паролей к ним гораздо чаще происходит за счет банальной социальной инженерии.

Перехват пароля может осуществляться как на канальном уровне, так и на прикладном. От перехвата пароля на прикладном уровне эффективно защищают простейшие меры предосторожности. Например, во многих системах после нескольких неудачных попыток ввода пароля учетная запись, к которой вводился неверный пароль, блокируется. Разблокировка может производиться после истечения определенного тайм-аута автоматически либо же вручную человеком, наделенным административными правами в системе.

Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа. Такая угроза эффективно реализуется в системах, где применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т. д. При реализации атаки может использоваться канальный и прикладной уровень.

Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т. п.), легально подключенный к серверу. Последствия от реализации угрозы – изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных, несанкционированный доступ к сетевым ресурсам, навязывание ложной информации.

Навязывание ложного маршрута сети. Данная угроза реализуется на канальном и прикладном уровнях одним из двух способов: путем внутрисегментного или межсегментного на-

вязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИС. Реализация угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно-адресные таблицы. Последствия – несанкционированное изменение маршрутно-адресных данных, анализ и модификация передаваемых данных, навязывание ложных сообщений.

Внедрение ложного объекта сети. Эта угроза основана на использовании 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 нарушителем 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. Последствиями могут являться перехват и просмотр трафика, несанкционированный доступ к сетевым ресурсам, навязывание ложной информации.

Для реализации этого рода угроз используется канальный и прикладной уровень эталонной модели. Такого рода атаки получили название «фишинг» (англ. *fishing* – «рыбалка»).

В данном случае фишинг может быть двух видов: как бы законный фишинг, когда в результате невнимательности пользователя его запрос переадресуется с необходимого объекта на ложный объект, и незаконный, когда идет подстановка (замена) маршрута.

Примерами фишинга можно считать и другие атаки. Скажем, факсимильным сообщением в офис организации доставляется письмо с просьбой прислать идентификационные данные ПО для проверки. Таким образом злоумышленники собирают ключи ПО и дальше их перепродают.

Отметим, что большинство вариантов фишинга основано преимущественно на социальной инженерии и эксплуатации невнимательности или неграмотности пользователей в области ИТ.

Отказ в обслуживании. Эти угрозы основаны на недостатках сетевого ПО, его уязвимостях, позволяющих нарушителю создавать условия, когда ОС оказывается не в состоянии обрабатывать поступающие пакеты (производится на сеансовом уровне), либо же ширины физической среды передачи данных становится недостаточно для транспортировки количества и объема передаваемых через нее пакетов данных (производится на канальном уровне). Результатом реализации этой угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к информации, переполнение очереди запросов одной или нескольких сетевых служб, даже полная остановка ОС компьютера из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

Удаленный запуск приложений. Угроза заключается в стремлении запустить на хосте ИС различные, предварительно внедренные, вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых – нарушение конфиденциальности, целостности, актуальности и доступности информации, вплоть до полного контроля за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для получения необходимых нарушителю данных, запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса таких угроз:

1) распространение файлов, содержащих несанкционированный исполняемый код (используется прикладной уровень);

2) удаленный запуск приложения путем переполнения буфера приложений-серверов (используется сеансовый уровень);

3) удаленный запуск приложения через возможности удаленного управления системой, предоставляемые скрытыми программными и аппаратными закладками либо используемые штатными средствами (используется прикладной уровень).

Классификация по виду нарушаемого свойства ИБ. По виду несанкционированных действий, осуществляемых по отношению к информации, выделяются следующие группы угроз [2]:

- угрозы, приводящие к нарушению конфиденциальности информации (утечке, копированию или несанкционированному распространению), при реализации которых не осуществляется непосредственного воздействия на содержание информации;
- угрозы, приводящие к несанкционированному (в том числе случайному) воздействию на содержание информации (нарушение целостности, актуальности);
- угрозы, приводящие к несанкционированному (в том числе случайному) воздействию на программно-аппаратные элементы информационной системы, в результате которого осуществляется блокирование информации (нарушение доступности).

Классификация по виду используемой уязвимости включает [3]:

- угрозы, реализуемые с использованием уязвимости системного ПО;
- угрозы, реализуемые с использованием уязвимости прикладного ПО;
- угрозы, возникающие в результате использования уязвимости в аппаратных средствах;
- угрозы, реализуемые с использованием уязвимостей протоколов сетевого взаимодействия и каналов передачи данных;
- угрозы, реализуемые с использованием уязвимостей, обусловливающих наличие технических каналов утечки информации.

Классификация по объекту воздействия содержит угрозы безопасности информации:

- реализуемые через автоматизированные рабочие места пользователей;
- реализуемые посредством воздействия на серверы (в том числе в кластеры и облачные хранилища);
- хранящейся и обрабатываемой в выделенных средствах обработки (принтерах, плоттерах, графопостроителях, вынесенных мониторах, видеопроекторах, средствах звуковоспроизведения и т. п.);
- реализуемые в процессе взаимодействия с каналами связи.

Классификация по виду активов, подверженных угрозам ИБ, включает:

- угрозы безопасности пользовательских данных и документов, хранящихся на рабочих станциях пользователей;
- угрозы безопасности пользовательских данных и документов, хранящихся на серверах (в том числе в кластерах и облачных хранилищах);
- угрозы работоспособности сетевых сервисов, оборудования и ПО рабочих станций и серверов, которые могут быть вызваны успешными атаками на отказ в обслуживании или другими причинами, ведущими к нарушениям свойства доступности информации.

Заключение

В данной работе проведены анализ и классификация основных угроз и уязвимостей ИБ, в том числе описана общая характеристика угроз ИБ, реализуемых с использованием протоколов межсетевого взаимодействия.

Основная цель создания классификации угроз – наиболее полная, детальная классификация, которая описывает все существующие угрозы ИБ, по которой каждая из угроз попадает только под один классификационный признак и которая, таким образом, наиболее применима для анализа рисков реальных ИС.

---

[2] Модель угроз и нарушителя безопасности персональных данных, обрабатываемых в типовых информационных системах персональных данных отрасли (Решение секции № 1 Научно-технического совета Минкомсвязи России «Научно-техническое и стратегическое развитие отрасли» от 21 апреля 2010 года № 2).

[3] См. базовую модель угроз безопасности.

Список литературы

1. *Мазов Н. А., Ревнивых А. В., Федотов А. М.* Классификация рисков информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2011. Т. 9, вып. 2. С. 80–89.

2. *Ревнивых А. В., Федотов А. М.* Обзор политик информационной безопасности // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2012. Т. 10, вып. 3. С. 66–79.

3. *Галатенко В. А.* Основы информационной безопасности. М., 2004. 264 с.

4. *Raúl Rojas, Ulf Hashagen.* The First Computers: History and Architectures. MIT Press, 2002.

5. *Камер Д.* Сети TCP/IP. = Internetworking with TCP/IP. М.: Вильямс, 2003. Т. 1: Принципы, протоколы и структура.

6. *Паркер Т., Сиян К.* TCP/IP. Для профессионалов. 3-е изд. СПб.: Питер, 2004.

7. *Вихорев С. В.* Классификация угроз информационной безопасности. URL: http://www.cnews.ru/reviews/free/oldcom/security/elvis_class.shtml.

8. *Скрипник Д. А.* Общие вопросы технической защиты информации. М.: ИНТУИТ.РУ Интернет-университет информационных технологий, 2004.

9. *Цирлов В. Л.* Основы информационной безопасности автоматизированных систем: Краткий курс. М.: Феникс, 2008.

10. *Киреенко А. Е.* Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. 2012. № 3.

11. *Радько Н. М., Скобелев И. О.* Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: Радио Софт, 2010.

12. Технические средства и методы защиты информации: Учебник для вузов / Под ред. А. П. Зайцева, А. А. Шелупанова. М.: Машиностроение, 2009.

Материал поступил в редколлегию 22.05.2013

A. A. Mukhanova, A. V. Revnivykh, A. M. Fedotov

CLASSIFICATION OF THREATS AND VULNERABILITIES OF INFORMATION SECURITY IN CORPORATE SYSTEMS

This paper describes devotion and the analysis of threats and vulnerabilities of information security in corporate systems. As an example for the detailed analysis network attacks to level of reference model of interaction of open systems (ISO/OSI) on which the threat using vulnerabilities of protocols of network.

Keywords: information security, classification of threats, classification of vulnerabilities, access to information, the distributed information resources.

УДК 004.942

В. В. Прокошев, **В. А. Скляренко**, **П. Ю. Шамин**

Владимирский государственный университет
ул. Горького, 87, Владимир, 600000, Россия

E-mail: trace83@mail.ru

ОПЫТ ПРИМЕНЕНИЯ МОДЕЛЕЙ ПЕРКОЛЯЦИОННОГО ТИПА ДЛЯ АНАЛИЗА ПРОЦЕССА ПРОХОЖДЕНИЯ СИГНАЛА В БОЛЬШИХ АНСАМБЛЯХ ДВИЖУЩИХСЯ ОБЪЕКТОВ *

Рассмотрены вопросы применения теории перколяции для моделирования динамических информационных сетей. Подтверждается существование порога перколяции и качественного изменения надежности доставки пакетов данных при его превышении.

Ключевые слова: динамические сети, порог перколяции, прохождение сигнала.

Введение

Перколяционные модели различных видов в настоящее время весьма широко используются в приложениях, см. например, [1]. Математическая же перколяционная теория (дискретный случай) заключается в следующем. За основу берется бесконечный граф; часто это просто регулярная решетка. Далее, выделяется случайный подграф этого графа, а именно: вершинам случайно и независимо с одинаковой вероятностью p присваивается состояние «проводящая». Подграф состоит только из проводящих вершин; смежными вершинами подграфа считаются любые соседние вершины исходного графа, находящиеся в проводящем состоянии. Основным предметом изучения теории является структура связных компонент. Наиболее интересный обнаруженный эффект – перколяционный фазовый переход по параметру p. Установлено, что в ряде случаев существует p^* (порог перколяции). А именно: при $p < p^*$ «почти наверное» все связные компоненты конечны, а при $p > p^*$ «почти наверное» существует бесконечная связная компонента, которая называется «перколяционным кластером». В случае его существования говорят, что происходит протекание на бесконечность – перколяция. В ситуации квадратной решетки, например, $p^* = 0{,}5$ см [2].

В данной работе исследуется взаимодействие (передача «сигнала») внутри ансамбля движущихся объектов. В этом случае естественно использовать именно дискретный вариант перколяционной модели. Более того, учитывая специфику подобных задач, удобнее рассматривать граф, где в двух состояниях могут находиться не вершины, а ребра, модель связей. При этом в подграф входят все вершины, а смежными считаются только те, которые соединены ребром, находящимся в проводящем (сигнал проходит) состоянии. Естественно, при

* Данная работа выполнена в рамках НИР по госзаданию «Наука» (регистрационный № 8.3534.2011 от 23.11.2011).

Прокошев В. В., Скляренко В. А., Шамин П. Ю. Опыт применения моделей перколяционного типа для анализа процесса прохождения сигнала в больших ансамблях движущихся объектов // Вестн. Новосиб. гос. ун-та. Серия: Информационные технологии. 2013. Т. 11, вып. 2. С. 73–81.

ISSN 1818-7900. Вестник НГУ. Серия: Информационные технологии. 2013. Том 11, выпуск 2

моделировании рассматриваются достаточно большие, но все же конечные графы. В этом случае порог перколяции – это значение вероятности p^*, при котором в графе образуется «перколяционный кластер» – связная область, обеспечивающая протекание, прохождение сигнала от одной границы до другой. Характерной особенностью всех упомянутых выше моделей является свойство независимости розыгрыша состояния (узла или связи). Это условие, как показано ниже, нарушается в исследуемой нами модели. Сначала в статье обосновывается существование таких зависимостей и их влияние на значение порога перколяции, а затем рассматривается влияние одного из параметров передачи сигнала (времени жизни) на передачу сигнала в изучаемых моделях и предлагается возможный подход к сведению модели динамической системы к ранее рассмотренным моделям с независимым розыгрышем состояния.

Определение порога перколяции в среде движущихся объектов

Теоретический анализ. Учитывая роль, которую играют циклические периодические и почти периодические процессы, мы рассматриваем задачу о прохождении сигнала в среде, состоящей из объектов, движущихся циклически (по окружности). Данная часть посвящена определению порогового значения вероятности $p*$, наличия связи между двумя соседними объектами, при котором вероятность прохождения сигнала через среду меняется скачком. Разумеется, постановка задачи допускает разного рода обобщения.

Опишем рассматриваемую модель. Полагаем, что в узлах плоской квадратной решетки размера $m{\cdot}n$ с шагом d расположены центры окружностей радиуса r ($d > 2r$), по которым равномерно, с несоизмеримыми скоростями вращаются объекты. Сигнал подается на все объекты $(1, j)$, $1 \le j \le m,$ и считается прошедшим через систему, если он будет передан хотя бы на один из объектов (n, j), $1 \le j \le m.$ Сигнал может быть передан мгновенно и без задержки от объекта (i, j) только своим соседям $(i, j+1)$, $(i-1, j)$, $(i+1, j)$ при выполнении условия: расстояние между объектами, для которых осуществляется связь не больше, чем k, $(d - 2r < k < d + 2r)$. В отличие от классического случая перколяции (см. обзорную статью [1]) возможность передачи сигнала между соседними объектами зависит от момента времени.

Конфигурационным пространством системы является тор размерности $m \cdot n$, эволюция системы описывается траекторией на торе $\boldsymbol{\varphi}(t) = \boldsymbol{\varphi}(0) + \boldsymbol{\omega} t$, где $\boldsymbol{\varphi}(0)$ – вектор начальных фаз объектов, а $\boldsymbol{\omega}$ – вектор частот вращения объектов по окружностям. Поскольку частоты вращения несоизмеримы, то, по следствию из теоремы об усреднении [3. С. 248], справедливо равенство

$$\lim_{T\to\infty} \frac{1}{T}\tau(T) = \frac{1}{(2\pi)^{mn}} |D|, \qquad (1)$$

где D – жорданова область на торе, $|D|$ – ее мера, $\tau(T)$ – время, в течение которого за промежуток $[0, T]$ траектория $\boldsymbol{\varphi}(t)$ находится в D. Другими словами, вероятность нахождения системы в том или ином состоянии пропорциональна мере области в конфигурационном пространстве, соответствующей этому в состоянию.

Пользуясь равенством (1), найдем вероятность p, с которой сигнал может быть передан между двумя соседними объектами.

Пусть область D на двумерном торе задана условием (рис. 1)

$$|AB|^2 = r^2(\sin\alpha - \sin\beta)^2 + (d - r\cos\alpha - r\cos\beta)^2 \le k^2$$

или

$$4r^2\cos^2\frac{\alpha+\beta}{2} + 4rd\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2} \le k^2 - d^2.$$

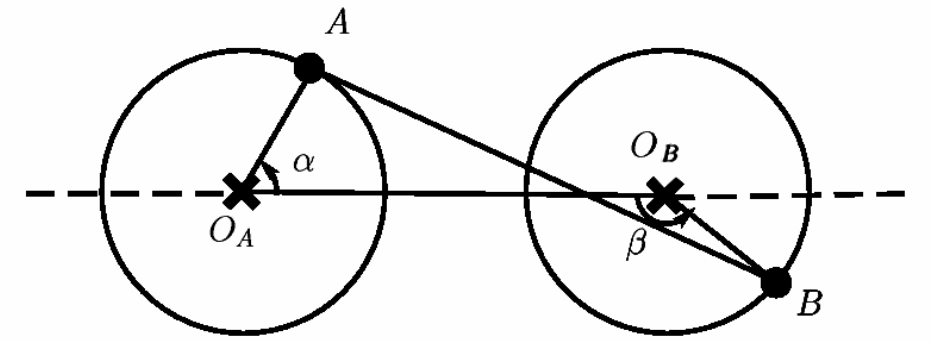


Рис. 1. Параметры области D

Ограничимся случаем $d=3,\ \ r=1,\ \ k=3$. На развертке двумерного тора $(-\pi,\pi]^2$ область D имеет вид, показанный на рис. 2.

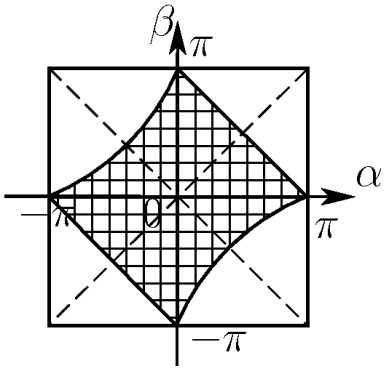


Рис. 2. Область D на развертке двумерного тора

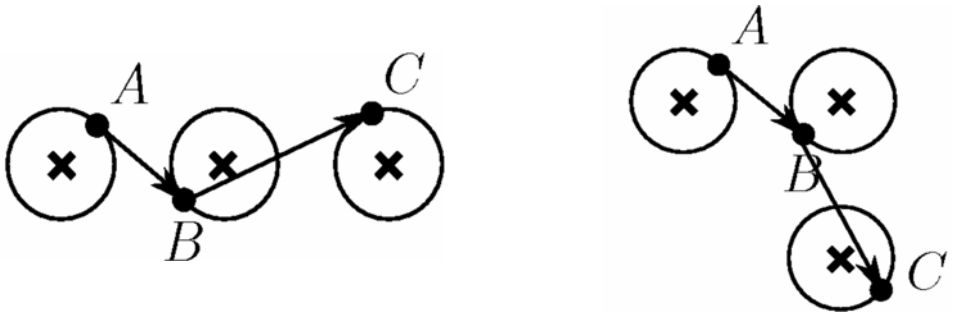
Из неравенства, описывающего D, следует, что область симметрична относительно прямых $\alpha-\beta=0$ и $\alpha+\beta=0$. Таким образом, вероятность наличия связи может быть найдена как

$$p=\frac{1}{(2\pi)^2}\iint\limits_D d\alpha\, d\beta=\frac{1}{\pi^2}\iint\limits_{\substack{\beta\ge\alpha,\ \ \beta\ge-\alpha,\,|\alpha|\le\pi,\,|\beta|\le\pi,\\ 4r^2\cos^2\frac{\alpha+\beta}{2}+4rd\cos\frac{\alpha+\beta}{2}\cos\frac{\alpha-\beta}{2}\le k^2-d^2}} d\alpha\, d\beta=$$

$$=\left|\begin{array}{l} x=\cos\frac{\alpha+\beta}{2}\\ y=\cos\frac{\alpha-\beta}{2}\\ \frac{D(\alpha,\beta)}{D(x,y)}=\frac{-2}{\sqrt{(1-x^2)(1-y^2)}}\end{array}\right|=\frac{2}{\pi^2}\iint\limits_{\substack{y\ge-x,\,|x|\le1,\,|y|\le1,\\ 4r^2x^2-4rdxy\le k^2-d^2}}\frac{dx\,dy}{\sqrt{(1-x^2)(1-y^2)}}. \qquad (2)$$

Так, при $d=3,\ \ r=1,\ \ k=3$ формула (2) дает $p=0{,}4316$.

Поскольку далее вероятности оценивались через относительные частоты, полученные в численном эксперименте, а реализовать на практике несоизмеримость частот ω_A и ω_B невозможно, был проведен численный эксперимент: при $d=3,\ \ r=1,\ \ k=3,$ сдвиге фазы $\varphi(0)=1$, величине шага 0,01, числе шагов 10 000, частотах вращения $\omega_A=11,\ \ \omega_B=13$ доля тех точек, для которых $|AB|\le k$ составила 0,4318. При других исходных данных результаты также были достаточно близки.



а б

Рис. 3. Конфигурации подвижных узлов

Заметим, что события, состоящие в передаче сигнала от A к B и от B к C (рис. 3) не являются независимыми. Как вычисления, основанные на теореме об усреднении, так и численный эксперимент при $d=3,\ \ r=1,\ \ k=3$ показывают, что вероятность перехода сигнала от A к C в конфигурации рис. 3, *а* равна 0,1098, при том что произведение вероятностей передачи сигнала от A к B и от B к C, напомним, равно $0,4316^2=0,1863$. Для конфигурации рис. 3, *б* результаты ближе – 0,1866.

Численный эксперимент. Моделируется процесс прохождения сигнала через систему («запуск»), при этом делаются некоторые предположения. Каждый объект системы интерпретируется как узел, движущийся по определенному закону и принимающий / отправляющий сигнал. Считается, что сигнал распространяется по системе мгновенно и узлы не меняют свое положение за время запуска. Также считается, что связь между двумя узлами может быть использована только один раз. Целью моделирования является определение критического значения вероятности p^*, при которой вероятность прохождения сигнала через систему скачком меняется с нуля на единицу.

Эксперимент проводился на разработанном нами сетевом симуляторе (ПСС), установленном на высокопроизводительной кластерной системе [5; 6]. Для решения задачи были реализованы следующие модули расширения.

1. Модуль начальной инициализации координат узлов. Случайным образом располагает каждый узел системы на соответствующей ему окружности. Входные параметры: d – шаг решетки, r – радиус окружностей, N – количество узлов в одном слое.

2. Модуль генерации топологии сети. Для каждого узла проверяет условие возможности связи с соседними узлами ($|AB| < k$). Если условие выполнено, то соседний узел добавляется к списку узлов, связь с которыми возможна. Входным параметром является k – максимальное расстояние, связь на котором возможна.

3. Основной модуль. Реализует пересылку пакетов в соответствии с поставленной задачей. Также проверяет условия окончания моделирования:

а) пакет доставлен на последний слой (считаем проход успешным);

б) невозможно передать ни один пакет.

Принципиальная схема эксперимента такова. При неизменном значении набора входных параметров производится нескольких запусков, при этом в каждом повторном запуске случайным образом меняется положение узлов на окружностях (это моделирует их движение). Оценивается вероятность прохождения сигнала через систему; вычисляется отношение числа успешных проходов к общему количеству запусков. Меняются значения параметров, выясняется, когда происходит качественная перестройка процесса прохождения сигнала.

Машинный эксперимент был проведен для квадратной решетки размеров $N\times N$ ($N=100$, 300, 500). Входные параметры (см. выше), используемые в эксперименте: d, r постоянны ($d=3$, $r=1$); k изменяется в некотором диапазоне. Результаты машинного эксперимента отражены на графике (рис. 4). Отметим также, что под осью k дополнительно указаны значения p (вероятности передачи сигнала между парой соседних узлов). Они определяются парамет-