ДОВЕРЕННАЯ СРЕДА

УДК 004.4

Расчет рисков информационной системы в терминах сетей Петри

Д. А. Корнев, канд. техн. наук
Московский технологический институт, Москва, Россия

Представлена методика расчета вероятности потери конфиденциальности информации на защищенном вычислительном ресурсе, позволившая получить хорошую сходимость со статистикой уязвимостей корпоративных информационных систем. Для реализации методики используются математический аппарат цветных сетей Петри и метод статистических испытаний (Монте-Карло). Рассчитаны вероятности обеспечения конфиденциальности информации ресурса с криптографической защитой информации при MITM-атаке и пяти основных типах защит ресурса.

Ключевые слова: вычислительный комплекс, математическая модель, риски информационной системы, MITM-атака, сети Петри.

В современных условиях значимости информации меры ее защиты разрабатываются в соответствии с техническим заданием и структурой информационной системы (ИС), учитывающей физиче-ские, логические, функциональные и технологические взаимосвязи между ее сегментами. Для определения степени возможного ущерба от нарушения конфиденциальности, целостности или доступности должны применяться национальные стандарты и методический документ "Меры защиты информации в государственных информационных системах" (11 февраля 2014 г.), разработанный в соответствии с п/п 4 п. 8 "Положения о Федеральной службе по техническому и экспортному контролю", утвержденного Указом Президента Российской Федерации, от 16 августа 2004 г. № 1085.

Для снижения уровня рисков передаваемой через сеть информации применяются методы криптографии, однако из опыта следует, что даже в этом случае информацию нельзя считать защищенной. В 2011—2012 гг. компания Positive Technologies провела тестирование на проникновение в информационные системы наиболее крупных государственных и коммерческих компаний (в том числе входящих в рейтинг 400 крупнейших компаний России в 2012 г. по объему реализации продукции по версии агентства "Эксперт") [1] .

В результате проведенных работ в 75 % случаев специалистам Positive Technologies удалось получить полный контроль над критическими ресурсами тестируемых систем, при этом почти в половине случаев (45 %) подобный уровень доступа мог быть получен со стороны любого внешнего нарушителя. Три четверти рассмотренных систем содержали уязвимости высокого уровня риска, связанные с недостатками конфигурации; еще в 25 % систем были выявлены недостатки среднего уровня риска.

Поскольку внедрение защиты связано с финансовыми затратами и дополнительным использованием вычислительного ресурса, применение того или иного типа защиты информационной системы должно выполняться после расчета риска как сравнения потерь от потенциальной угрозы и затрат на внедрение механизма защиты. При поиске рационального варианта защиты необходимо учитывать структуру информационной среды и вероятный способ поиска доступа к ней.

В статье приведена методика решения задачи по расчету потенциальной угрозы доступа к ресурсу информационного комплекса (ИК) в случае проведения атаки типа Man in the Middle (MITM-атаки).

Для решения задачи определения вероятности угрозы доступа к информационной системе целесообразно использовать математический аппарат цветных сетей Петри. Этот аппарат позволяет объединить преимущества графового представления и дискретной динамической модели системы, рассчитывать количественные показатели ее работы, которые характеризуются параллельными и асинхронными процессами. Графически в терминах цветных сетей Петри динамическая модель ИК, использующего криптографическую защиту информации, представляется ориентированным маркированным графом, состоящим из множества по-

Корнев Дмитрий Алексеевич, инженер первой категории.
E-mail: da.kornev@gmail.com

Статья поступила в редакцию 19 сентября 2016 г.

зиций P и множества переходов T, соединенных между собой цветными дугами (рис. 1) [2]:

$$\Pi = \{P, T, I, O, \mu\},$$

где I — входная функция переходов, определяющая кратность входных дуг переходов $I(t_j)$;

O — выходная функция переходов, определяющая кратность выходных дуг переходов $O(t_j)$;

μ — вектор маркировки;

$$P = \left\{ \begin{array}{c} p_1, p_2, p_{10}, p_{11}, p_{12}, p_{13}, p_{14}, p_{15}, \\ p_{20}, p_{21}, p_{30}, p_{31}, p_{140}, p_{150}, \\ p_{160}, p_{170}, p_{180}, p_{190} \end{array} \right\}.$$

Элементами множества позиций P являются: p_1, p_2 — передача и получение клиентом информации; p_{10}, p_{11}, p_{12} — легитимный канал передачи данных от клиента к ресурсу; p_{13}, p_{14}, p_{15} — легитимный канал передачи данных от ресурса к клиенту; p_{20}, p_{21} — получение и передача пакета (информации) ресурсом; p_{30} — легитимные настройки систем маршрутизации; p_{31} — скомпрометированные настройки систем маршрутизации; p_{140} — получение атакующим зашифрованного пакета от клиента; p_{150} — пакет клиента расшифрован атакующим; p_{160} — пакет клиента зашифрован атакующим; p_{170} — получение атакующим зашифрованного пакета от ресурса; p_{180}, p_{190} — пакет ресурса расшифрован и пакет ресурса зашифрован атакующим.

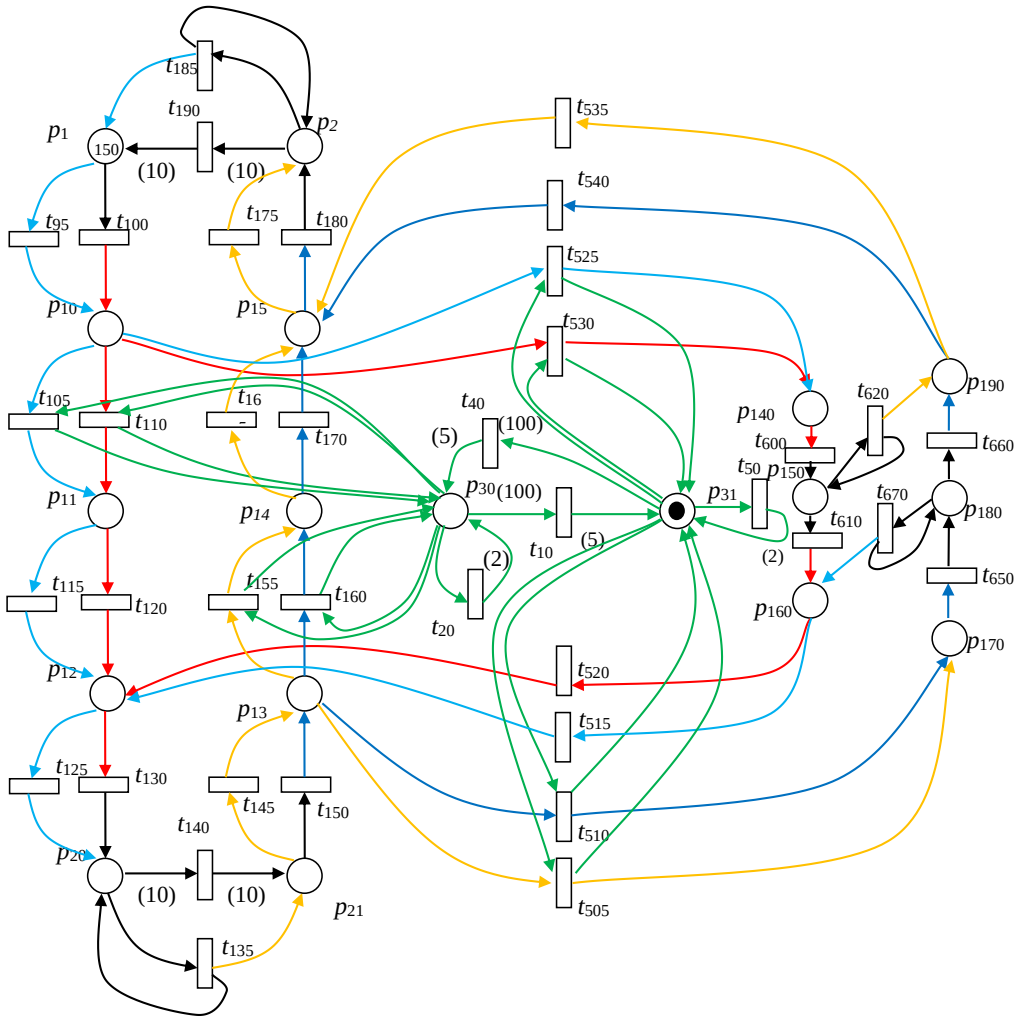

Рис. 1. Модель расчета рисков для шифрованной информации ИК в терминах цветных сетей Петри (в скобках указана кратность перехода)

Элементами множества позиций T являются: t_{10} — перенаправление трафика через атакующего; t_{40} — перенаправление трафика через легитимные каналы связи; t_{20}, t_{50} — воздействие на средства маршрутизации атакующим; t_{100} — шифрование пакета клиентом и передача его ресурсу; t_{110}, t_{120} — передача зашифрованного пакета по легитимному каналу от клиента к ресурсу; t_{130} — дешифрование пакета ресурсом; t_{140} — формирование ответа ресурсом; t_{150} — шифрование пакета ресурсом и передача его клиенту; t_{95}, t_{105}, t_{115}, t_{125} — передача подтверждения получения пакета клиентом; t_{135} — формирование подтверждения получения пакета ресурсом; t_{145}, t_{155}, t_{165}, t_{175} — передача подтверждения получения пакета ресурсом; t_{160}, t_{170} — передача зашифрованного пакета по легитимному каналу от ресурса клиенту; t_{180} — дешифрование пакета клиентом; t_{185} — формирование подтверждения получения пакета клиентом; t_{190} — формирование ответа клиентом; t_{505} — передача подтверждения о получении пакета от ресурса к атакующему; t_{510} — передача пакета от ресурса к атакующему; t_{515} — передача подтверждения о получении пакета клиентом, сфальсифицированного атакующим; t_{520} — передача пакета от атакующего к ресурсу; t_{525} — передача подтверждения получения пакета от клиента к атакующему; t_{530} — передача пакета от клиента к атакующему; t_{535} — передача подтверждения получения пакета ресурсом, сфальсифицированного атакующим; t_{540} — передача пакета от атакующего к клиенту; t_{600} — расшифровка пакета клиента атакующим; t_{610} — шифрование пакета клиента атакующим; t_{620} — фальсификация подтверждения получения пакета ресурсом; t_{650} — расшифровка пакета ресурса атакующим; t_{660} — шифрование пакета ресурса атакующим; t_{670} — фальсификация получения пакета клиентом.

Моделирование маршрутов в маркированном графе цветных сетей Петри должно удовлетворять условиям

$$\left|I\left(p_i\right)\right| = \left|\left\{t_j | p_i : \text{color} \in O : \text{color}\left(t_j\right)\right\}\right| = 1;$$

$$\left|O\left(p_i\right)\right| = \left|\left\{t_j | p_i : \text{color} \in I : \text{color}\left(t_j\right)\right\}\right| = 1,$$

где $\left\{t_j | p_i : \text{color} \in I : \text{color}\left(t_j\right)\right\}$ — множество переходов с дугами соответствующих цветов, для которых p_i является входом;

$\left\{t_j | p_i : \text{color} \in O : \text{color}\left(t_j\right)\right\}$ — множество переходов с дугами соответствующих цветов, для которых p_i является выходом.

Разрешение на выполнение перехода $t_i \in T$ определяется условием [2]

$$t_j : \mu : \left(p_i\right) \geq \#\left(p_i : \text{color}, I : \text{color}\left(t_j\right)\right) \qquad (1)$$

для всех $p_i \in P$, где $\left(p_i : \text{color}, I : \text{color}\left(t_j\right)\right)$ — кратность входной позиции p_i соответствующего цвета для дуги перехода t_j этого же цвета, т. е. переход t_j разрешен при некоторой маркировке $\mu : \left(p_i\right)$ если позиция $p_i \in P$ имеет разметку соответствующего цвета, не меньшую, чем кратность дуги этого же цвета, соединяющей p_i и t_j.

Результатом выполнения разрешенного перехода $t_i \in T$ является новая маркировка μ':

$$\mu'\left(p_i\right) = \mu\left(p_i\right) - \#: \text{color}\left(p_i, I\left(t_j\right)\right) + \\ + \#: \text{color}\left(p_i, O\left(t_j\right)\right). \qquad (2)$$

В итоге динамическая модель, состоящая из 57 логических уравнений типа (1), (2), описывает алгоритм взаимодействия клиента и ресурса при работе с шифрованной информацией в штатном режиме функционирования ИК и при проведении MITM-атаки.

Динамический процесс функционирования ИК в штатном режиме и при проведении MITM-атаки представлен на рис. 2. Кроме действий клиента, ресурса и атакующего, здесь отражены процессы получения подтверждений о передаче пакетов информации от клиента ресурсу ($p_{2:\text{orange}}$) и от ресурса клиенту ($p_{20:\text{cyan}}$) в текущем времени.

Клиент формирует запрос (состояние p_1), и передает его ресурсу; при этом каждый пакет информации шифруется (переход t_{100}) (рис. 1, 2). Получение ресурсом шифрованного пакета идентифицируется состоянием p_{12}. После этого информация пакета дешифруется (переход t_{130}) и передается ресурсу (состояние p_{20}). Ресурс формирует подтверждение получения пакета (переход t_{135}).

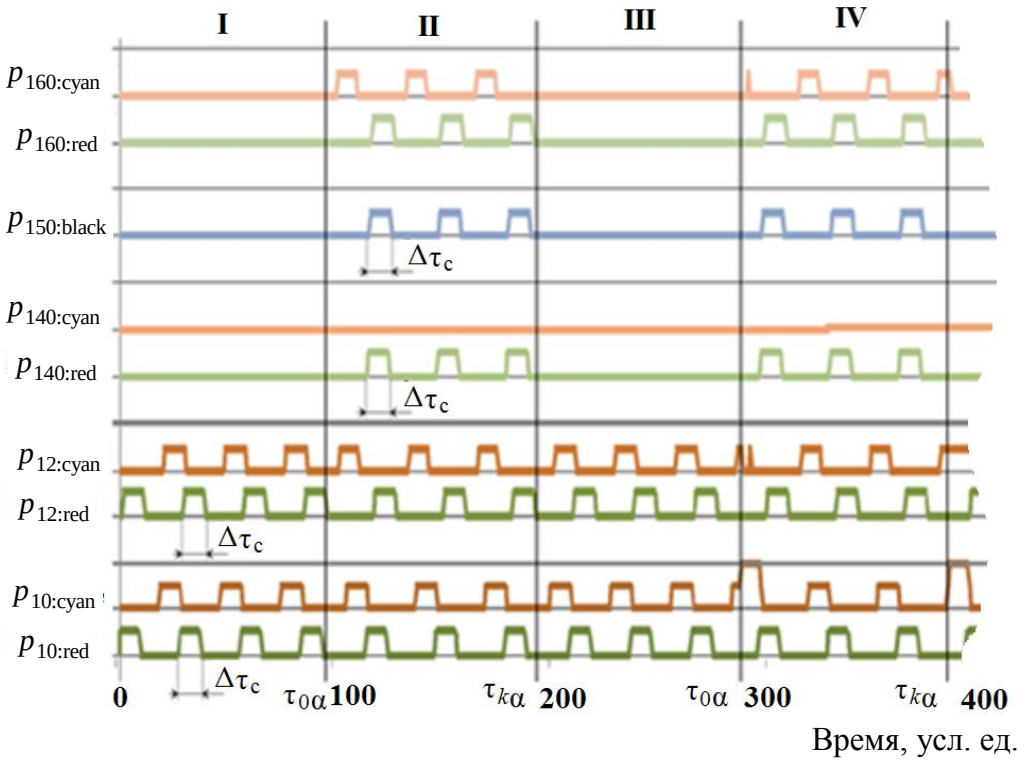

Рис. 2. Результаты моделирования MITM-атаки на информационный комплекс при условии криптографической защиты передаваемой информации:

$\tau_{0\alpha}$, $\tau_{k\alpha}$ — моменты начала и окончания атаки; τ_c — время передачи сообщения; $p_{10:red}$, $p_{12:red}$ — получение клиентом и ресурсом шифрованной информации; $p_{10:cyan}$, $p_{12:cyan}$ — получение клиентом и ресурсом подтверждения о передаче пакетов информации; $p_{140:red}$ — получение атакующим шифрованного пакета; $p_{140:cyan}$ – получение атакующим подтверждения о передаче шифрованного пакета; $p_{150:black}$, $p_{160:red}$ — пакет клиента расшифрован и зашифрован атакующим; $p_{160:cyan}$ — фальсификация атакующим подтверждения о получении шифрованного пакета

Передача клиенту подтверждения получения ресурсом каждого пакета информации осуществляется через переходы $t_{145}, t_{155}, t_{165}, t_{175}$. После получения ресурсом исходного сообщения (всех пакетов информации) он формирует ответ, что идентифицируется состоянием p_{21}, и передает его клиенту (состояние p_{15}), шифруя при этом каждый пакет. Процедуре шифрования каждого пакета информации соответствует переход t_{150}. После получения клиентом каждого шифрованного пакета (состояние p_{15}) он дешифруется (переход t_{180}) в открытый текст (состояние p_2). Клиент формирует подтверждение получения каждого пакета (переход t_{185}) и передает его ресурсу (переходы $t_{95}, t_{105}, t_{115}, t_{125}$). После получения клиентом всего пакета информации (состояние p_2) он формирует новый запрос ресурсу (переход t_{190}).

При штатном функционировании ИК переход t_{10} пассивен и маркер присутствует в состоянии p_{30}. Это соответствует тому, что передача трафика между клиентом (состояния p_1, p_2) и ресурсом (состояния p_{20}, p_{21}) осуществляется по легитимному каналу связи через промежуточные состояния системы p_{10}, p_{11}, p_{12} и p_{13}, p_{14}, p_{15}.

В случайный момент времени атакующий воздействует на средства маршрутизации (переход t_{20}) и в случае успеха перенаправляет информацию через себя. При этом переход t_{10} активизируется и изменяет маркировку сети: маркеры из состояния p_{30} переходят в состояние p_{31}, в результате чего закрываются переходы t_{110} и t_{160}, а трафик между клиентом и ресурсом проходит через атакующего (переходы $t_{505}, t_{510}, t_{525}, t_{530}$, состояния p_{140} и p_{170}). Атакующий дешифрует полученные пакеты (переходы t_{600}, t_{650}), получая при этом доступ к информации (состояния p_{150} и p_{180}), затем фальсифицирует подтверждения о получении соответствующих пакетов (переходы t_{620}, t_{670}) и передает их клиенту (переход t_{535}) или

ресурсу (переход t_{515}). "Прочитав" каждый пакет, атакующий снова шифрует его (переходы t_{610}, t_{660}) и передает ресурсу или клиенту (переходы t_{540}, t_{520}).

Такие действия эквивалентны закрытию легитимного канала передачи информации между клиентом и ресурсом и открытию канала через атакующего, обеспечивающего "перехват" и "прослушивание" конфиденциальной шифрованной информации. Время прослушивания информации определяется функционированием перехода t_{50}. Собрав необходимую информацию, нарушитель уходит из сети, и легитимные каналы передачи информации восстанавливаются, что соответствует срабатыванию перехода t_{40}.

Разработанная модель была использована для расчета вероятности доступа к информации, хранящейся на виртуальном ресурсе, при следующих типах защит:

- защита ресурса;
- защита файловой системы ресурса;
- защита серверной системы;
- применение средств обеспечения безопасности сетевой инфраструктуры.

Поскольку информационные риски в общем случае можно рассматривать как конфликтные ситуации, в разработанной методике был использован метод статистических испытаний (метод Монте-Карло) [3]. Метод Монте-Карло применим для описания работы систем, случайные процессы в которых не являются марковскими (к последним относится и сетевой ресурс), и дает возможность получения адекватного результата, когда построение аналитической модели объекта трудноосуществимо.

Задача решалась для дерева атак на ресурс, где представлены угрозы его элементам (рис. 3).

Угрозы в отношении сервера могут быть реализованы любым доступным способом взлома: заражением, фишингом и т. д. ($l_{10}, l_{11}, l_{15}, l_{17}$). Результатом этих действий являются доступ к терминалу сервера (l_6), возможность установки сниффера или анализатора трафика (l_3) и, соответственно, доступ к сетевому интерфейсу (l_1).

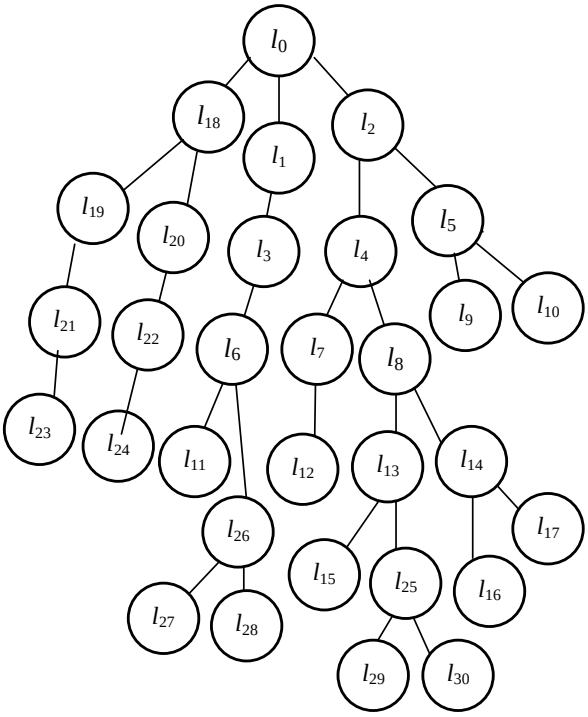

Рис. 3. Граф дерева атаки, направленной на прослушивание трафика сетевого ресурса:
l_0 — прослушивание трафика сетевого ресурса; l_1 — доступ к сетевому интерфейсу сервера; l_2 — доступ к сетевому интерфейсу ресурса; l_3 — установка сниффера или анализатора трафика на сервер; l_4 — установка сниффера или анализатора трафика на ресурс; l_5 — доступ к гипервизору; l_6 — доступ к терминалу сервера; l_7 — доступ к терминалу ресурса; l_8 — доступ к файлам ресурса; l_9, l_{16} — удаленный доступ к гипервизору; l_{10}, l_{11}, l_{15}, l_{17} — доступ к хосту (заражение, фишинг и т.д.); l_{12} — доступ к ресурсу (заражение, фишинг и т.д.); l_{13} — доступ к файлам хоста; l_{14} — доступ к гипервизору ; l_{18} — перенаправление компрометируемого трафика; l_{19} — ARP-компрометация; l_{20} — DNS-ком-прометация; l_{21} — доступ к LAN; l_{22} — доступ к DNS-службе; l_{23}, l_{24} — анализ структуры LAN; l_{25}, l_{26} — развертывание скомпрометированной системы и целевого ресурса на одном сервере; l_{27}, l_{29} — доступ к любой системе инфраструктуры как к независимому объекту (заражение, фишинг и т. д.); l_{28}, l_{30} — доступ к репозиторию

Угрозы в отношении гипервизора могут быть достигнуты либо после взлома сервера, либо путем несанкционированного удаленного управления гипервизором (l_9, l_{16}). Взлом гипервизора позволит получить контроль над эмуляцией сетевого интерфейса и, соответственно, перехватить входящий и исходящий трафик l_5.

Угрозы в отношении ресурса могут быть реализованы путем взлома физических аппаратных средств (сервера или репозитория) или гипервизора, что позволит модифицировать его файлы (l_{13}) и файлы ресурса (l_8, l_{14}). Также можно рассматривать ресурс как независимое физическое устройство; соответственно возможен его непосредственный взлом любым доступным способом: заражением, фишингом и т. д. (l_{12}). Это опять же открывает доступ к терминалу ресурса (l_7), так как позволяет установить сниффер или анализатор трафика (l_4) и получить доступ к сетевому интерфейсу ресурса (l_2).

Угроза безопасности конечному сетевому ресурсу может быть реализована атакующим через доступную ему среду (l_{27}, l_{29}) или репозиторий (l_{28}, l_{30}). После развертывания скомпрометированной системы (l_{25}, l_{26}) она используется для атаки на сетевой ресурс.

Можно рассматривать сетевой ресурс как независимый объект и провести на него типовую MITM-атаку, используя ARP-poising или через DNS-службу. Для этого необходимо проанализировать структуру компрометируемой локальной сети (LAN) (l_{23}, l_{24}), после чего провести атаку на любой ее элемент (l_{21}) или используемый DNS-сервер (l_{22}). Это позволяет осуществить ARP-poising (l_{19}) или переопределение службы DNS (l_{20}), за счет чего компрометируемый трафик перенаправляется через атакующего.

Очевидно, что вес каждой ветви дерева атак определяется вероятностями реализации конкретной последовательности угроз.

Особенностью информационной системы с гипервизором является возможность провести атаку на сетевой ресурс за счет трансляции трафика через сетевой интерфейс сервера, существенно снизив при этом риск обнаружения атаки. Этому процессу соответствует наличие ветви $(l_{11}, l_6, l_3, l_1, l_0)$ на графе дерева атак.

В алгоритме моделирования процесса MITM-атака—защита учитывались разветвленная конфигурация системы защиты и случайный характер параметров системы защиты и параметров проведения атаки. Для расчета вероятности успешной атаки на защищенный ресурс использовались статистические данные о совершении атак на информационные системы, приведенные в [4]; при этом первоначально предполагалось, что параметры атак и защиты имеют равномерное распределение.

В соответствии с алгоритмом разработанного метода начало атаки может реализовываться воздействием на одну из начальных (листовых) вершин дерева атак, множество которых

$$P\left(P_{0,m}\right) = \left\{ \begin{matrix} P_{0,1}, P_{0,2}, P_{0,3}, P_{0,4}, \\ P_{0,5}, P_{0,6}, P_{0,7}, P_{0,8}, P_{0,9} \end{matrix} \right\}, \qquad (3)$$

где "0" — индекс вектора исходных вершин маршрутов атак; $m = R0$ — номер маршрута проведения атаки; $R0$ — случайное число с равномерным распределением, $R0 = \{1, 2, \ldots, 9\}$, т. е. выбор начальной вершины маршрута атаки имеет случайный характер и задается генератором случайных чисел.

Параметр квалификации атакующего для каждой моделируемой атаки задается количеством маркеров в исходной вершине маршрута $\mu_{0,m}$. В соответствии с принятым алгоритмом работы системы

$$\mu_{0,m} = R1_m, \qquad (4)$$

где $R1_m$ — случайная величина с равномерным распределением ($1 \le R1_m \le 100$ с шагом $\Delta R1_m = 1$). В соответствии с [1] атакующие по степени квалификации распределяются следующим образом: 41 % имеет низкую квалификацию, 43 % — среднюю, а 16 % — высокую. Это было учтено при создании алгоритма моделирования: при $1 \le R1_m \le 41$ предполагалось, что атакующий имеет низкую квалификацию; при $42 \le R1_m \le 84$ — среднюю квалификацию; при $85 \le R1_m \le 100$ — высокую квалификацию. Разыгранное значение параметра $R1_m$ для каждого маршрута атаки с индексом "m" функционально влияет на время срабатывания переходов данного маршрута $\tau_{j,m}$, где j — индекс перехода по маршруту.

Таким образом, исходное состояние для проведения атаки по маршруту с индексом "m" опреде-

ляется комбинацией двух случайных чисел: $P_{0,m}(R0, R1_m)$. Попадая на случайную листовую вершину дерева, атакующий с учетом своей квалификации может реализовать успешную атаку, пройдя по определенному маршруту до его корня.

В соответствии с алгоритмом модели для совершения перехода от одной вершины дерева к другой атакующему необходимо выполнить ряд действий некоторой сложности, занимающих определенное время. Результирующее время срабатывания каждого перехода $\tau_{j,m}$ определяется значениями трех параметров: сложностью проводимой атаки, квалификацией атакующего и собственно временем проведения атаки:

$$\tau_{j,m} = k2_{j,m} R2_{j,m} + k3_{j,m} R3_{j,m} + k4_{j,m} R4_{j,m}, \quad (5)$$

где $R2_{j,m}$, $R3_{j,m}$, $R4_{j,m}$ — случайные величины, определяющие сложность проводимой атаки, квалификацию атакующего с точки зрения решения текущей задачи и процедуру эксплуатации уязвимости; $k2_{j,m}$, $k3_{j,m}$, $k4_{j,m}$ — весовые коэффициенты соответствующих параметров атаки.

Момент возникновения атаки задавался случайной величиной $R5 = \{1, 2, \ldots, 10000\}$, полученной из распределения интенсивности проведения атак на ресурс с учетом характеристик его информации [5].

Проведенный анализ статистической информации о получении несанкционированного доступа к информационным системам показывает, что экономически оправданное время, затрачиваемое на компрометацию ресурса, в среднем составляет 7 рабочих дней; статистика, приведенная в [1], была использована для определения масштаба времени при моделировании процессов компрометации защищенного ресурса.

Применительно к математическому аппарату сетей Петри процедура отыскания и эксплуатации уязвимости на переходе $t_{j,m}$ соответствует времени его срабатывания. При этом сложность атаки характеризуется кратностью входной дуги этого перехода $I(t_{j,m})$:

$$\left|I(p_{j,m})\right| = \left|\left\{t_{j,m} \middle| p_{j,m} \in O(t_{j,m})\right\}\right|, \quad (6)$$

где $I(p_{j,m})$ — кратность входной дуги состояния $p_{j,m}$;

$O(t_{j,m})$ — кратность выходной дуги перехода $t_{j,m}$.

Квалификация атакующего определяется кратностью выходной дуги каждого перехода $O(t_{j,m})$, а срабатывание перехода $t_{j,m}$ может быть реализовано только при выполнении условия

$$\mu(p_{i,m}) \geq \#(p_{j,m}, I(t_{j,m})), \quad (7)$$

где $\mu(p_{j,m})$ — случайное число маркеров в состоянии, предшествующем переходу $t_{j,m}$, зависящее от числа выходных дуг предыдущего перехода $O(t_{j-1,m})$ и от числа циклов, определяющих срабатывание предыдущего перехода $t_{j-1,m}$. Поэтому процедура эксплуатации уязвимости определяется числом циклов программы, при которых $\mu(p_{i,m}) < \#(p_{j,m}, I(t_{j,m}))$.

Кратность входной дуги перехода $I(t_{j,m})$ задавалась генератором случайных чисел $R2_{j,m}$:

$$I(t_{j,m}) = R2_{j,m}, \quad (8)$$

а кратность выходной дуги перехода $O(t_{j,m})$ определялась квалификацией атакующего:

$$O(t_{j,m}) = R3_{j,m}. \quad (9)$$

Количество необходимых процедур N_n для выполнения условия (7)

$$N_n = R4_{j,m}. \quad (10)$$

Таким образом, при моделировании процесса атака-защита с использованием математического аппарата расширенных сетей Петри выполнялось разыгрывание шести случайных величин, $R0, R1_m, R2_{j,m}, R3_{j,m}, R4_{j,m}, R5$, имеющих различные законы распределения.

В соответствии с разработанным алгоритмом было выполнено моделирование динамического процесса атаки на ресурс с указанными типами защит. При моделировании был принят "уровень доверия" $\varepsilon = 0{,}03$, что обеспечивалось числом розыгрышей в каждом варианте защиты L = 65300.

В качестве базовой системы защиты, успешная атака на которую может быть реализована за контрольное время 168 ч, принят стандартный комплекс мер на основе мониторинга сетевых процес-

сов и разграничения прав доступа к ресурсам без использования специализированного анализирующего или защитного ПО.

Результаты моделирования процессов при проведении MITM-атаки в случае использования средств защиты сетевого ресурса показали, что на момент контрольного времени (168 ч) вероятность защиты от несанкционированного доступа к информации составила 0,14 (рис. 4). Поскольку сервер и гипервизор ресурса не получили дополнительной защиты, время доступа к ним не меняется по сравнению с базовой системой защиты.

В случае, если ресурс использует комплекс защитных средств и ПО для обеспечения конфиденциальности файлов, на момент контрольного времени вероятность защиты от несанкционированного доступа к информации составляет 0,12, а время доступа к гипервизору увеличивается на 2 ч (3 %) по сравнению с базовой системой.

Наиболее эффективной системой защиты информации оказывается комплекс защитного ПО для сервера. Его использование увеличивает вероятность защиты за контрольное время до 0,2, при этом хост оказывается доступен атакующему через 90 ч, а гипервизор — через 120 ч. Ориентировочное время доступа к информации составит 240 ч.

Использование средств обеспечения безопасности сетевой инфраструктуры ресурса оказалось наименее эффективным средством защиты. К контрольному времени информация будет защищена с вероятностью 0,1; время доступа к хосту составляет 67 ч, а к гипервизору — 90 ч.

В завершение были выполнены расчеты вероятности обеспечения конфиденциальности информации ресурса при комплексной защите, т. е. использовании всех четырех типов рассмотренных защит (рис. 4). Результаты показали, что в этом случае за контрольное время информация будет защищена с вероятностью 65 %.

Таким образом, разработана методика, позволяющая оценить эффективность применяемой защиты для ИК любой структуры. Это подтверждается сопоставлением полученных расчетных рисков для информационной системы с результатами тестирования, проведенного компанией Positive Technologies. Рассмотренная методика может быть рекомендована для использования разработчиками систем защиты информационных комплексов.

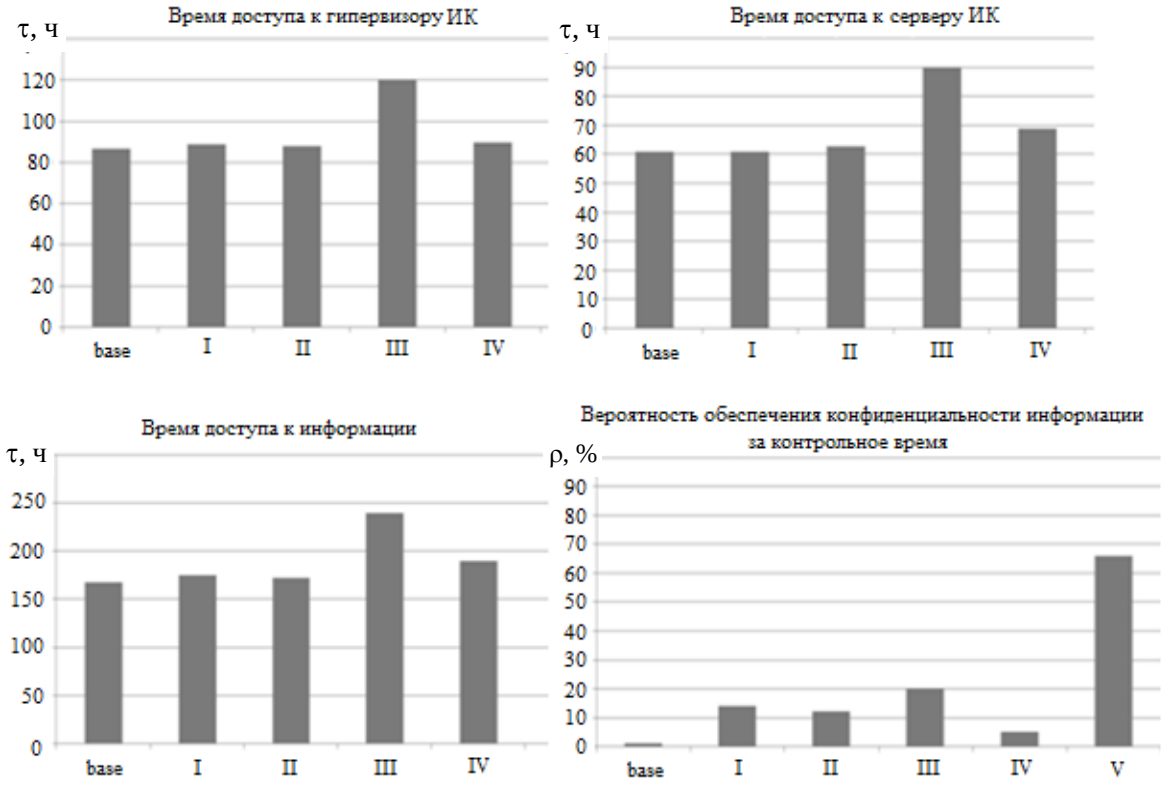

Рис. 4. Вероятностные характеристики защиты ресурса при проведении MITM-атаки при различных системах используемой защиты:

Base— стандартный комплекс мер на основе мониторинга сетевых процессов и разграничения прав доступа к ресурсам без использования специализированного анализирующего или защитного ПО;
I — защита ресурса; II — защита файловой системы; III — защита сервера;
IV — средства обеспечения безопасности сетевой инфраструктуры;
V — комплексная защита, включающая I, II, III и IV типы защит

Литература

1. Статистика уязвимостей корпоративных информационных систем за 2011—2012 годы: аналитический отчет. — М.: Positive Technologies, 2013. URL: http://www.ptsecurity.ru/download/Analitika_pentest.pdf

2. *Лескин А. А., Мальцев П. А., Спиридонов А. М.* Сети Петри в моделировании и управлении . — Л.: Наука, 1989. — 133 с.

3. *Ермаков С. М.* Метод Монте-Карло в вычислительной математике. — СПб.: Невский Диалект. Бином. Лаборатория знаний, 2009. — 192 с.

4. *Коллегов Д. Н.* Проблемы синтеза и анализа графов атак // Вестник Томского ун-та. Приложение. 2007. № 23. С. 180—188.

5. *Соловьев В. П., Корнев Д. А.* Влияние характеристик источника информации на вероятность проведения атак // Вопросы защиты информации. 2014. № 2 (106). С. 37—43.

Calculation of information system's risk in terms Petri nets

D. A. Kornev
Moscow Technological Institute, Moscow, Russia

The paper presents a methodology for calculating the probability of loss of confidentiality of the information on a secure computing resources, allowing to get a good agreement with the statistics of corporate information systems vulnerabilities. To implement the methodology used mathematical apparatus of colored Petri nets and the method of statistical tests (Monte Carlo). Calculated the probability of confidentiality resource information with cryptographic protection of information in MITM-attack and the five major types of resource protection.

Keywords: computer system, mathematical model, information system risks, MITM attack, Petri nets.

Bibliography — 5 references. *Received September 19, 2016*