9 МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

УДК 004.056

МЕТОДИКА АНАЛИЗА АРХИТЕКТУРЫ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ТИПОВЫХ ЭЛЕМЕНТОВ

М.Е. Сухопаров, И.Н. Соловьев, И.С. Лебедев, И.И. Комаров

Предложен метод анализа архитектуры системы защиты информации на основе типовых элементов. Подход основан на использовании вероятностных характеристик типовых элементов защиты, учитывает поток событий для одного типового элемента системы защиты информации, что позволяет производить сравнительный анализ и обоснование выбора архитектуры на ранних этапах жизненного цикла. Приведен пример анализа архитектуры системы.
Ключевые слова: анализ архитектур СЗИ, выбор архитектуры, оценка уязвимости.

Введение

Повсеместное использование глобальных вычислительных сетей, систем распределенных вычислений, облачных технологий, появление элементов «открытого контура» в системах управления, где необходимо обеспечение конфиденциальности, целостности и доступности циркулирующих данных, обусловливает важность задач защиты информационно-телекоммуникационных объектов.

Развитие современных технологий проектирования и возрастающие возможности средств передачи информации дают возможность реализовывать различные топологии информационных систем, оптимизированные для решения предметно ориентированных задач, что требует прогнозной оценки показателей качества обеспечения информационной безопасности на различных стадиях жизненного цикла [1].

Общий подход к построению защиты информационных объектов состоит в том, чтобы для каждой угрозы внедрить решение, которое снизит вероятность ее реализации до приемлемого уровня. Особенностью современных средств обеспечения информационной безопасности является многоуровневый принцип защиты, где злоумышленнику для осуществления угроз конфиденциальности, целостности и доступности необходимо преодолеть разные элементы [2].

Постановка задачи

Широкое распространение типовых средств защиты информации известных производителей ведет к увеличению активности по поиску существующих в них уязвимостей [3]. Если одно из таких средств недостаточно снижает риски, то внедряются несколько решений разных разработчиков.

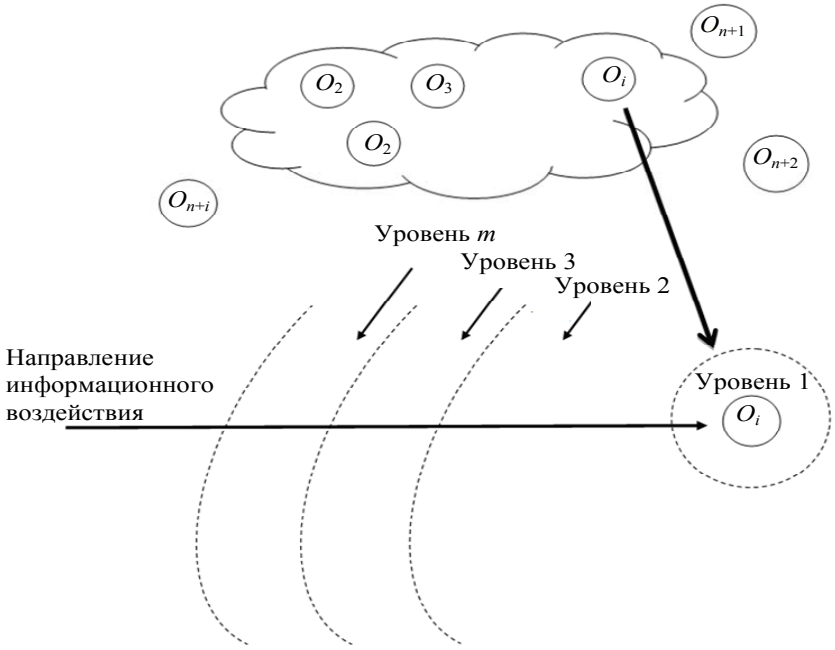

Рис. 1. Структура защищаемого объекта

Например, для информационно-телекоммуникационных систем, имеющих доступ в Интернет, устанавливаются различные антивирусы на шлюз, почтовый сервер и рабочие станции. Удаленные и мо-

бильные рабочие места, имеющие доступ к информационным ресурсам информационно-телекоммуникационной системы (ИТКС), оснащаются средствами защиты, рекомендованными администраторами политики безопасности. Таким образом, в системе появляется регламентированный набор средств защиты. В связи с этим возникает ряд задач, связанных с оценкой заданных показателей защищенности объектов.

Рассмотрим систему защиты распределенных ресурсов S, где для каждого защищаемого объекта $o_i \in O$ подсистема защиты может состоять из набора элементов системы защиты информации (СЗИ) из $m_i \in M$. В качестве примера можно привести систему, препятствующую утечке, например, текстовых документов. Преодоление элементов СЗИ, обрабатывающих текстовую информацию, может быть связано с уязвимостями, возникающими вследствие несовершенства алгоритмов обработки текстовой информации на морфологическом, синтаксическом и семантическом уровнях, с применением средств примитивного кодирования, использованием псевдографики в отправляемых и принимаемых сообщениях, систем программирования, содержащихся в обычных текстовых редакторах и офисных приложениях. Исходя из этого, необходимо учитывать широкий спектр возможностей, имеющихся у потенциального нарушителя, и использовать разнообразные элементы защиты на разных уровнях.

На рис. 1 представлен защищаемый информационно-технический объект. Особенностью преодоления защиты является возможность не только прямого воздействия на последовательные уровни защиты элементов СЗИ, но поиск уязвимостей в каждом элементе защиты по отдельности.

Предлагаемый подход

Допустим, что в ИТКС осуществляются процессы информационного противоборства, одной из составляющих которого являются атаки на лингвистический модуль определения данных, содержащих конфиденциальную информацию центрального сервера управления DLP-системы [4]. Исследуя систему, возможно определить уязвимости, связанные с несовершенством алгоритмов морфологического, синтаксического, семантического уровней обработки естественного языка, которые с определенной вероятностью позволят преодолеть средства защиты, осуществляющие идентификацию информации сообщений [5]. Например, для лингвистического модуля определения данных использование методов примитивного кодирования дает возможность обойти подсистемы поиска по точному совпадению слов с учетом морфологии, анализа регулярных выражений, но должно быть обнаружено при идентификации цифровых отпечатков или подсистемой поведенческого анализа. При посылке различных видов потенциально опасных сообщений в зависимости от свойств информации могут быть преодолены одни типовые элементы и в то же время обнаружена угроза другими [6].

Обозначим λ – количество преодолений типового элемента СЗИ в единицу времени t. Для упрощения модели будем считать, что для одного типового элемента СЗИ поток событий обладает свойствами стационарности, отсутствия последействия и ординарности. Событие преодоления одного элемента защиты зависит только от длины временного промежутка, в течение которого приходится обрабатывать текстовые сообщения. Событие преодоления одного элемента защиты не зависит в любом промежутке времени от того, появлялись события в прошлом или нет. Появление более одного события за малый промежуток времени практически невозможно. Вероятность того, что произойдет преодоление n типовых элементов СЗИ, будет определяться как

$$p(n) = \frac{(\lambda t)^n}{n!} e^{-\lambda t}.$$

Одной из задач построения СЗИ является получение количественных оценок, позволяющих производить сравнение и выбор элементов систем, а также выносить обоснованное решение об использовании той или иной архитектуры.

Допустим, что система состоит из типовых элементов. Для определения архитектуры необходимо определить их требуемое количество.

Введем порог $l < N$, показывающий предельно допустимый уровень преодоленных элементов. Вероятность того, что в течение времени t не менее l элементов СЗИ будут преодолены, равна

$$p(n \ge l) = 1 - \sum_{n=1}^{l} \frac{(\lambda t)^n}{n!} e^{-\lambda t}.$$

На рис. 2 приведены зависимости для λ=1 при значениях n и l, равных (12 и 8), (10 и 7), (15 и 10) соответственно.

На рис. 3 приведены зависимости для различных λ при значениях n и l, равных (12 и 8), (10 и 7), (15 и 10) соответственно и периода времени t = 1.

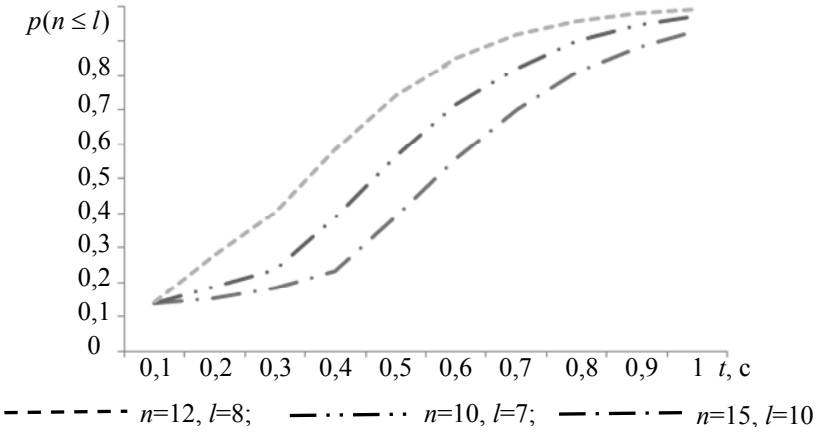

Рис. 2. Вероятность преодоления защиты в течение периода времени t

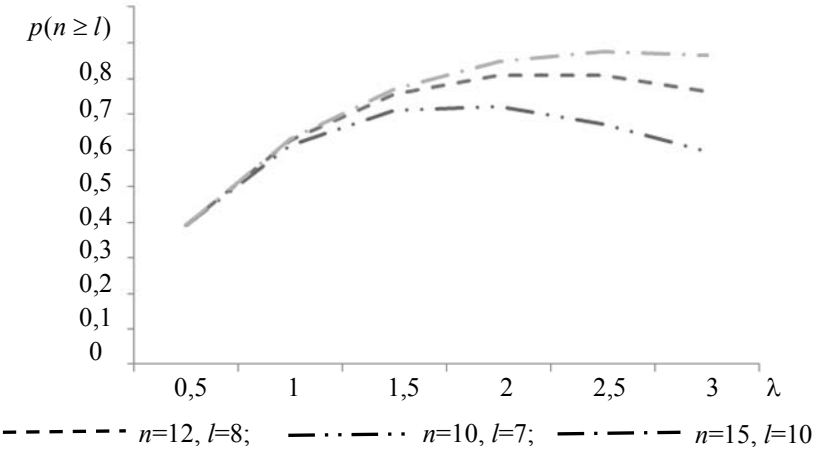

Рис. 3. Вероятность преодоления защиты при различных интенсивностях

С другой стороны, данный подход позволяет сравнивать архитектуры СЗИ. Поясним подход на примере. Пусть для последнего рассмотренного случая необходимо выбрать структурную схему, позволяющую потенциально достигать наибольшие показатели защищенности.

Допустим, что необходимо обосновать создание последовательности из элементов СЗИ по первому или второму типу в зависимости от статистических показателей, характеризующих преодоление. Для этого составляем отношение

$$\frac{p(n \ge l_1)}{p(n \ge l_1)} = \frac{1 - \sum_{n=1}^{l_1} \frac{(\lambda t)^n}{n!} e^{-\lambda t}}{1 - \sum_{n=1}^{l_2} \frac{(\lambda t)^n}{n!} e^{-\lambda t}}$$

На рис. 4 показаны отношения вероятностей непреодоления защиты различных архитектур.

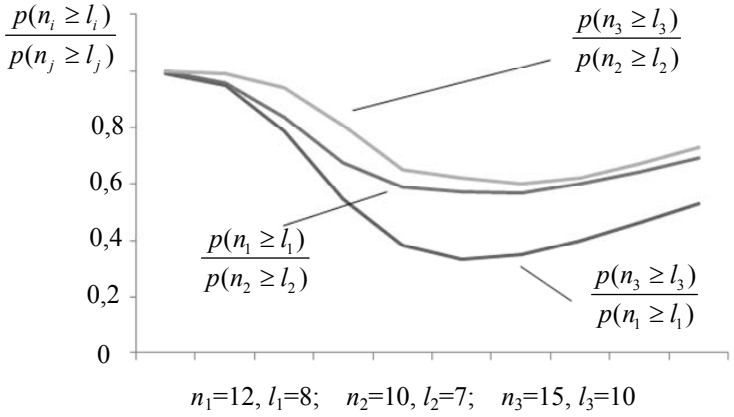

Рис. 4. Отношения вероятностей непреодоления защиты различных архитектур

Анализ зависимости показывает предпочтение той или иной архитектуры в зависимости от интенсивности отказов элементов СЗИ.

Заключение

Широкое распространение типовых средств защиты информации известных производителей, их постоянный анализ с целью преодоления со стороны субъектов информационного противоборства обусловливает необходимость развития прогнозных методов, основанных на технических характеристиках отдельных элементов системы защиты информации.

В работе продемонстрирована возможность применения метода анализа архитектуры систем защиты информации на основе типовых элементов для решения типовой задачи анализа и оценки заданных показателей защищенности объектов, зависящих от выбора элементов системы защиты информации.

Предложенный метод обеспечивает возможность формальной оценки преимуществ разных архитектур, определяющих свойства системы защиты информации, получить прогнозные результаты расчетов для оценки системы защиты информации, выделить наиболее уязвимые элементы системы защиты информации и определить направления повышения защищенности системы.

Работа выполнена в рамках НИР № 12360.

Литература

1. Гвоздев А.В., Зикратов И.А., Лебедев И.С., Лапшин С.В., Соловьев И.Н. Прогнозная оценка защищенности архитектур программного обеспечения // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 126–130.
2. Зикратов И.А., Одегов С.В. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 4 (80). – С. 121–126.
3. Лебедев И.С., Борисов Ю.Б. Анализ текстовых сообщений в системах информационной безопасности. // Информационно-управляющие системы. – 2011. – № 2 (51). – С. 37–43.
4. Артамонов В.А. Модели безопасности информационных технологий критичных информационно-измерительных систем [Электронный ресурс]. – Режим доступа: http://itzashita.ru/publications/modeli-bezopasnosti-informacionnyx-texnologij-kritichnyx-informacionno-izmeritelnyx-sistem-chast-1.html, свободный. Яз. рус. (дата обращения 26.02.2013).
5. Manning C.D., Raghavan P., Schutze H. Introduction to Information Retrieval. – Cambrige University Press, Cambrige, England. – 2009. – 504 p.
6. Медведовский И.Д., Семьянов П.В., Леонов Д.Г., Лукацкий А.В. Атака из Internet. – М.: Солон-Р, 2002. – С. 140–144.

Сухопаров Михаил Евгеньевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, sukhoparovm@gmail.com

Соловьев Игорь Николаевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, аспирант, solovyev.i.n@yandex.ru

Лебедев Илья Сергеевич – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, доктор технических наук, доцент, lebedev@cit.ifmo.ru

Комаров Игорь Иванович – Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, кандидат физ.-мат. наук, доцент, Komarov@cit.ifmo.ru