УДК 681.3.06

ПОСТРОЕНИЕ ЛОГИКО-ВЕРОЯТНОСТНОЙ МОДЕЛИ ЗАЩИЩЕННОЙ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Алексей Новиков, Андрей Тимошенко*

*Физико-технический институт НТУУ «КПИ», *ООО «Институт компьютерных технологий»*

Анотація: **Розглянуто питання побудови логико-імовірнісної моделі захищеної комп'ютерної системи з відкритою архітектурою і багаторівневим стеком протоколів, придатної для використання в процесі аналізу ризиків, пов'язаних з реалізацією різних загроз інформації і вибору механізмів захисту від цих загроз.**

Summary: **The problems of construction of a logical-probability model of the secured computer system with open architecture and multilevel stack of the protocols, suitable for use during the threat's risks analysis and the protection mechanism's choice are considered.**

Ключові слова: **Загроза інформації, аналіз ризиків, логико- імовірностна модель.**

Актуальность проблемы применения метода логико-вероятностного моделирования (ЛВМ) в процессе построения системы защиты информации (СЗИ), обрабатываемой в компьютерной системе (КС) с открытой архитектурой и многоуровневым стеком протоколов, объясняется рядом причин. Во-первых, это необходимость, согласно действующим в Украине нормативным документам в области технической защиты информации [1], проведения анализа угроз информации, обрабатываемой в КС, оценки вероятности реализации данных угроз и величины возможного ущерба, а также оценки рисков, связанных с их реализацией, как функции вероятности и величины возможного ущерба с последующим выбором включаемых в СЗИ средств защиты на основании полученных результатов. Во-вторых, это отсутствие в действующих в Украине нормативных документах утвержденных методик анализа рисков, связанных с реализацией угроз информации, обрабатываемой в КС. В-третьих, это наличие у известных методик [2, 3] ряда недостатков, таких, как слабая формализация, необходимость привлечения грамотных экспертов и т. п. И, наконец, в-четвертых, это стремительное расширение сферы применения КС с открытой архитектурой.

Проблемы оценки вероятности отказов различных компонентов систем и анализа рисков, связанных с их реализацией, достаточно хороши исследованы [4] в ходе решения задач обеспечения безопасности структурно-сложных систем (ССС), под которыми понимаются сложные технические системы различной природы (объекты энергетики, транспорта и т.п.). Одним из эффективных направлений в теории безопасности ССС (не только технических, но и организационно-технических) можно признать логико-вероятностную теорию (ЛВТ) безопасности [5], основным понятием в которой является понятие опасного состояния системы (ОСС) и соответствующей логической функции опасности системы (ФОС). Рассматривая КС с открытой архитектурой как частный случай ССС, проанализируем возможность использования аппарата ЛВТ безопасности (применения метода ЛВМ) при построении СЗИ, обрабатываемой в КС. Согласно [6], при решении задач обеспечения безопасности ССС в качестве параметров ФОС ССС используются булевы переменные, характеризующие факт наличия соответствующих инициирующих условий (ИУ) аварии, а также факт работоспособности элементов ССС. В процессе перехода к вероятностной модели данные переменные заменяются соответствующими вероятностями возникновения ИУ аварии и вероятностями сохранения работоспособности элементов ССС. Для построения ФОС и последующего перехода к вероятностной модели КС необходимо определить, какие характеристики будут моделироваться, а также какие параметры КС и каким образом будут учитываться в модели.

В качестве моделируемой характеристики предлагается использовать вероятность сохранения защищенности информации, обрабатываемой в КС. При этом в качестве ИУ нарушения безопасности функционирования моделируемой КС предлагается использовать попытки реализации угроз информации. Для этого в набор параметров модели должны быть включены вероятностные характеристики реализации данных угроз. Так нас интересует рассмотрение КС с точки зрения возможности обеспечения защиты от угроз информации, то в качестве элементов моделируемой защищенной КС необходимо рассматривать механизмы защиты, реализующие различные услуги безопасности на различных уровнях стека протоколов, а в качестве вероятности работоспособности элементов системы использовать вероятность предотвращения данными механизмами защиты тех или иных угроз информации.

Для проведения логико-вероятностного моделирования функционирования КС с учетом попыток реализации различных угроз информации (атак), выступающих в качестве ИУ, необходимо определить вероятностные характеристики различных угроз. Поскольку угрозы информации, обрабатываемой в КС,

относятся к классу так называемых «редких» событий, использование для оценки вероятности их реализации классических методов определения относительных частот событий при длительных испытаниях невозможно. Поэтому предлагается в качестве вероятностной оценки угроз, используемой в процессе логико-вероятностного моделирования защищенной КС, использовать показатель эффективности реализации угрозы информации, отражающий в себе как статистические характеристики реализации угрозы, так и привлекательность угрозы с точки зрения реализации конечных целей злоумышленника и определяемый следующим образом:

$$E_{ij} = Q_{ij} R_{ij} \tag{1}$$

где Q_{ij} – показатель, характеризующий долю (величину), вносимую i-й угрозой информации, реализованной на протоколе j-го уровня КС, в суммарный выходной эффект действий злоумышленника; R_{ij}– показатель, характеризующий статистическую вероятность реализации i-й угрозы информации, реализованной на протоколе j-го уровня КС.

Для оценки значений показателей Q_{ij} можно использовать, например, методы теории принятия решений, а для оценки показателя R_{ij} – публикуемые различными организациями статистические данные об инцидентах с безопасностью в различных распределенных сетях, например, в Internet.

Фактически, эффективность реализации угрозы информации, представленная в виде (1), представляет собой показатель оценки риска, связанного с реализацией данной угрозы информации.

Согласно [7, 8] функционирующий на каком-либо уровне стека протоколов и реализующий услугу безопасности, обеспечивающую защиту от угроз определенного типа (конфиденциальности, целостности или доступности), механизм защиты информации обеспечивает защиту от угроз того же типа, реализованных как на данном, так и на более высоких уровнях стека протоколов. С точки зрения построения логико-вероятностной модели это означает, что для защиты от угрозы информации, реализуемой на протоколе j-го уровня, в КС должен быть реализован соответствующий механизм защиты на j-м или более низких уровнях стека протоколов. Работоспособность механизма защиты означает возможность предотвращения с его помощью (в случае его наличия) определенной угрозы информации. Приняв допущение о том, что, в случае наличия механизм защиты всегда обеспечивает предотвращение угрозы информации, для защиты от которой он предназначен, мы можем использовать в качестве оценки вероятности предотвращения реализованными в СЗИ механизмами защиты тех или иных угроз информации параметр M_{ij}, определяющий факт наличия механизма защиты от i-й угрозы на протоколе j-го уровня и принимающий значение 1 в случае наличия данного механизма и значение 0 в случае его отсутствия.

Поскольку конечной целью использования метода ЛВМ является выбор для включения в СЗИ не только оптимального с точки зрения обеспечения максимальной вероятности сохранения защищенности информации, но и приемлемого по стоимости набора механизмов защиты, это ограничение необходимо учитывать в процессе моделирования. Ограничение по стоимости средств защиты, включаемых в СЗИ, можно записать следующим образом:

$$\sum_{i=1}^{L}\left(\sum_{j=1}^{N} M_{ij} \cdot C_{ij}\right) \le C_0 \tag{2}$$

где L – количество потенциальных угроз информации, обрабатываемой в КС; N – количество уровней стека протоколов КС; M_{ij} – параметр, значение которого определяет факт наличия/отсутствия механизма защиты от i-й угрозы на протоколе j-го уровня; C_{ij} – стоимость реализации механизма защиты от i-й угрозы на протоколе j-го уровня; C_o – максимальное значение затрат на реализацию системы защиты.

С учетом изложенного, построим логико-вероятностную модель и определим вероятностную функцию оценки защищенности информации в компьютерной системе с двухуровневым стеком протоколов. Согласно методике, изложенной в [6], в процессе построения логико-вероятностной модели последовательно должны быть построены:

- содержательное описание модели поведения (развития опасного состояния) КС;
- описание сценария поведения (развития опасного состояния) моделируемой КС на языке продукций (логических высказываний);
- структурная граф-схема (граф-модель) развития опасного состояния моделируемой КС, позволяющая осуществить событийно-логическое описание ее функционирования;
- логическая модель КС в виде логической ФОС, аргументами которой должны быть простые бинарные события, собственные вероятностные параметры которых известны;
- вероятностная модель КС, позволяющая выполнять непосредственные расчеты требуемых вероятностных характеристик.

Содержательное описание модели поведения КС выглядит следующим образом.

Успешная реализация угрозы информации в КС произойдет в случае если:

1) отсутствует попытка реализации угрозы информации на верхнем уровне стека протоколов, имеется попытка реализации угрозы информации на нижнем уровне стека протоколов и отсутствуют средства защиты на нижнем уровне стека протоколов;

2) имеется попытка реализации угрозы информации на верхнем уровне стека протоколов, отсутствует попытка реализации угрозы информации на нижнем уровне стека протоколов и не реализованы механизмы защиты как на верхнем, так и на нижнем уровне стека протоколов;

3) имеется попытка реализации угрозы информации как на верхнем, так и на нижнем уровне стека протоколов и не реализованы механизмы защиты как на верхнем, так и на нижнем уровне стека протоколов;

4) имеется попытка реализации угрозы информации как на верхнем, так и на нижнем уровне стека протоколов, реализованы механизмы защиты на верхнем уровне стека протоколов и не реализованы механизмы защиты на нижнем уровне стека протоколов.

Для составления сценария развития опасного состояния на языке продукций (логических высказываний) выделим в выше приведенном содержательном описании модели поведения:

-факты–события, связанные с наличием/отсутствием попыток реализации угроз информации – заглавными буквами (и идентификаторами X/ X' с индексами для использования в граф-схеме);

-факты–события, связанные с наличием/отсутствием реализованных механизмов защиты – заглавными буквами (и идентификаторами Y/ Y' с индексами для использования в граф-схеме);

-факты–события, связанные с успешной реализацией угрозы информации – заглавными буквами (и идентификаторами F с индексами для использования в граф-схеме);

-союзы «и», «или» как отношения заглавными буквами И, ИЛИ.

Сценарий развития опасного состояния моделируемой КС имеет следующий вид.

Правило 1. УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ (F) имеет место
ЕСЛИ имеет место УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ НА НИЖНЕМ УРОВНЕ (F_1)
ИЛИ имеет место УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ НА ВЕРХНЕМ УРОВНЕ (F_2)
ИЛИ имеет место УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ НА ОБЕИХ УРОВНЯХ (F_{12});

Правило 2. УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ НА НИЖНЕМ УРОВНЕ (F_1) имеет место
ЕСЛИ имеет место ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА НИЖНЕМ УРОВНЕ (X_1)
И отсутствует ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА ВЕРХНЕМ УРОВНЕ (X_2')
И отсутствуют МЕХАНИЗМЫ ЗАЩИТЫ НА НИЖНЕМ УРОВНЕ (Y_1');

Правило 3. УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ НА ВЕРХНЕМ УРОВНЕ (F_2) имеет место
ЕСЛИ отсутствует ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА НИЖНЕМ УРОВНЕ (X_1')
И имеет место ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА ВЕРХНЕМ УРОВНЕ (X_2)
И отсутствуют МЕХАНИЗМЫ ЗАЩИТЫ НА НИЖНЕМ УРОВНЕ (Y_1')
И отсутствуют МЕХАНИЗМЫ ЗАЩИТЫ НА ВЕРХНЕМ УРОВНЕ (Y_2');

Правило 4. УСПЕШНАЯ РЕАЛИЗАЦИЯ УГРОЗЫ НА ОБЕИХ УРОВНЯХ (F_{12}) имеет место
ЕСЛИ имеет место ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА НИЖНЕМ УРОВНЕ (X_1)
И имеет место ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА ВЕРХНЕМ УРОВНЕ (X_2)
И отсутствуют МЕХАНИЗМЫ ЗАЩИТЫ НА НИЖНЕМ УРОВНЕ (Y_1')
И отсутствуют МЕХАНИЗМЫ ЗАЩИТЫ НА ВЕРХНЕМ УРОВНЕ (Y_2')
ИЛИ
ЕСЛИ имеет место ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА НИЖНЕМ УРОВНЕ (X_1)
И имеет место ПОПЫТКА РЕАЛИЗАЦИИ УГРОЗЫ НА ВЕРХНЕМ УРОВНЕ (X_2)
И отсутствуют МЕХАНИЗМЫ ЗАЩИТЫ НА НИЖНЕМ УРОВНЕ (Y_1')
И имеются МЕХАНИЗМЫ ЗАЩИТЫ НА ВЕРХНЕМ УРОВНЕ (Y_2).

Структурная граф-схема развития опасного состояния моделируемой КС с двухуровневым стеком протоколов имеет вид, приведенный на рис. 1.

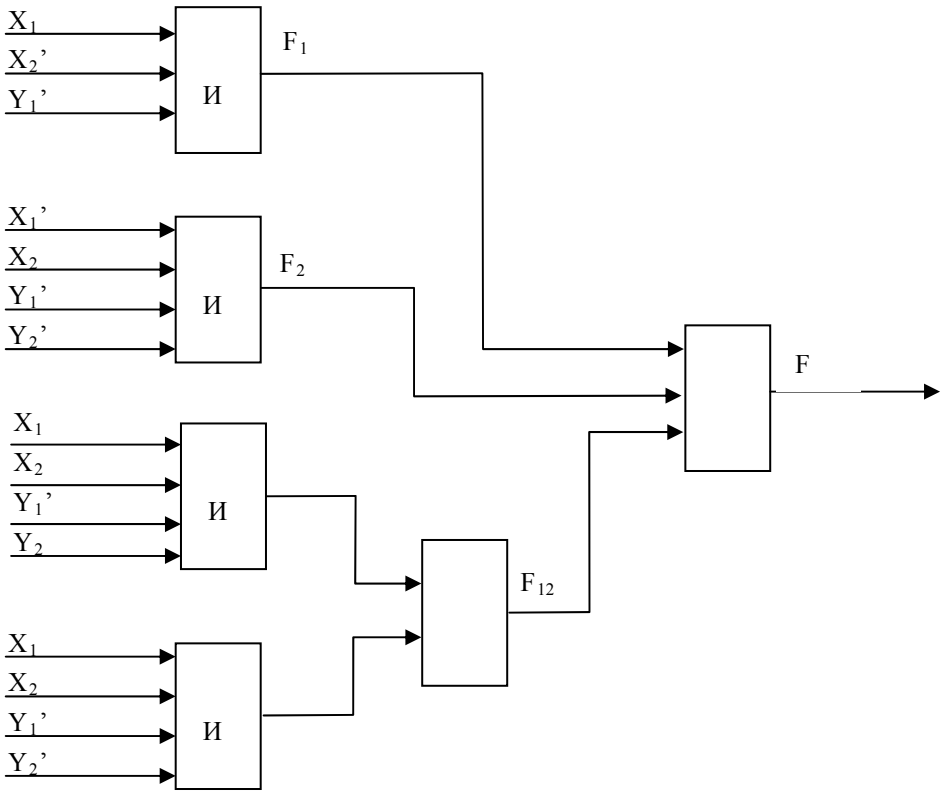

Рисунок 1 – Структурная граф-схема развития опасного состояния в КС

На основании приведенной структурной граф-схемы получим выражение для логической ФОС с двухуровневым стеком протоколов:

$$\begin{aligned} F &= F_1 \vee F_2 \vee F_{12} = X_1 \cdot X_2' \cdot Y_1' \vee X_1' \cdot X_2 \cdot Y_1' \cdot Y_2' \vee X_1 \cdot X_2 \cdot Y_1' \cdot Y_2 \vee X_1 \cdot X_2 \cdot Y_1' \cdot Y_2' = \\ &= X_1 \cdot X_2' \cdot Y_1' \vee X_1' \cdot X_2 \cdot Y_1' \cdot Y_2' \vee X_1 \cdot X_2 \cdot Y_1' \cdot (Y_2 \vee Y_2') = \\ &= X_1 \cdot X_2' \cdot Y_1' \vee X_1' \cdot X_2 \cdot Y_1' \cdot Y_2' \vee X_1 \cdot X_2 \cdot Y_1' = X_1 \cdot Y_1' \cdot (X_2 \vee X_2') \vee X_1' \cdot X_2 \cdot Y_1' \cdot Y_2' = \\ &= X_1 \cdot Y_1' \vee X_1' \cdot X_2 \cdot Y_1' \cdot Y_2'. \end{aligned} \tag{3}$$

Таким образом, окончательное выражение логической модели КС с двухуровневым стеком протоколов (в виде логической ФОС) имеет вид:

$$F = X_1 \cdot Y_1' \vee X_1' \cdot X_2 \cdot Y_1' \cdot Y_2' \tag{4}$$

где X_1 – переменная (X_1’ – ее инверсия), характеризующая факт реализации угрозы на протоколе нижнего уровня (0 – нет угрозы, 1 – есть угроза); X_2 – переменная (X_2’ – ее инверсия), характеризующая факт реализации угрозы на протоколе верхнего уровня (0 – нет угрозы, 1 – есть угроза); Y_1 – переменная (Y_1’ – ее инверсия), характеризующая факт реализации механизмов защиты на протоколе нижнего уровня (0 – нет, 1 – есть); Y_2 – переменная (Y_2’ – ее инверсия), характеризующая факт реализации механизмов защиты на протоколе верхнего уровня (0 – нет, 1 – есть);

Выражение (4) представляет собой дизъюнктивную нормальную форму со взаимно ортогональными членами и, согласно доказанной в вероятностной логике теореме замещения [9], может быть преобразована в функцию вычисления вероятности реализации опасного события путем замены логических переменных вероятностями их реализации, отрицаний логических переменных – на единица минус вероятность реализации, логических сложений и логических умножений – их арифметическими аналогами. Учитывая, что в нашем случае вместо понятия вероятности используется понятие эффективности реализации угрозы информации и обозначая через E_i оценку эффективности реализации угрозы информации на i-м уровне протокола, а через M_i вероятность предотвращения угрозы информации механизмом защиты, реализованным на i-м уровне протокола (которая определяется фактом наличия соответствующих механизмов и может принимать только значение 0 и 1), получим следующее выражение:

$$T_2 = E_1\left(1 - M_1\right) + \left(1 - E_1\right)E_2\left(1 - M_1\right)\left(1 - M_2\right) \quad (5)$$

Таким образом, вероятностная модель КС с двухуровневым стеком протоколов, представляющая собой выражение вероятностной функции оценки защищенности информации, обрабатываемой в КС, имеет вид:

$$P_2 = 1 - T_2 = \left(1 - E_1\right)\left(1 - E_2\right) + E_1 M_1 + \left(1 - E_1\right)E_2\left(M_1\left(1 - M_2\right) + M_2\right) \quad (6)$$

Аналогичное выражение, полученное для КС с N уровнями протоколов, для случая L угроз информации имеет следующий вид:

$$P(M) = \prod_{i=1}^{L}\left(\prod_{j=1}^{N}\left(1 - E_{ij}\right) + \sum_{j=1}^{N}\left[E_{ij}\prod_{k=1}^{j-1}\left(1 - E_{ik}\right)\cdot\left(\sum_{k=1}^{j} M_{ik}\cdot\prod_{l=k+1}^{j}\left(1 - M_{il}\right)\right)\right]\right) \quad (7)$$

где L – количество угроз информации, обрабатываемой в КС; N – количество уровней стека протоколов КС; M_{ij} – целочисленная переменная, значение которой определяет факт наличия/отсутствия механизма защиты от i-й угрозы на протоколе j-го уровня; E_{ij} – показатель эффективности реализации i-й угрозы на протоколе j-го уровня.

Выражение (7) представляет собой вероятностную модель защищенной КС с открытой архитектурой и произвольным количеством уровней стека протоколов, позволяющую оценить вероятность сохранения защищенности информации при воздействии на КС произвольного множества угроз. Данное выражение, совместно с ограничениями, заданными в виде (2), может быть использовано в качестве целевой функции (ЦФ), подлежащей максимизации путем решения соответствующей задачи математического программирования. В результате максимизации данной ЦФ может быть получено множество механизмов защиты $M=\{M_{ij}\}$, реализация которых в КС с открытой архитектурой обеспечит максимальную защищенность от множества угроз с эффективностями $E=\{E_{ij}\}$ при соблюдении заданных ограничений на суммарную стоимость включенных в состав СЗИ средств защиты, реализующих соответствующие механизмы.

Литература: 1. НД ТЗИ 1.1-002-99. Общие положения по защите информации в компьютерных системах от несанкционированного доступа. 2. Гайкович В., Першин А. Безопасность электронных банковских систем.– М.: Изд-во компания "Единая Европа", 1993. 3. Federal Information Processing Standard (FIPS PUB) 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, June, 1974. 4. Рябинин И. А. Научная школа логико-вероятностных методов и концепция логико-вероятностной теории безопасности сложных систем // Теория и информационная технология моделирования безопасности сложных систем. Вып. 1 / Под ред. И. А. Рябинина. Препринт 101. СПб. ИПМАШ РАН, 1994. 5. Рябинин И. А. Концепция логико-вероятностной теории безопасности.– Приборы и системы управления, № 10, 1993.– с. 6–9. 6. Соложенцев Е. Д., Соложенцев В. Е. Моделирование поведения структурно-сложных систем: параметры, модели, знания, визуализация // Теория и информационная технология моделирования безопасности сложных систем. Вып. 2 / Под ред. И. А. Рябинина. Препринт 104. СПб. ИПМАШ РАН, 1994. 7. ISO 7498-2. Basic Reference Model – Part 2: Security Architecture. – February 1989. 8. IEEE802.10B. IEEE Standards for Interoperable Local Area Network (LAN) Security (SILS): Part B – Secure Date Exchange. – April 1992. 9. Рябинин И. А., Черкесов Г. Н. Логико-вероятностные методы исследования надежности структурно-сложных систем. М.: Радио и связь, 1981.

УДК 681.3.06

ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЦЕНТРАЛИЗОВАННОГО КОНТРОЛЯ И АУДИТА СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Виктор Кондратюк, Андрей Тимошенко
ООО «Институт компьютерных технологий»

Анотація: **Сформульовано основні вимоги і викладено принципи побудови систем централізованого контролю та аудиту засобів захисту корпоративної комп'ютерної мережі. Показано, як дані вимоги реалізовані в системі «Міраж».**
Summary: **The main ideas and principles of designing of centralized security monitoring and audit systems for corporate computer networks are formulated. The example of realization in a system «Mirage» is**