УДК 004.056.53

ОЦЕНКА ПОКАЗАТЕЛЕЙ МОНИТОРИНГА БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

М.Н. БОБОВ

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

Поступила в редакцию 2 ноября 2015

Приведен подход к оценке мониторинга безопасности информационных систем. Показано, что показателями мониторинга безопасности могут быть вероятности пропуска события безопасности, потери события безопасности при доставке в центр мониторинга и пропадания сигнала тревоги администратору безопасности. Предложены методы оценки указанных показателей мониторинга безопасности.

Ключевые слова: мониторинг безопасности, угрозы безопасности, оценка показателей.

Введение

Большое разнообразие методов и механизмов обеспечения информационной безопасности информационных систем предопределяет необходимость формальных моделей и методик анализа эффективности систем защиты. Данные модели и методики включают агрегированную оценку эффективности методов и механизмов как программно-технического, так и нормативно-организационного характера для защиты активов информационной системы. Решение подобных задач основывается на теоретико-графовом подходе в виде так называемой «модели систем с полным перекрытием [угроз безопасности]». Система защиты в рамках данной формализации представляется дольным графом, вариант которого представлен на рис. 1 [1].

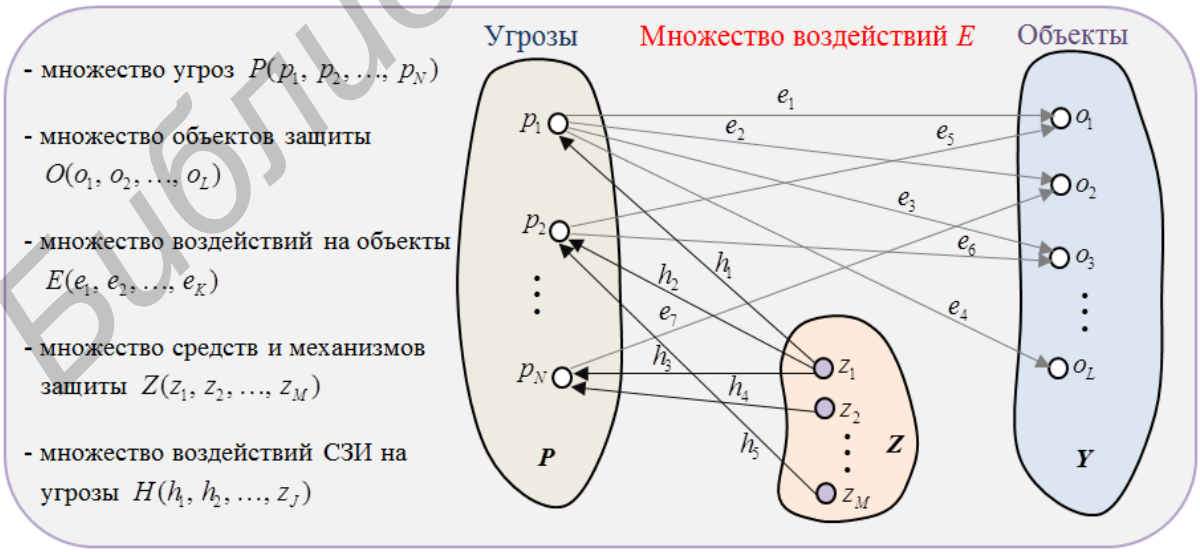

Рис. 1. Модель системы защиты в виде 3-дольного графа

Каждое ребро графа $G(P,O,Z,E,H)$ специфицирует воздействие конкретной угрозы на конкретный актив (объект) или устранение (нейтрализацию) определенным защитным ме-

ханизмом угрозы безопасности. При этом от каждой угрозы может быть несколько воздействий на различные объекты и каждый объект может быть подвергнут нескольким угрозам (связь «многие – ко многим»).

Для получения и оперирования количественными параметрами граф $G(P,O,Z,E,H)$ взвешивается и эквивалентно представляется следующей совокупностью векторов и матриц:

- вектор $P(p_1, p_2, \ldots, p_N)$, где p_i – вероятность осуществления соответствующей угрозы;

- вектор $O(o_1, o_2, \ldots, o_L)$, где o_i – стоимость соответствующего объекта защиты;

- $N \times L$ матрица $E\{eij\}$, где $e, j = 1$ при воздействии i-й угрозы на j-й объект, и $e, j = 0$ в противном случае;

- вектор $Z(z_1, z_2, \ldots, z_M)$, где z_i – стоимость соответствующего способа или средства защиты;

- $N \times M$ матрица $H\{hij\}$, где hij – вероятность устранения (или степень снижения ущерба) i-й угрозы от применения j-го средства защиты.

В рамках данной формализации возможно решение таких важных практических задач, как оценка технико-экономической или тактико- технической эффективности систем защиты.

Теоретический анализ

Оценка технико-экономической эффективности системы защиты основывается на определении количественного критерия, отражающего влияние реализованной системы защиты на снижение опасности от воздействия угроз, или иначе на величину ущерба от угроз безопасности.

В качестве такого критерия технико-экономической эффективности, в частности, можно использовать следующий показатель:

$$\frac{U - U'}{\sum_{i=1}^{L} O_i + \sum_{k}^{M} Z_k},$$

где U – оценка величины ущерба от угроз безопасности при отсутствии защитных мер и механизмов; U' – оценка величины остаточного ущерба при реализации защитных мер и механизмов.

Расчет величин U и U' осуществляется по следующим соотношениям:

$$U = \sum_{i=1}^{L} O_i \left(1 - \prod_{j}^{N} e_{ij} \left(1 - P_j\right)\right),$$

$$U' = \sum_{i=1}^{L} O_i \left(1 - \prod_{j=1}^{N} e_{ij} \left(1 - P_j \left(\prod_{k=1}^{M} (1 - h_{ik})\right)\right)\right).$$

Оценка величин U и U' изложена в методике, приведенной в стандарте банка России СТО БР ИББС-1.2-2014 [2]. В указанной методике используется 10 показателей оценки информационной безопасности (ИБ), из которых для автоматизированных информационных систем можно использовать следующие:

- обеспечение ИБ при назначении и распределении ролей и обеспечении доверия к персоналу;
- обеспечение ИБ на стадиях жизненного цикла;
- обеспечение ИБ при управлении доступом и регистрацией;
- обеспечение ИБ средствами антивирусной защиты;
- обеспечение ИБ при использовании ресурсов сети Интернет;
- обеспечение ИБ при использовании средств криптографической защиты информации;
- обеспечение ИБ информационных технологических процессов.

Вместе с тем, указанные показатели определяются комиссионным образом на стадии ввода информационной системы в эксплуатацию или по истечении определенного периода эксплуатации. Поэтому использовать изложенный в методике подход по оценке информацион-

ной безопасности для текущего контроля состояния информационной безопасности с помощью технических средств не представляется возможным.

Задачи тактико-технического анализа эффективности систем защиты заключаются в определении остаточной вероятности реализации всех возможных угроз без учета стоимости объектов и мер защиты, что может быть вычислено по следующему соотношению:

$$P'_{\text{преод.}} = 1 - \prod_{i=1}^{N}\left(1 - P_i\left(1 - \prod_{k=1}^{M}\left(1 - h_{ik}\right)\right)\right). \quad (1)$$

Считая, что во введенной в действие информационной системе реализована система защиты, средства и механизмы которой в полной мере защищают от угроз безопасности, т.е. $h_{ik} = 1$, выражение (1) можно записать в виде:

$$P'_{\text{преод.}} = 1 - \prod_{i=1}^{N}\left(1 - P_i\right), \quad (2)$$

где вероятности P_i являются остаточными вероятностями реализации угроз и определяются конструктивными свойствами системы мониторинга.

Методика оценки показателей мониторинга безопасности

Применительно к системе мониторинга безопасности информационной системы в условиях, когда все установленные угрозы перекрыты системой защиты, оценка состояния ИБ может быть определена из (2) по формуле

$$P'_{\text{преод.}} = 1 - \prod_{i=1}^{3}\left(1 - P_i\right), \quad (3)$$

где P_1 – вероятность пропуска события безопасности; P_2 – вероятность потери события безопасности при доставке в центр мониторинга; P_3 – вероятность пропадания сигнала тревоги администратору безопасности.

Рассмотрим подходы по определению вероятностей в выражении (3).

Природа угрозы P_1 не позволяет вычислить ее вероятность на основе известных соответствующих физических закономерностей (априорный подход). В некоторых случаях возможен апостериорный подход, основанный на накопленной статистике проявления соответствующей угрозы в данной или подобной компьютерной системе (в подобных условиях) [3]. Оценки вероятности реализации угрозы при этом вычисляются на основе методов статистических оценок. Альтернативой аналитическому и статистическому подходу для определения вероятности P_1 является метод экспертных оценок, широко используемый для оценок сложных, неформализуемых объектов.

Суть метода экспертных оценок заключается в том, что в качестве инструментария оценок (в качестве измерительного прибора) выступают специалисты-эксперты, которые на основе профессионального опыта, глубокого представления многокомпонентной природы оцениваемых объектов, дают эвристические оценки по одному или группе параметров [4]. В кратком изложении методика экспертных оценок включает следующие этапы.

Этап 1. Отбор экспертов (формальные и неформальные требования к специалистам-экспертам, метод «снежного кома», когда известного специалиста просят назвать других ему известных специалистов, в свою очередь, опрашивают их и т.д., до тех пор пока множество экспертов не прекращает расширяться. На практике количество экспертов – 10-12 человек).

Этап 2. Выбор параметров, по которым оцениваются объекты (при этом определяются сущностные параметры оценивания, которые должны выражать природу оцениваемых объектов и быть независимыми друг от друга, определяются веса параметров).

Этап 3. Выбор шкал оценивания и методов экспертного шкалирования. Применяются порядковые, ранговые, интервальные, абсолютные и другие шкалы. В качестве методов шкалирования выступают ранжирование объектов по предпочтительности выраженности оцениваемого параметра (порядковая шкала оценки), попарные оценки сравнительной предпочтительности во всех возможных парах оцениваемых объектов, и непосредственная оценка выражен-

ности оцениваемого параметра (например, эксперты непосредственно дают оценку вероятности реализации угроз, в других случаях на основе специальных балльных шкал оценки).

Этап 4. Выбор и осуществление процедуры опроса экспертов (с непосредственным взаимодействием экспертов или без взаимодействия, т.н. итерационный метод опроса «Дельфи», когда эксперты непосредственно не взаимодействуют, но после каждого тура опроса им сообщают усредненные оценки прежнего тура и просят на этой основе скорректировать свои прежние оценки, исключая тем самым влияние на результаты опроса мнений конкретных «авторитетов», и т.д.).

Этап 5. Агрегирование оценок, анализ их устойчивости и согласованности, осуществляемые на основе подходов, подобных методам обработки статистических данных.

Следует отметить, что экспертные оценки, несмотря на их «субъективность» на основе хорошо подобранных экспертных комиссий, правильно установленных методов шкалирования и опроса, при соответствующей обработке дают результаты, действенность которых многократно апробирована в крупных проектах и процедурах, не допускающих другие, в особенности, аналитические и статистические подходы.

В отличие от вероятности P_1 значения вероятностей P_2 и P_3 могут быть вычислены аналитически. Так, вероятность P_2 может быть вычислена как вероятность потери сообщения, величина которой полностью определяется характеристиками сети передачи. Одним из подходов [5] может быть определение вероятности потери сообщения на основе статистики работы сети по формуле

$$P_{\text{пот}} = 1 - C_{\text{пол}} / C_{\text{отпр}},$$

где $C_{\text{пол}}$ – количество полученных сообщений; $C_{\text{отпр}}$ – количество отправленных сообщений.

Для расчета вероятности потери сообщения можно воспользоваться также методами теории массового обслуживания, приведенными в [6]. В данном случае вероятность потери сообщения можно определить по формуле

$$P_{\text{пот}} = \frac{(1-\rho)}{1-\rho^{s+1}} \cdot \rho^{s}, \qquad (4)$$

где ρ – коэффициент загрузки сети ($\rho < 1$); s – емкость запоминающего устройства (в сообщениях).

Для современных телекоммуникационных сетей расчеты по формуле (4) могут дать неоправданно оптимистические оценки, так как они основаны на марковских моделях потоков заявок и их обслуживания. Так как трафик телекоммуникационной сети обладает свойствами фрактальности, для оценки вероятности потери сообщения используют параметр Херста. Выражение вероятности потерь принимает вид

$$P_{\text{пот}} = \frac{(1-\rho)}{1-\rho^{(S+1)^{2(1-H)}}} \cdot \rho^{S^{2(1-H)}}, \qquad (5)$$

где H – параметр Херста.

Если параметр Херста $H \le 0{,}5$, то поток не обладает свойством фрактальности и выражение (5) преобразуется к виду (4). В [7] приведены следующие данные о фрактальности различных типов трафика (см. табл.).

Фрактальность различных типов трафика

Тип трафика	Фрактальность трафика (*H*)
Ethernet	0,9
HTTP	0,75-0,92
Видео	0,6-0,9
Аудио	0,6-0,9
P2P	0,6-0,9

Как видно из таблицы, основные типы сетевых приложений имеют коэффициент Херста больше 0,6. При таком трафике вероятность потери сообщения желательно определять по формуле (5).

Для расчета вероятности пропадания сигнала тревоги администратору безопасности P_3 фиксируется совокупность технических средств, составляющих тракт доведения сигналов тревоги администратору. Вероятность P_3 вычисляется по формуле

$$P_3 = 1 - e^{\sum_{i-1}^{m} \lambda_i x t_i},$$

где λ_i – интенсивность отказа или сбоя *i*-го аппаратного средства *i*-го программного средства в тракте сигнализации; t_i – интервал времени, в течение которого функционирует аппаратное или программное средство в тракте сигнализации; m – число технических средств, составляющих тракт сигнализации.

Параметр λ может быть определtn следующим образом [8]. Для периода эксплуатации информационной системы, когда $\lambda = \text{const}$, т.е. интенсивность отказов λ не зависит от времени, вероятность того, что в заданном интервале времени T не произойдет отказа, определяется по формуле

$$P(T) = e^{-\lambda T}.$$

При известном или принятом значении $P(T)$ интенсивность отказа можно вычислить по формуле

$$\lambda = -\frac{\ln P(T)}{T},$$

где T – время безотказной работы (час).

Для программных средств защиты вероятность сбоя может быть определена из соотношения $\lambda_{\text{сб.}} = 0{,}1\lambda_{\text{отк.}}$

Заключение

Разработана методика оценки показателей мониторинга безопасности информационных систем, к которым относятся:

- вероятность пропуска события безопасности;
- вероятность потери события безопасности при доставке в центр мониторинга;
- вероятность пропадания сигнала тревоги администратору безопасности.

Для каждого показателя определены методы расчета численных значений, которые можно легко использовать в практической деятельности служб обеспечения безопасности автоматизированных информационных систем.

ASSESSMENT OF INFORMATION SYSTEMS SECURITY MONITORING

M.N. BOBOV

Abstract

The article shows the approach to assessment of information systems security monitoring. It is revealed that possibilities of omitting or loss the security events in the process of delivering them to the security administrator as well as loss of the alarm signal are important security monitoring showings. The methods of assessment of the revealed security monitoring indexes are offered further in the article.

Список литературы

1. *Гайдамакин Н.А.* Теоретические основы компьютерной безопасности. Екатеринбург, 2008.
2. Стандарт Банка России СТО БР ИББС-1.2-2014.
3. *Антюхов В.И.* Системный анализ и принятие решений. СПб., 2009.
4. *Воробьёв С.Н., Егоров Е.С., Торбин В.У.* Методы выработки решений. Надежность и эффективность в технике. Том 3. М., 1988.
5. *Боев В.Д., Ушкань А.О.* // Сб. докладов IV Всероссийской научно-практической конференции «Имитационное моделирование. Теория и практика». 2009. С. 299-303.
6. *Ланин М.И.* // Автоматика и телемеханика. 1962. Том 23. Вып. 3.
7. *Лосев Ю.И., Руккас К.М.* // Вісник Харківського національного університету. Серія «Математичне моделювання. Інформаційні технології. Автоматизовані системи управління». 2008. №833. С. 163-168.
8. *Рембеза А.И., Патрушев В.И.* Проектный анализ надежности. Том 5. М., 1988.