УДК 004.056.53

М. М. Бусько

КОЛИЧЕСТВЕННАЯ ОЦЕНКА АКТУАЛЬНОСТИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРОЕКТИРУЕМЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Разработка и построение модели угроз безопасности информации является важным элементом в системе информационной безопасности. На основе модели угроз определяются требования к защитным мерам.

В статье предлагается способ количественной оценки актуальности угроз информационной безопасности в информационных системах на этапе их разработки. Вычисление осуществляется в соответствии с проектом «Методики определения угроз безопасности информации в информационных системах» ФСТЭК России. Способ может иметь практическое применение для автоматизации расчетов, при условии разработки системы численных значений для таких параметров, как уровень проектной защищенности, степени возможного ущерба в результате нарушения конфиденциальности, целостности и доступности информации.

Ключевые слова: угроза информационной безопасности, актуальная угроза, оценка актуальности угрозы, возможность реализации угрозы, потенциал нарушителя.

M. M. Busko

QUANTITATIVE EVALUATION OF THE TOPICAL INFORMATION SECURITY THREAT IN THE PROJECTED INFORMATION SYSTEMS

The development and construction of a model of threats to information security is an important element in the information security system. Based on the threat model, the requirements for protective measures are defined.

The article proposes a method of quantitative assessment of the urgency of information security threats in information systems at the stage of their development. The calculation is carried out in accordance with the project «Methods for determining threats to information security in information systems» of the FSTEC of Russia. The method can have practical application for automation of calculations, provided the system of numerical values is developed for such parameters as the level of project security, the degree of possible damage as a result of violation of confidentiality, integrity and availability of information.

Keywords: threat of information security, topical threat, evaluation of the topical threat, the possibility of threat realization, potential of the offender.

Любая система защиты должна однозначно определять, что и от чего следует защищать. Не является исключением и система защиты информации в проектируемых информационных системах. Основополагающие нормативные документы в области информационной безопасности рекомендуют требования к системе защиты информации определять на основе модели угроз безопасности информации. ФСТЭК России обнародовала на рассмотрение проект «Методики

определения угроз безопасности информации в информационных системах» (далее – Методика) [1]. Документ призван установить единый методический подход к определению угроз безопасности информации и разработке моделей угроз безопасности информации в государственных информационных системах. Для остальных организаций, включая и операторов ПДн и организаций, осуществляющих работы по созданию (проектированию) информационных систем данный документ носит рекомендательный характер. Методика вызвала в основном положительные отзывы экспертов в области информационной безопасности. Однако отмечается большая трудоемкость практического применения методики, анализ угроз в ручную становится фактически нереальным либо нерентабельным [2]. Выходом является применение средств автоматизации расчетов актуальности угроз.

Методика предусматривает идентификацию каждой угрозы. Идентифицированная угроза безопасности информации подлежит нейтрализации (блокированию), если она является актуальной для информационной системы [1]. Оценка актуальности угрозы ($УБИ_j^A$) рассматривается как двухкомпонентный вектор, первый компонент которого характеризует вероятность реализации угрозы (P_j), а второй – степень возможного ущерба в случае ее реализации (X_j) [1]. Следовательно, актуальность угрозы является функцией двух аргументов от вероятности реализации угрозы (P_j) и степени ущерба (X_j):

$$УБИ_j^A = [P_j; X_j]. \quad (1)$$

Причем P_j и X_j оцениваются экспертным путем качественными мерами с использованием таких вербальных определений, как «низкие», «средние» или «высокие». Отсутствие четких правил формализации экспертных знаний, несомненно, является препятствием автоматизации расчетов актуальности угроз.

В настоящей работе предлагается способ вычисления количественной оценки актуальности угрозы, на основании Методики. Действие Методики распространяется на оценку угроз обусловленных антропогенными факторами. В этом ракурсе и будем рассматривать возможность формализованного представления параметра актуальности угроз безопасности информации в информационных системах.

В соответствии с [1] P_j определятся на основе анализа статистических данных о частоте реализации угроз безопасности информации. На этапе проектирования информационной системы, особенно целевого назначения, такие данные либо не обладаю требуемой достоверностью, либо отсутствуют. В этих случаях, как предусмотрено Методикой, берется оценка возможности реализации угрозы безопасности информации (Y_j):

$$УБИ_j^A = [Y_j; X_j]. \quad (2)$$

Y_j определятся на основе оценки уровня защищенности информационной системы (Y_1) и потенциала нарушителя (Y_2), т. е.

$$Y_j = [Y_1; Y_2]. \quad (3)$$

Тогда оценку актуальности угрозы можно представить:

$$УБИ_j^A = [Y_1; Y_2; X_j]. \quad (4)$$

На этапе создания информационной системы меры защиты информации еще не реализованы и только стоит вопрос об их реализации. В этом случае оценка возможности реализации *j*-ой угрозы безопасности информации (Y_j) проводится относительно уровня проектной защищенности информационной системы ($Y_1^П$):

$$УБИ_j^A = [Y_1^П; Y_2; X_j]. \quad (5)$$

Уровень проектной защищенности ($Y_1^П$) определяется на основе анализа проектных структурно-функциональных характеристик и приводится к качественной шкале («низкий», «средний», «высокий»).

Потенциал нарушителя (Y_2) – это оценка возможностей нарушителя по идентификации и использованию уязвимости в информационной системе. Y_2 проводится по результатам определения следующих показателей [1]:

Y_2^T – время, затрачиваемое нарушителем на идентификацию и использование уязвимости (затрачиваемое время);

Y_2^K – техническая компетентность нарушителя;

Y_2^M – знание нарушителем проекта и информационной системы;

Y_2^U – оснащенность нарушителя;

Y_2^P – возможности нарушителя по доступу к информационной системе. Таким образом, потенциал нарушителя является функцией вида:

$$Y_2 = [Y_2^T; Y_2^K; Y_2^M; Y_2^U; Y_2^P]. \quad (6)$$

Методика предусматривает числовые значения указанных показателей (табл. 1).

Таблица 1

Числовые значения показателей возможностей нарушителя [1]

Возможности нарушителя		Значение при идентификации уязвимости	Значение при использовании уязвимости
Y_2^T	< 0,5 час	0	0
	< 1 день	2	3
	< 1 месяц	3	5
	> 1 месяц	5	8
Y_2^K	Непрофессионал	0	0
	Специалист	2	3
	Профессионал	5	4
Y_2^M	Отсутствие знаний	0	0
	Ограниченные знания	2	2
	Знание чувствительной информации	5	4
Y_2^U	Отсутствует	0	0
	Стандартное оборудование	1	2
	Специализированное оборудование	3	4
	Оборудование, сделанное на заказ	5	6
Y_2^P	< 0,5 час или не обнаруживаемый доступ	0	0
	< 1 день	2	4

Возможности нарушителя		Значение при идентификации уязвимости	Значение при использовании уязвимости
	< 1 месяц	3	6
	> 1 месяц	4	9
	Не возможно		

Числовые значения характеристик потенциала нарушителя суммируются:

$$Y_2 = Y_2^T + Y_2^K + Y_2^M + Y_2^U + Y_2^P . \quad (7)$$

Полученная сумма значений характеристик соотносится с диапазонами значений в соответствии, с которыми определяется потенциал нарушителя в качественных категориях: «потенциал недостаточен для реализации угрозы безопасности», «базовый (низкий)», «базовый повышенный (средний)» и «высокий».

Для оценки степени возможного ущерба (X_j) рассматривается непосредственное или опосредованное воздействие на конфиденциальность (X_j^K), целостность ($X_j^Ц$), доступность информации ($X_j^Д$), содержащейся в информационной системе. При этом так же оперируют качественными характеристиками («низкая», «средняя», «высокая») для нарушения каждого свойства безопасности информации. Результирующая степень возможного ущерба определяется по наивысшему значению:

$$X_j = \max\left(X_j^K, X_j^Ц, X_j^Д\right). \quad (8)$$

Подставив оценки уровня проектной защищенности ($Y_1^П$), потенциала нарушителя (Y_2) и степени возможного ущерба (X_j) в формулу (5) получим:

$$УБИ_j^A = \left[Y_1^П; \left(Y_2^T + Y_2^K + Y_2^M + Y_2^U + Y_2^P\right); \left(\max\left(X_j^K, X_j^Ц, X_j^Д\right)\right)\right]. \quad (9)$$

Рассмотрим формулу (3) в соответствии с которой возможность реализации угрозы безопасности информации (Y_j) зависит от уровня проектной защищенности информационной системы ($Y_1^П$) и потенциала нарушителя (Y_2). Вполне логично предположить, что эта зависимость от обоих аргументов линейна. Соответственно возможность реализации угрозы будет определяться суммой:

$$Y_j = \left[Y_1^П + Y_2\right]. \quad (10)$$

Как было сказано ранее оценка актуальности угрозы ($УБИ_j^A$) в Методике рассматривается как функция от вероятности реализации угрозы (P_j) и степени ущерба (X_j). По терминологии ГОСТ Р ИСО/МЭК 27005-2010 риск информационной безопасности – возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации. Он измеряется исходя из комбинации вероятности события и его последствия [3], вычисляется риск путем умножения этих двух показателей. Другим нормативным документом оперирующим понятием риск информационной безопасности являются РС БР ИББС-2.2-2009. Документ определяет риск, как меру, учитывающую вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы [4], количественно оценивается так же произведением. Вполне уместно считать оценку актуальности угроз аналогичной

риску информационной безопасности и численно представить, как произведение вероятности реализации угрозы (P_j) и степени ущерба (X_j). Для проектируемых информационных систем соответственно произведение возможности реализации угрозы безопасности информации (Y_j) и степени ущерба (X_j). С учетом этих рассуждений, в окончательном виде формализованная количественная оценка актуальности угрозы будет выглядеть следующим образом:

$$УБИ_j^A = \left(Y_1^{П} + Y_2^T + Y_2^K + Y_2^M + Y_2^U + Y_2^P\right) \cdot \max\left(X_j^{К}, X_j^{Ц}, X_j^{Д}\right). \quad (11)$$

Предложенная количественная оценка актуальности угроз в информационных системах на этапе их разработки соответствует требованиям «Методики определения угроз безопасности информации в информационных системах» ФСТЭК России и может иметь практическое применение. При условии разработки системы численных значений для таких параметров, как уровень проектной защищенности ($Y_1^{П}$), степени возможного ущерба в результате нарушения конфиденциальности ($X_j^{К}$), целостности ($X_j^{Ц}$) и доступности информации ($X_j^{Д}$), данный способ может использоваться для автоматизации расчетов актуальности угроз.

Список использованной литературы

1. «Методика определения угроз безопасности информации в информационных системах» [Электронный ресурс] / ФСТЭК России. Проект. – Режим доступа: http://fstec.ru/component/attachments/download/812 (дата обращения 14.06.2017).

2. Борисов С. СОИБ. Анализ. Определение угроз безопасности [Электронный ресурс] / Часть 1 // SecurityLab.ru – информационный портал. 20 мая 2015 г. – Режим доступа: http://www.securitylab.ru/blog/personal/sborisov/139182.php (дата обращения 14.06.2017).

3. ГОСТ Р ИСО/МЭК 27005-2010. «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». – М. : «ИПК Издательство стандартов», 2011.

4. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности» РС БР ИББС-2.2-2009 (приняты и введены в действие Распоряжением Банка России от 11.11.2009 № Р-1190).

Информация об авторе

Бусько Михаил Михайлович – кандидат технических наук, доцент, кафедра информатики и кибернетики, Байкальский государственный университет, 664003, г. Иркутск, ул. Ленина, 11, e-mail: buskomm@bgu.ru.

Author

Busko Mikhail Mikhailovich – Ph.D. (Engineering), Associate professor of the Department of computer science and cybernetics, Baikal State University, 11 Lenin St., 664003, Irkutsk, e-mail: buskomm@bgu.ru.