4. *Gulyaev D.N., Batmanova O.V.* Impul'sno-kodovoe gidroproslushivanie i algoritmy mul'tiskvazhinnoj dekonvolyucii – novye tekhnologii opredeleniya svojstv plastov v mezhskvazhinnom prostranstve // Vestnik Rossijskogo novogo universiteta. Seriya "Slozhnye sistemy: modeli, analiz i upravlenie". 2017. № 4. S. 26–32.

5. *Aslanyan A. et al.* Assessing Waterflood Efficiency with Deconvolution Based Multi-Well Retrospective Test Technique. Stat'ya SPE-195518-MS.

6. *Ilk D., Valko P., Blasingame T.* A Deconvolution Method Based on Cumulative Production for Continuously Measured Flowrate and Pressure Data. SPE-111269-MS.

DOI: 10.25586/RNU.V9187.19.03.P.092 УДК 004

Е.А. Витенбург

ФОРМАЛИЗОВАННАЯ МОДЕЛЬ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

Рассмотрены основные методы оценки защищенности информационной системы (ИС) предприятия, а именно: метод оценки защищенности ИС предприятия от несанкционированного доступа (НСД) на основе экспертной информации, метод экспертных оценок, графовый метод, метод деревьев отказов, метод на основе модели комплекса механизмов защиты. Приведен сравнительный анализ методов оценки защищенности ИС с функциональной точки зрения. На базе анализа выявлены наиболее эффективные методы для оценки защищенности ИС предприятия: метод оценки защищенности ИС предприятия от НСД на основе экспертной информации, метод экспертных оценок. Разработана математическая модель, включающая в себя метод оценки защищенности ИС предприятия от НСД на основе экспертной информации, метод экспертных оценок. Данная математическая модель является источником для формирования программного комплекса «Оценка защищенности информационной системы предприятия».

Ключевые слова: информационная система, информационная безопасность, оценка защищенности, методы оценки защищенности, критерии оценки защищенности.

E.A. Vitenburg

FORMALIZED MODEL FOR ASSESSING THE SECURITY OF AN ENTERPISE INFORMATION SYSTEM

The article describes the main methods for assessing the security of an enterprise information system (IS), namely: a method for assessing the security of an enterprise IP from unauthorized access (UNA) based on expert information, an expert assessment method, a graph method, a fault tree method, a method based on a complex mechanism model protection. A comparative analysis of the methods for assessing IS security from a functional point of view is given. Based on the analysis, the most effective methods for assessing the security of an enterprise's IS have been identified: a method for assessing the security of an enterprise's IS from unauthorized access based on expert information, and a method of expert assessment. A mathematical model has been developed, which includes a method for assessing the

© Витенбург Е.А., 2019

security of an enterprise IS from unauthorized access based on expert information, a method of expert assessments. This mathematical model is the basis for the formation of the software package "Assessment of the security of the enterprise information system".
Keywords: information system, information security, security assessment, security assessment methods, security assessment criteria.

Защищенность определяется как обобщенный показатель корректности реализации механизмов защиты информации. Ее оценка позволяет выявить наиболее «слабые» места информационной системы (ИС) предприятия, своевременно предотвратить реализацию угроз безопасности, направленных на нарушение таких свойств информации, как конфиденциальность, целостность и доступность. Далее проанализированы методы оценки защищенности ИС [1; 2].

Существует довольно большое количество методов анализа защищенности. Наиболее популярными являются графовый метод, метод деревьев отказов, метод экспертных оценок, метод оценки защищенности информации от НСД на основе экспертной информации, метод на основе модели комплекса механизмов защиты [4].

Для проведения критериального сравнительного анализа методов оценки защищенности использованы критерии, представленные в таблице 1.

Таблица 1

Критерии оценки метода

Критерий оценки метода	**Описание**
Скорость расчетов	Критерий определяет, с какой скоростью осуществляется обработка исходных данных, используемых для оценки защищенности
Трудоемкость расчетов	Критерий определяет затраты вычислительных ресурсов, в том числе человеческих
Эффективность применения	Критерий отображает соотношение между результатом метода и использованными для его реализации ресурсами, удобство применения. Показывает степень удобства для данного метода оценки
Точность расчетов	Критерий определяет адекватность работы метода, показывает степень объективности полученных результатов
Генерация количественной оценки защищенности	Критерий определяет возможность формирования числового показателя оценки
Наглядность результатов использования метода	Критерий определяет возможность визуализации полученных результатов оценки
Возможность работ с нестрого формализованной информацией	Критерий определяет необходимость формализации имеющихся сведений об ИС предприятия
Нахождение уязвимостей	Критерий определяет функциональную особенность метода в обнаружении уязвимостей в ИС предприятия

На основе данных критериев проведен сравнительный анализ методов оценки защищенности ИС предприятия (табл. 2).

Таблица 2

Критерии методов оценки защищенности ИС

Критерии/методы	Скорость расчетов	Трудоемкость расчетов	Эффективность применения	Удобство использования	Точность расчетов	Генерация количественной оценки	Наглядность результатов	Возможность работ с неформализованной информацией	Нахождение уязвимостей	Итог
Графовый	0	0	0	0	0,5	0,5	0,5	0	0,5	2
Деревьев отказов	0	0	0	0	0,5	0,5	0,5	0	0,5	2
Экспертных оценок	1	0,5	1	1	0,5	0,5	1	1	0,5	7
Оценки защищенности информации от НСД (экспертный подход)	0,5	0,5	0,5	0,5	0,5	1	1	1	1	6,5
На основе модели комплекса механизмов защиты	0,5	0.5	0,5	0,5	0,5	0	0	0	1	3,5

Из критериального анализа методов оценки защищенности ИС предприятия можно сделать вывод о том, что не все методы подходят для оценки защищенности ИС. Из дальнейшего рассмотрения исключаются графовый метод, метод на основе модели комплекса механизмов защиты и метод деревьев отказов. Сравнительный анализ показал, что метод экспертной оценки и метод оценки защищенности информации от НСД на основе экспертной информации позволяют дать наиболее корректную оценку защищенности ИС.

На основе анализа, в ходе которого были определены наиболее подходящие методы, была сформирована математическая модель оценки защищенности информационной системы. Данная модель основывается на синтезе двух методов оценки защищенности, а именно метода экспертных оценок и метода оценки защищенности ИС предприятия от НСД на основе экспертной информации [5; 6; 7].

Метод экспертных оценок основан на взаимодействии специалистов (экспертов), на получении и обработке сложившихся мнений экспертов по возникшим вопросам. Экспертные решения формируются с целью подготовки информации для принятия решений об уровне защищенности системы.

Для проведения экспертной оценки необходимо сформировать множество оцениваемых компонентов ИС:

$$IS = \{k_1, ..., k_n\}, \quad (1)$$

где k_n – компоненты ИС;

$n \in N$ – количество компонентов ИС.

Далее необходимо определить события безопасности (2), которые могут свидетельствовать о реализации угрозы (3):

$$S = \{s_1, ..., s_n\}, \tag{2}$$

где S – множество совершаемых событий в ИС;

s_n – события ИС;

$n \in N$ – количество событий в ИС.

$$U = \{u_1, ..., u_m\}, \tag{3}$$

где U – множество актуальных угроз;

u_m, $m \in N$ – количество угроз.

В зависимости от сгенерированных в ИС событий безопасности определяют возможность реализации той или иной угрозы. Формализация данного процесса представлена в формуле

$$U = \begin{cases} U_1 = (S_1, S_4), \\ U_2 = (S_4, S_7), \\ U_3 = (S_4, S_7), \\ U_4 = (S_1), \\ U_5 = (S_2, S_8), \\ U_6 = (S_3, S_5, S_6), \end{cases} \tag{4}$$

где U – множество актуальных угроз;

S_1 – вход учетной записи в системы;

S_2 – управление учетными записями в системе;

S_3 – события маршрутизации и удаленного доступа;

S_4 – событие доступа к объекту системы;

S_5 – изменение политики системы;

S_6 – использование субъектом особых привилегий;

S_7 – функционирование процессов системы;

S_8 – события входа субъектов в систему;

U_1 – угрозы утечки;

U_2 – угрозы искажения;

U_3 – угрозы утраты;

U_4 – угрозы блокирования;

U_5 – угрозы взлома;

U_6 – угрозы злоупотребления.

После этого следует для каждой угрозы U_i из набора актуальных угроз U определить возможные исходы реализации угроз I_{ij}, или, другими словами, риски, которые зависят от вероятности реализации угрозы A_{ij} и ущерба Y_{ij} (табл. 3):

$$I_{ij} = A_{ij} Y_{ij}, \tag{5}$$

где I_{ij} – риск реализации угрозы *i*-й угрозы для *j*-го компонента;

A_{ij} – вероятность реализации *i*-й угрозы для *j*-го компонента;

Y_{ij} – ущерб от реализации от *i*-й угрозы для *j*-го компонента ИС.

Таблица 3

Возможные исходы реализации угрозы

№ п/п	Вероятность реализации угрозы A_{ij}	Ущерб от реализации угрозы Y_{ij}
1	Маловероятно	Отсутствует
2	Маловероятно	Низкий
3	Средняя	Низкий
4	Средняя	Средний
5	Выше среднего	Средний
6	Выше среднего	Выше среднего
7	Выше среднего	Средний
8	Выше среднего	Выше среднего
9	Высокая	Выше среднего
10	Высокая	Высокий

Вероятности реализации оцениваются следующим образом:

- маловероятно [0;0,2);
- низкая (0,2;0,4];
- средняя (0,4;0,5];
- выше среднего (0,5;0,8];
- высокая [0,8;1).

В связи с тем, что уровни предприятий различны, следовательно, и ущерб будет иметь относительную количественную оценку. Распределение количественных оценок, в соответствии с качественными значениями уровня ущерба, приведено ниже:

- отсутствует [0;0,2);
- низкий (0,2;0,4];
- средний (0,4;0,5];
- выше среднего (0,5;0,8];
- высокий [0,8;1).

Далее рассчитывается сумма рисков реализации *i*-х угроз для *j*-го компонента:

$$E_{ij} = \sum_{i=1}^{n} I_{ij}, \quad (6)$$

где E_{ij} – сумма рисков от реализации угроз для *j*-го компонента;

I_{ij} – возможные риски реализации *i*-й угрозы для *j*-го компонента ИС.

Суммарная оценка защищенности ИС имеет следующий вид:

$$Z = \sum_{i=1}^{n} E_{ij}, \tag{7}$$

где E_{ij} – сумма возможных рисков реализации i-х угроз для j-го компонента;

Z – суммарная оценка защищенности ИС.

Качественная оценка защищенности ИС O_z определяется так:

$$O_z = \begin{cases} \text{не защищена, если } Z \in (40;90]; \\ \text{менее половины компонентов защищены, если } Z \in (20;40]; \\ \text{более половины компонентов защищены, если } Z \in (10;20]; \\ \text{защищена, если } Z \in (0;10]. \end{cases} \tag{8}$$

По результатам определения оценки защищенности ИС формируются рекомендации по улучшению защищенности ИС.

Метод оценки защищенности информации от НСД на основе экспертной информации имеет следующий алгоритм оценки защищенности ИС предприятия.

Исходными данными для оценки уровня защищенности ИС от НСД на основе экспертной информации являются перечень защищаемых компонентов ИС (9), а также интенсивность снижения защищенности и интенсивность восстановления защищенности:

$$K = \{k_1, ..., k_n\}, \tag{9}$$

где K – множество защищаемых компонентов ИС;

k_n – компоненты ИС, $n \in N$ – количество компонентов ИС.

Определены три группы угроз нарушения ИБ ИС:

$$The\_type = (C; I; A), \tag{10}$$

где C – группа угроз нарушения конфиденциальности ИС;

I – группа угроз нарушения целостности ИС;

A – группа угроз нарушения доступности ИС.

Интенсивности снижения защищенности компонентов ИС *Intens* рассчитываются для трех выбранных групп угроз нарушения ИБ ИС предприятия:

$$Intens = (\beta^C; \beta^I; \beta^A), \tag{11}$$

где β^C – интенсивность нарушения конфиденциальности;

β^I – интенсивность нарушения целостности;

β^A – интенсивность нарушения доступности для компонентов ИС.

Интенсивности нарушений защищенности компонентов ИС определяются экспертно.

Определяется интенсивность восстановления защищенности ИС после нарушения конфиденциальности, целостности, доступности:

$$Intens\_rec = (a^C; a^I; a^A), \tag{12}$$

где a^C – интенсивности восстановления конфиденциальности;

a^I –интенсивности восстановления целостности;

a^A – интенсивности восстановления доступности для компонентов ИС.

По результатам анализа рассчитываются показатели защищенности отдельных компонентов ИС. При этом расчет коэффициента защищенности компонентов ИС от угроз нарушения конфиденциальности осуществляется по формуле

$$\text{Sec\_coef}_{\text{i}}^{\text{C}} = \frac{\alpha_i^C}{\beta_i^C + \alpha_i^C}, \quad (13)$$

где $\text{Sec\_coef}_{\text{i}}^{\text{C}}$ – коэффициент защищенности информации, обрабатываемой в компонентах ИС, от угроз нарушения конфиденциальности;

α_i^C – интенсивности восстановления защищенности ИС после нарушения конфиденциальности;

β_i^C – интенсивность нарушения конфиденциальности информации.

Расчет коэффициента защищенности компонентов ИС от угроз нарушения целостности осуществляется по формуле

$$\text{Sec\_coef}_{\text{i}}^{\text{I}} = \frac{\alpha_i^I}{\beta_i^I + \alpha_i^I}, \quad (14)$$

где $\text{Sec\_coef}_{\text{i}}^{\text{I}}$ – коэффициент защищенности информации, обрабатываемой в компонентах ИС, от угроз нарушения целостности;

α_i^I – интенсивности восстановления защищенности ИС после нарушения целостности;

β_i^I – интенсивность нарушения целостности информации ИС.

Расчет коэффициента защищенности компонентов ИС от угроз нарушения доступности осуществляется по формуле

$$\text{Sec\_coef}_{\text{i}}^{\text{A}} = \frac{\alpha_i^A}{\beta_i^A + \alpha_i^A}, \quad (15)$$

где $\text{Sec\_coef}_{\text{i}}^{\text{A}}$ – коэффициент защищенности информации, обрабатываемой в компонентах ИС, от угроз нарушения доступности;

α_i^A – интенсивности восстановления защищенности ИС после нарушения доступности;

β_i^A – интенсивность нарушения доступности информации ИС.

На основе полученных показателей защищенности отдельных компонентов ИС проводится расчет показателей защищенности ИС предприятия в целом. Показатель защищенности ИС от угроз нарушения конфиденциальности рассчитывается по формуле

$$\text{Sec}_{\text{IS}}^{\text{C}} = \prod_{i=1}^{N} \text{Sec\_coef}_{\text{i}}^{\text{C}}, \quad (16)$$

где $\text{Sec}_{\text{IS}}^{\text{C}}$ – показатель защищенности всей ИС;

N – количество защищаемых компонентов;

$\text{Sec\_coef}_{\text{i}}^{\text{C}}$ – коэффициенты защищенности i-го компонента.

Показатель защищенности ИС от угроз нарушения целостности рассчитывается по формуле

$$\text{Sec}_{\text{IS}}^{\text{I}} = \prod_{i=1}^{N} \text{Sec\_coef}_{\text{i}}^{\text{I}}, \quad (17)$$

где $\text{Sec}_{\text{IS}}^{\text{I}}$ – показатель защищенности ИС;

N – количество защищаемых компонентов;

$\text{Sec\_coef}_{\text{i}}^{\text{I}}$ – коэффициенты защищенности i-го компонента.

Показатель защищенности ИС от угроз нарушения доступности рассчитывается по формуле

$$\mathrm{Sec}_{\mathrm{IS}}^{\mathrm{A}} = \prod_{i=1}^{N} \mathrm{Sec\_coef}_{\mathrm{i}}^{\mathrm{A}}, \tag{18}$$

где $\mathrm{Sec}_{\mathrm{IS}}^{\mathrm{A}}$ – показатель защищенности ИС;

N – количество защищаемых компонентов;

$\mathrm{Sec\_coef}_{\mathrm{i}}^{\mathrm{A}}$ – коэффициенты защищенности i-го компонента.

По результатам расчета показателя защищенности компонентов в ИС производится оценка уровня защищенности информации от НСД на основе экспертной информации по принятому критерию «защищенность». Качественная оценка защищенности ИС осуществляется по формуле (19):

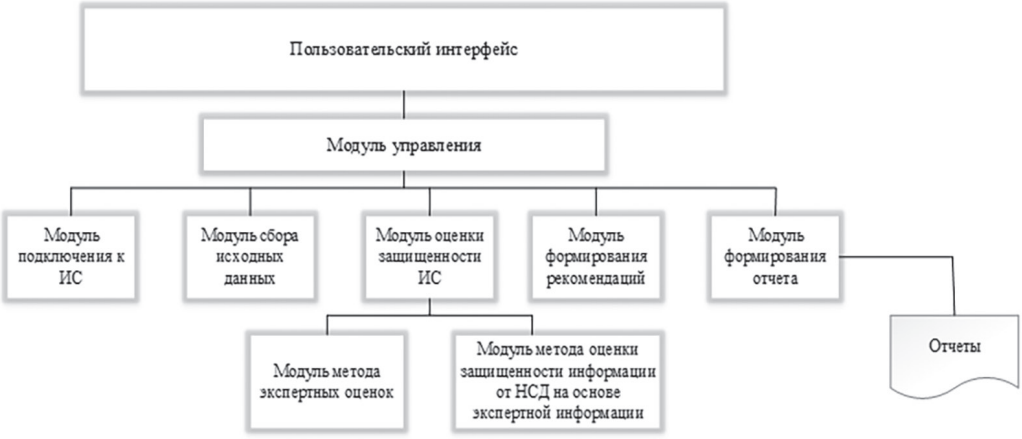
$$O_z = \begin{cases} \text{не защищена, если } \mathrm{Sec}_{IS}^{CLA} \in (0;0,5]; \\ \text{менее половины компонентов защищены, если } \mathrm{Sec}_{IS}^{CLA} \in (0,5;0,7]; \\ \text{более половины компонентов защищены, если } \mathrm{Sec}_{IS}^{CLA} \in (0,7;0,9]; \\ \text{защищена, если } \mathrm{Sec}_{IS}^{CLA} \in (0,9;1], \end{cases} \tag{19}$$

где Q_z – оценка защищенности ИС;

Sec_{IS}^{CLA} – показатель защищенности конфиденциальности, целостности и доступности всей ИС.

По результатам определения оценки защищенности ИС формируются рекомендации по улучшению защищенности ИС.

Сформированная математическая модель «Оценка защищенности информационной системы» позволит разработать программный комплекс оценки защищенности ИС предприятия. На основе описанной математической модели была разработана архитектура программного комплекса «Оценка защищенности информационной системы» (рис.).



Архитектура программного комплекса

Данная архитектура состоит из следующих модулей: пользовательский интерфейс, модуль управления, модуль подключения к ИС, модуль сбора исходных данных, модуль оценки защищенности ИС, модуль метода экспертных оценок, модуль метода оценки защищенности информации от НСД на основе экспертной информации, модуль формирования рекомендаций, модуль формирования отчета, документ отчетов.

На основе математической модели и архитектуры будет разработан программный комплекс «Оценка защищенности информационной системы». Планируется проведение ряда экспериментальных исследований, направленных на повышение защищенности информационной системы за счет корректной оценки защищенности ИС.

Литература

1. *Звонов Д.В., Нестерук Ф.Г., Осовецкий Л.Г.* К оценке уровня защищенности корпоративной сети // Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18, № 2. С. 156–159.
2. *Кравченко А.В.* Методика оценки эффективности информационных систем // Прикладная информатика. 2015. № 1 (55).
3. *Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В.* Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищенности // Труды СПИИРАН. 2012. Вып. 2. С. 41–55.
4. *Левцова А.А., Витенбург Е.А.* Методы оценки защищенности информационной системы // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: сборник материалов V Всероссийской научно-практической конференции (Волгоград, 27–28 апреля 2017 г.). Волгоград: Издательство ВолГУ, 2017. С. 55–58.
5. *Козунова С.С., Бабенко А.А.* Модель построения защищенной информационной системы корпоративного типа // Информационные системы и технологии. 2016. № 3 (95). С. 112–120.
6. *Витенбург Е.А., Пушкарская А.И., Оладько В.С.* Модель оценки безопасности на основе мониторинга информационной системы // Информационные системы и технологии. 2017. № 3 (101). С. 21–30.
7. *Зефиров С.Л., Щербакова А.Ю.* Оценка инцидентов информационной безопасности // Доклады ТУСУРА. 2014. № 2 (32). С. 77–81. URL: http://cyberleninka.ru/article/n/otsenka-intsidentov-informatsionnoy-bezopasnosti (дата обращения: 23.10.2017).
8. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1: Введение и общая модель.
9. *Полянский Д.А.* Комплексная защита объектов информации. Оценка защищенности: учебное пособие. 1-е изд. Владимир, 2005. С. 36–45.
10. ГОСТ Р ИСО/МЕК 15408-2-2001. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 2: Функциональные требования безопасности.

Literatura

1. *Zvonov D.V., Nesteruk F. G., Osovetsky L.G.* K otsenke urovnya zashchishchennosti korporativnoj seti // Nauchno-tekhnicheskij vestnik informatsionnykh tekhnologij, mekhaniki i optiki. 2018. T. 18, № 2. S. 156–159.

2. *Kravchenko A.V.* Metodika otsenki effektivnosti informatsionnykh sistem // Prikladnaya informatika. 2015. № 1 (55).
3. *Kozlenko A.V., Avramenko V.S., Saenko I.B., Kij A.V.* Metod otsenki urovnya zashchity informatsii ot NSD v komp'yuternykh setyakh na osnove grafa zashchishchennosti // Trudy SPIIRAN. 2012. Vyp. 2. S. 41–55.
4. *Levtsova A.A., Vitenburg E.A.* Metody otsenki zashchishchennosti informatsionnoj sistemy // Aktual'nye voprosy informatsionnoj bezopasnosti regionov v usloviyakh globalizatsii informatsionnogo prostranstva: sbornik materialov V Vserossijskoj nauchno-prakticheskoj konferentsii (Volgograd, 27–28 aprelya 2017 g.). Volgograd: Izdatel'stvo VolGU, 2017. S. 55–58.
5. *Kozunova S.S., Babenko A.A.* Model' postroeniya zashchishchennoj informatsionnoj sistemy korporativnogo tipa // Informatsionnye sistemy i tekhnologii. 2016. № 3 (95). S. 112–120.
6. *Vitenburg E.A., Pushkarskaya A.I., Olad'ko V.S.* Model' otsenki bezopasnosti na osnove monitoringa informatsionnoj sistemy // Informatsionnye sistemy i tekhnologii. 2017. № 3 (101). S. 21–30.
7. *Zefirov S.L., Shcherbakova A.Yu.* Otsenka intsidentov informatsionnoj bezopasnosti // Doklady TUSURA. 2014. № 2 (32). S. 77–81. URL: http://cyberleninka.ru/article/n/otsenka-intsidentov-informatsionnoy-bezopasnosti (data obrashcheniya: 23.10.2017).
8. GOST R ISO/MEK 15408-1-2002. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologij. Ch. 1: Vvedenie i obshchaya model'.
9. *Polyanskij D.A.* Kompleksnaya zashchita ob"ektov informatsii. Otsenka zashchishchennosti: uchebnoe posobie. 1-e izd. Vladimir, 2005. S. 36–45.
10. GOST R ISO/MEK 15408-2-2001. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Kriterii otsenki bezopasnosti informatsionnykh tekhnologij. Ch. 2: Funktsional'nye trebovaniya bezopasnosti.