СИСТЕМА ВЫБОРА СРЕДСТВ АНАЛИЗА И ОЦЕНКИ РИСКА

Светлана Казмирчук, Андрей Гололобов, Ксения Никитина

Національний авіаційний університет

КАЗМІРЧУК Світлана Володимирівна

Рік та місце народження: 1985 рік, м. Алмати, Казахстан.
Освіта: Національний авіаційний університет, 2006 рік.
Посада: асистент кафедри безпеки інформаційних технологій з 2006 року.
Наукові інтереси: інформаційна безпека, системи менеджменту інформаційної безпеки, захист програмного забезпечення, комплексні системи захисту інформації, управління інформаційними ризиками.
Публікації: понад 15 друкованих наукових праць, серед яких наукові статті у вітчизняних фахових виданнях, матеріали і тези доповідей на конференціях, навчально-методичні комплекси дисциплін та навчальний посібник.
E-mail: sv902@mail.ru

ГОЛОЛОБОВ Андрій Юрійович

Рік та місце народження: 1983, м. Київ, Україна.
Освіта: Національний технічний університет України «КПІ», 2006 рік.
Посада: здобувач кафедри безпеки інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека, програмування.
E-mail: b2d@ukr.net

НІКІТІНА Ксенія Вікторівна

Рік та місце народження: 1991 рік, с. Грозине, Коростенський р-н, Житомирська обл.
Освіта: Національний авіаційний університет 2012 рік.
Посада: магістрант кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, управління інформаційними ризиками.
E-mail: nik1991@ukr.net

Аннотация. *В работе представлены базовые критерии выбора средств анализа и оценки риска информационной безопасности. На основании этих критериев и модели интегрированного представления параметров риска, разработана структурная схема системы выбора средств анализа и оценки риска. Предложенное структурное решение стало основой программной реализации соответствующей системы. Она дает возможность, для практикующих в области защиты информации экспертов, более эффективно осуществлять выбор подходящего инструментария, что в свою очередь значительно упростит решение задач связанных с анализом и оценкой риска.*

Ключевые слова: *анализ и оценка риска, система выбора средств, критерии выбора, информационная безопасность.*

На сегодняшний день существует широкий спектр средств анализа и оценки риска (АОР), при выборе которых эксперт сталкивается с множеством вопросов касающихся выбора параметров и математического аппарата, осуществления оценивания на основе использования качественных статистических данных, в неопределенной, слабоформализованной среде и д.р. условиях. Эти и другие факторы создают ряд трудностей при выборе соответствующих средств оценивания. С учетом этого в работах [2-4] осуществлен анализ таких средств АОР на основе использования модели интегрированного представления параметров риска (ИППР) [1] с определением их идентифицирующих и оценочных компонент, которые в дальнейшем можно использовать для анализа и сравнения соответствующих разработок. Предложенный подход, дает возможность относительно ИППР унифицировать процесс анализа таких инструментальных средств АОР и повысить эффективность осуществления их выбора. На сегодняшний день подобные системы выбора, не интегрированы в одной среде и не учитывают модель ИППР. В этой связи, целью данной работы

является определение базовых критериев выбора средств АОР и разработка соответствующей системы. На основании анализа [2-4] предложены базовые критерии, по которым будет осуществляться выбор средств (табл. 1).

Таблица 1

Критерии выбора САОР

Название критерия	*Значения критерия*
Страна-разработчик	Великобритания, Канада, Германия, Россия, США, Франция
Сфера деятельности организации	Правительственные, коммерческие, некоммерческие
Язык	Английский, русский, немецкий, французский, испанский
Масштаб организации	Малые, средние, большие
Стандарты	ISO / IEC 17799, ISO / IEC 27001(BS 7799), ISO/IEC 27002, ISO / IEC 27005, NIST SP 800-30, BS7799-3: 2006, ГОСТ Р ИСО/МЭК 15408-2002
Количество этапов	2, 3, 4, 6, 7, 9
Идентифицирующие и оценочные компоненты для АОР	Модель ИППР
Исходящие данные	Генерация поэтапных отчетов, генерация общего отчета с оценкой рисков, список рекомендуемых мер защиты, политика безопасности организации

Модель ИППР, представлена в виде десятикомпонентного кортежа **<E, A, M, C, P, D, S, F, L, V>,** где **E** – событие, **A** – действие, **M** – мера риска, **C** – характеристика ситуации, **P** – вероятность, **D** – опасность, **S** – ситуация выбора, **F** – частота, **L** – затраты и потери (расходы), **V** – отклонение от цели. При выборе учитываться будут наиболее часто использованные параметры в средствах АОР [2-4], а именно E, A, M, C, P, D, F, L.

Первый приведённый в кортеже компонент – **событие (E),** который можно отображать в виде символьной переменной, принимающей одно из значений конечного множества идентификаторов $E \in \{E_1, E_2,\ldots,E_e\}$ (e – количество идентификаторов событий) при e=7 могут идентифицироваться как, E_1="Нарушение конфиденциальности (НК)", E_2="Нарушение целостности (НЦ)", E_3="Нарушение доступности (НД)", E_4="Нарушение целостности и конфиденциальности (НЦК)" E_5="Нарушение целостности и доступности (НЦД)" E_6="Нарушение конфиденциальности и доступности (НКД)" E_7="Нарушение конфиденциальности, целостности и доступности (НКЦД)".

Следующий компонент кортежа – **действие (A),** которое привело к событию **E**. С точки зрения ИБ **A** связано с реализацией потенциальных **угроз** базовым характеристикам безопасности, которые привели к возникновению **E,** отображаемого одним из идентификаторов $\{E_1, E_2,\ldots,E_7\}$. В связи с этим, по аналогии с **E,** компонент **A** можно отобразить множеством идентификаторов $A \in \{A_1, A_2,\ldots,A_a\}$ (где a – количество идентификаторов угроз), например, A_1="Компьютерный шпионаж", A_2="Шпионаж", A_3="Сбой программного обеспечения" и т.д.

Для измерения риска в сфере ИБ обычно используются качественные и количественные шкалы. В этой связи, компонент **M,** с учетом характера измерений в области ИБ, можно отобразить трехкомпонентным множеством $M \in \{M_{кл}, M_{кч}, M_{и}\}$, где $M_{кл}$ – количественная (например, характеризуемая численно), $M_{кч}$ – качественная (например, характеризуемая лингвистически) и $M_{и}$ – интегрированная (например, характеризуемая численно и лингвистически) меры.

Рассматривая компонент кортежа **характеристика ситуации (C),** можно отобразить его двухкомпонентным множеством $C \in \{C_o, C_н\}$ где, C_o – характеризирует ситуацию как определённую, а $C_н$ – как нечеткую.

Четвертый компонент кортежа **вероятность (P)** появления события **E (**например, с идентификатором E_3). Эксперты используя логико-лингвистический подход отображают этот компонент через лингвистическую переменную (ЛП) [1] "ВЕРОЯТНОСТЬ" с базовым терм-множеством $\mathbf{P} = \bigcup_{i=1}^{p} P_i$ (p – количество термов), для членов которого справедливо отношение порядка $P_1<P_2<\ldots<P_p$.

Компонент кортежа **опасность (D)** рассматривается как величина характеризующая опасность события. По аналогии с **P** компонент **D** может отображаться численно (например, в процентах) или с помощью ЛП – "ОПАСНОСТЬ" с базовым терм-множеством $\mathbf{D} = \bigcup_{i=1}^{d} D_i$ ($D_1<D_2<\ldots<D_d$).

Следующий компонент кортежа **частота (F),** который в области ИБ связывается с частотой реализации "угрозы", приведшей к событию **E**, можно отображать численно или через ЛП – "ЧАСТОТА": $\mathbf{F} = \bigcup_{i=1}^{f} F_i$ ($F_1<F_2<\ldots<F_f$).

Компонент **затраты и потери** в области ИБ целесообразно определить через термин **расходы (L),** который по аналогии с предыдущим можно представлять числено, например, 1) 0 - $100; 2) $100 - $1000; 3) $1000 - $10 000; 4) $10 000 - $100 000, при этом **мере** соответствует $M_{кл.}$ Также **L** можно представить с помощью ЛП "РАСХОДЫ": – $\mathbf{L} = \bigcup_{i=1}^{l} L_i$ ($L_1<L_2<\ldots<L_l$).

Следует отметить, что при представлении риска, с помощью кортежа, можно выделить его идентифицирующие **E, A, M, C** и оценочные компоненты **P**, **D**, **F** и **L**. Описания использованных компонент в качестве критериев для выбора средств АОР закончено, теперь прейдем к описанию структурной схемы системы выбора.

На основании критериев предлагается структурная схема системы выбора средств АОР (рис. 1), которая содержит базу данных (БД) с четырьмя таблицами: систем АОР, в которой размешен список

средств Z_k ($k=\overline{1,26}$, где k – указатель (номер) текущего идентификатора средства АОР); названий критериев выбора K_i ($k=\overline{1,9}$, где i – указатель (номер) текущего идентификатора критерия) (табл. 1); значений критериев P_{ij}, где j – указатель (номер) текущего идентификатора критерия $j=\overline{1,n}$, а n – количество критериев; общей собранной справочной информацией о каждом средстве АОР.

В модуле процесса выборки (МПВ) осуществляется выбор согласно определенным критериям и их значению, которые удовлетворяют эксперта. В него поступают данные из таблицы со средствами, критериями и их значениями с помощью интерфейса (рис. 2). Эти данные обрабатываются и после этого передаются в модуль генерации отчета (МГО), где формируется список подходящих средств АОР Z_k с поступившей из соответствующей таблицы справочной информацией к ним (рис. 3).

Работу представленной системы выбора можно представить в виде четырех этапов.

Этап 1. Определение критериев и выбор их значений. Здесь вначале задаются девять критериев, по которым в дальнейшем будет осуществляться выборка. После этого устанавливаются связи с таблицами БД, в которых хранится информация о критериях и их порядковые номера. Далее каждому из критериев присваивается значение i, которые заносятся и хранятся в соответствующей таблице. Если при выборе их значений происходит пропуск хотя бы одного из критериев, система выводит сообщение "Не для всех критериев выбрано значение!" и система возвращается на предыдущий этап.

Этап 2. Проверка выбранных значений. После окончания выбора экспертом значений критериев осуществляется переход к формированию отчета, для этого осуществляется проверка наличия выбранных значений для каждого из 9 критериев.

Этап 3. Проверка соответствий выбранных значений и данных в БД. Здесь осуществляется проверка соответствий значений критериев со значениями средств АОР. Эти соответствия заносятся в таблицу МВП.

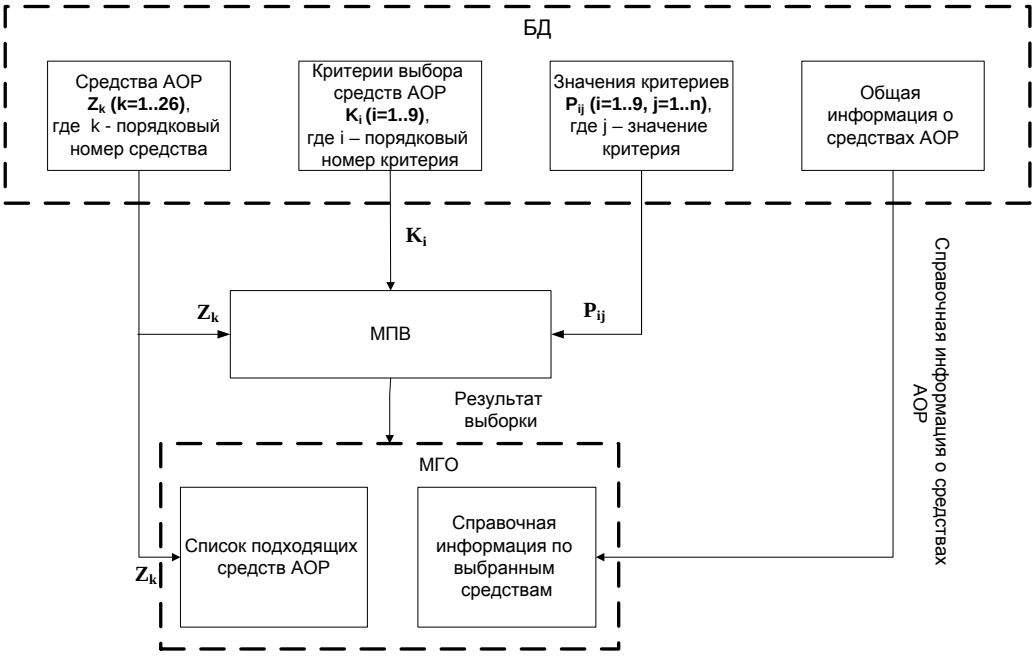

Рис. 1 Структурная схема системы выбора средств АОР

Этап 4. Подбор подходящих средств. На этом этапе система функционирует на основе таблицы МВП. Для формирования окончательного результатов устанавливается фильтр, который осуществляет подбор наиболее часто встречаемых в МВП средств АОР (по 7-9 критериям). Далее их названия заносится в отчет, где приведен перечень подходящих средств АОР со справочной информацией и основными их характеристиками.

Представленная система дает возможность более эффективно с учетом модели ИППР осуществить выбор подходящих средств АОР, что в свою очередь значительно упростит данную задачу для практикующих в области защиты информации экспертов.

Рис. 2 Окно выбора критериев

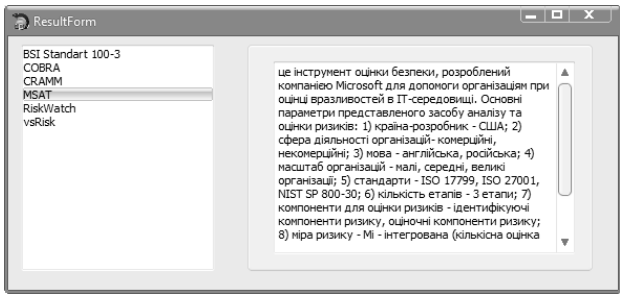

Рис. 3 Окно результатов выбора

Литература

[1] Корченко А.Г. Интегрированное представление параметров риска / Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации. – 2011. – №1 (50). – С. 96 – 101.

[2] Луцкий М.Г. Исследование программных средств анализа и оценки риска информационной безопасности / Луцкий М.Г., Корченко А.Г., Иванченко Е.В., Казмирчук С.В. // Защита информации. – 2011. – №3. – С. 97-108.

[3] Луцкий М.Г. Современные средства управления информационными рисками / Луцкий М.Г., Иванченко Е.В., Корченко А.Г., Казмирчук С.В., Охрименко А.А. // Защита информации. – 2012. – №1. – С. 5-16.

[4] Скульш Е.Д. Средства анализа и оценки риска информационной безопасности / Скульш Е.Д., Корченко А.Г., Горбенко Ю.И., Казмирчук С.В. // Інформаційна безпека. Людина, суспільство, держава. – 2011. – №3 (7). – С.31-48.

УДК 004.056.5 (045)

Казмірчук С.В., Гололобов А.Ю., Нікітіна К.В. Система вибору засобів аналізу та оцінки ризику
Анотація. *В роботі представлені базові критерії вибору засобів аналізу та оцінки ризику інформаційної безпеки. На підставі цих критеріїв і моделі інтегрованого представлення параметрів ризику, розроблена структурна схема системи вибору засобів аналізу та оцінки ризику. Запропоноване структурне рішення стало основою програмної реалізації відповідної системи. Вона дає можливість, для практикуючих в області захисту інформації експертів, більш ефективно здійснювати вибір відповідного інструментарію, що в свою чергу значно спростить вирішення завдань пов'язаних з аналізом і оцінкою ризику.*
Ключові слова: *аналіз і оцінка ризику, система вибору засобів, критерії вибору, інформаційна безпека.*

Kazmirchuk S.V., Gololobov A.Yu., Nikitina K.V. The system selection of the analysis methods and risk assessment
Abstract. *The paper represents the basic criteria for the selection of the analysis methods and Information security risk assessment. Based on these criteria and models for the integrated risk parameters presentation, it was created a structural diagram of the analysis methods and risk assessment selection. The proposed structural solution has become the basis for program implementation of the corresponding system. It provides the opportunity for practicing experts in the information security sphere, to carry out a choice of suitable toolkit more effectively, that in turn will significantly simplify the risk analysis and assessment problem solving.*
Keywords: *risk analysis and assessment, selection systems, selection criteria, information security*

Отримано *17 березня 2012 року*, затверджено редколегією *08 червня 2012 року*
(рецензент д.т.н., професор О.Г. Корченко)

БАГАТОЦІЛЬОВА ОПТИМІЗАЦІЯ В ЗАДАЧАХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ЧІТКИЙ І НЕЧІТКИЙ ПІДХОДИ

Мирослав Демчишин, Євгеній Левченко

Національний авіаційний університет

ДЕМЧИШИН Мирослав Володимирович

Рік та місце народження: 1988 рік, м. Луцьк, Україна.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: аспірант кафедри засобів захисту інформації.
Наукові інтереси: інформаційна безпека, математичне моделювання.
Публікації: 10 публікацій, серед яких наукові статті, тези доповідей.
E-mail: miroslawchuk@bigmir.net