Сравнительный анализ программного обеспечения для анализа рисков информационной безопасности в соответствии с ГОСТ Р ИСО/МЭК 27005-10

Е. К. Баранова[I], А.А. Мурзакова[II], Е.А. Мурзакова[II]

[I] Финансовый университет при Правительстве РФ; Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия
[II] Национальный исследовательский университет «Высшая школа экономики», г. Москва, Россия

Аннотация. Рассматриваются методики анализа рисков информационной безопасности согласно ГОСТ Р ИСО/МЭК 27005-10. Проводится сравнительный анализ программного инструментария Ra2, Vsrisk и MSAT на основании выделенных критериев.

Ключевые слова: информационная безопасность, анализ и управление рисками, Ra2, Vsrisk, MSAT, угрозы, уязвимости, механизмы контроля.

DOI 10.14357/20718632190208

Введение

Инструментальные средства и методики управления рисками информационной безопасности (ИБ) направлены на то, чтобы определить параметры риска, провести анализ рисков и дать им оценку, а также определить стратегию управления рисками.

Выделяют базовый и полный анализ рисков. Базовый анализ рисков применим в случае типовых проектных решений, когда предъявляемые требования минимальны и допустимы качественные оценки риска. При повышенных требованиях по безопасности применим полный анализ рисков, включающий количественные показатели оценки рисков.

Базовый (baseline) анализ рисков проводится в соответствии с требованиями базового уровня защищенности. Прикладные методы анализа рисков, ориентированные на данный уровень, обычно не рассматривают ценность ресурсов и не оценивают эффективность контрмер. Методы данного класса применяются в случаях, когда к информационной системе не предъявляется повышенных требований в области ИБ.

Полный (full) анализ рисков применим для информационных систем, предъявляющих повышенные требования в области ИБ, и включает в себя определение ценности информационных ресурсов, оценку угроз и уязвимостей, выбор адекватных контрмер, оценку их эффективности [1-3].

В рамках обеспечения информационной безопасности перед специалистами ИБ и руководителями компаний встают вопросы о подборе эффективных средств анализа рисков, действующих в соответствии с текущими требованиями нормативно-правовой базы по информационной безопасности, в частности, по анализу рисков и управлению ими. Это один из

способов оценки необходимого уровня инвестиций в ИБ. В работе рассматриваются программные комплексы по анализу рисков в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности». Обозначенный стандарт включает в себя менеджмент рисков ИБ, составленный в плане требований к системе менеджмента информационной безопасности (СМИБ) согласно ГОСТ Р ИСО/МЭК 27001. Как указано в данном стандарте: «Выбор подхода к менеджменту риска осуществляется организацией и зависит, например, от области применения СМИБ, контекста менеджмента риска или сферы деятельности». Рассмотрим ряд современных программных комплексов для анализа рисков: Ra2, Vsrisk и MSAT.

1 Ra2 art of risk

Инструментарий для оценки и управления информационными рисками Ra2 art of risk, разработан компаниями AEXIS Security Consultants и XiSEC Consultants Ltd. Разработчиками программного инструментария являются Тэд Хамфриз (Ted Humphreys) и Анжелика Плейт (Angelika Plate) – редакторы стандарта BS 7799, ISO 27001 и ISO 17799, авторы руководств Британского Института Стандартов по внедрению стандартов серии 27000 (BIP 0071-0074). Ra2 art of risk реализует процессный подход и предусматривает возможность адаптации к потребностям определенной организации.

Построение СМИБ включает в себя такие этапы, как сбор информации, оценка рисков и последующая их обработка, внедрение мер по обеспечению безопасности, механизмов контроля (Рис. 1). После завершения процесса проектирования и внедрения системы управления ИБ Ra2 дает возможность для создания архива с функцией хранения результатов, выступающих ценным материалом для проводимых в будущем оценок информационных рисков [4].

Программный комплекс призван решать следующие задачи [5]:

– определять область действия, политику, цели СУИБ;

– разрабатывать реестр активов СУИБ и проводить их оценку;

– оценивать угрозы и уязвимости СУИБ;

– идентифицировать и оценивать риски СУИБ;

– принимать решения по обработке рисков (подбираются контрмеры из приложения А к стандарту BS 7799-2);

– проводить анализ расхождения со стандартом ISO 27002;

– заниматься формированием документов СУИБ, включая Декларацию о применимости;

– внедрять выбранные защитные меры и средства управления.

Во вкладке меню Navigation –> 1. ISMS Scope and Risk Assessment Scales -> 1.3. Risk

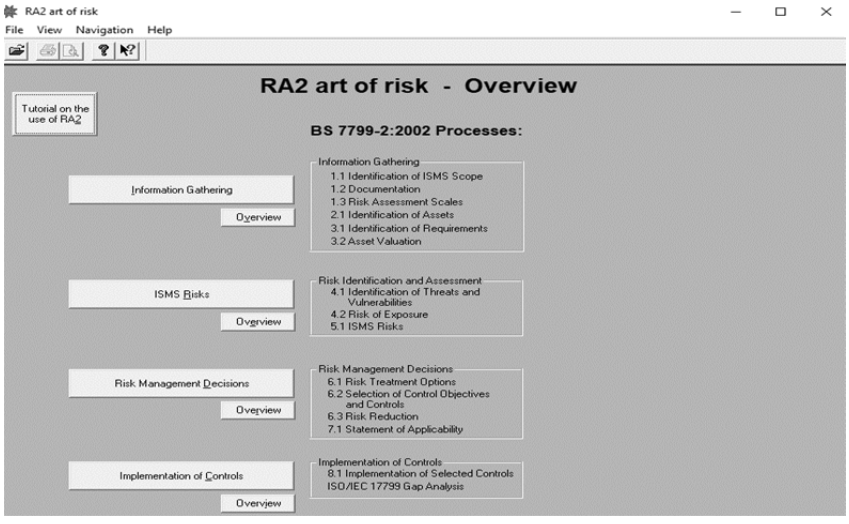

Рис. 1. Этапы риск-менеджмента в Ra2

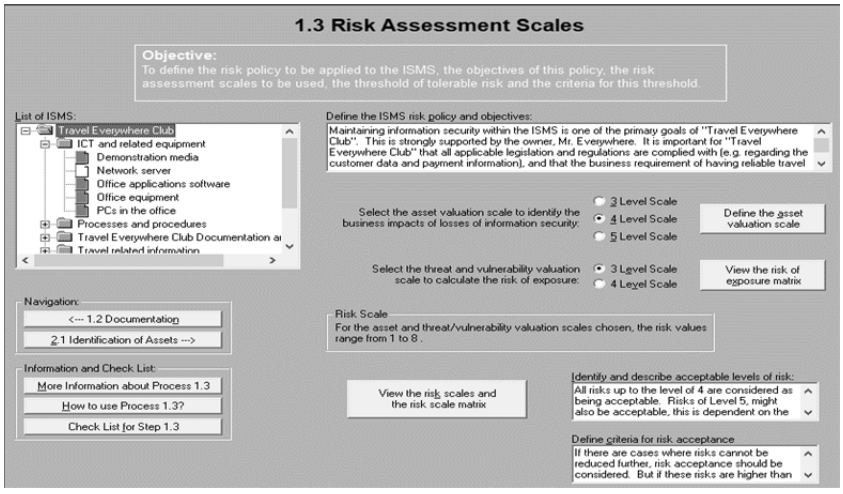

Рис. 2. Шкалы по анализу рисков в Ra2

Assessment Scales (Шкалы по анализу рисков, Рис. 2) можно выбрать шкалу оценки активов для определения степени влияния на потери, связанные с ИБ. Для активов, угроз, уязвимостей выбирается шкала оценки; риск ранжируется от 1 до 8.

В окне «Risk scale» (Шкала рисков) можно выбрать соответствующий уровень риска (Рис. 3) – незначительный, минимальный, значительный, наиболее значимый, катастрофический.

Матрица уровней риска основана на шкалах оценки активов, выбранных для активов, угроз и уязвимостей. В столбцах матрицы указывается RoE (риск воздействия), а в строках – Business Impact (масштаб влияния на бизнес). RoE и Business Impact представлены качественными шкалами. RoE со значениями от «очень низкий» до «очень высокий», а Business Impact – «низкий», «ниже среднего», «выше среднего», «высокий».

2. Vsrisk

Если комплекс Ra2 art of risk предполагает качественные оценки, то Vsrisk – смешанная методика, которая была разработана британской компанией IT Governance совместно с компанией Vigilant Software. Инструментарий базируется на стандарте ISO 27001, как и Ra2. При этом поддерживает такие стандарты, как ISO/IEC 27002, BS7799-3:2006, ISO/IEC TR 13335-3:1998, NIST SP 800-30.

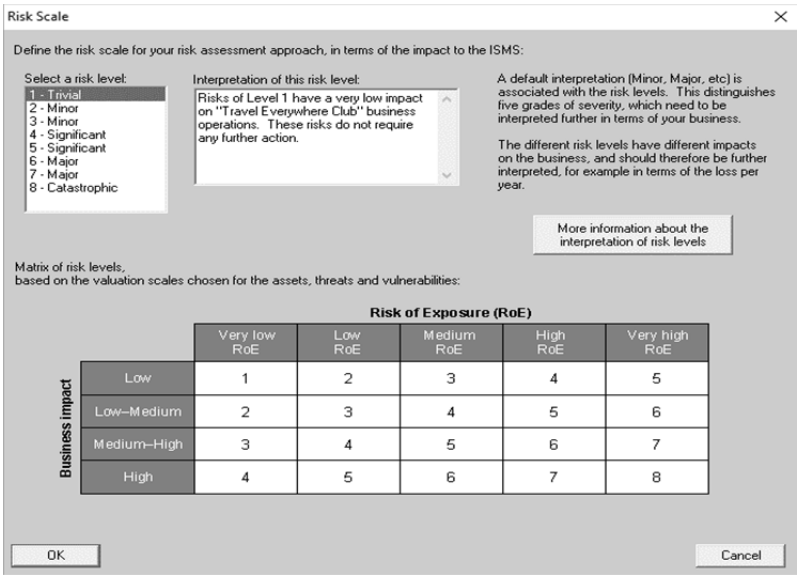

Рис. 3. Матрица уровней риска в Ra2

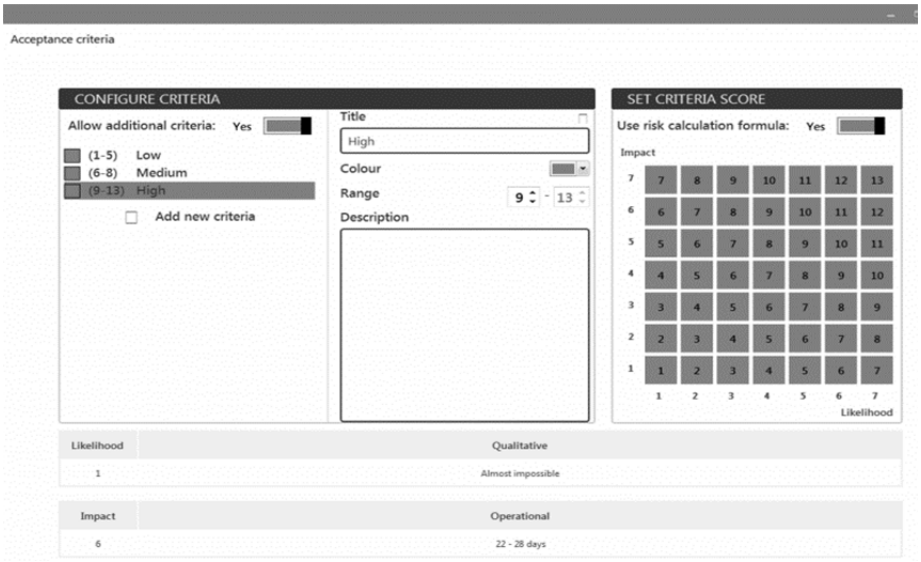

Рис. 4. Настройка критериев оценки рисков в Vsrisk

Vsrisk предназначен для оценки рисков нарушения конфиденциальности, целостности и доступности информации (Рис. 4). В программном комплексе присутствует возможность оценки всех факторов рисков, активов, угроз, уязвимостей и механизмов контроля [6]. По угрозам и уязвимостям содержится интегрированная, систематически обновляемая база данных. В журнале аудита программного инструментария отмечаются все изменения в базе данных, которые были внесены туда в процессе работы. Рассматриваемое средство анализа рисков дает возможность в итоге получить Декларацию о применимости механизмов контроля и План обработки рисков (в соответствии с требованиями ISO 27001).

В Vsrisk между угрозами и относящимися к ним типами уязвимостей и активов отсутствует связь. Так приходится производить выборку среди угроз, применимых к каждому рассматриваемому активу компании, из полного перечня угроз, где могут встретиться угрозы, не имеющие никакого отношения к этим типам активов, что повышает трудоемкость работы с программным инструментарием. Также среди минусов программного инструментария можно выделить такие, как отсутствие возможности добавлять поясняющие комментарии к тому, по какой причине были выбраны значения вероятности угроз и уязвимостей, а также тот факт, что механизмы контроля описаны только наименованием и целью. В Vsrisk отсутствуют средства для построения модели активов, которые не являются связанными друг с другом. Например, актив «сервер» в таком случае не связан с теми программными приложениями, которые установлены на нем, что при оценке ущерба от технических проблем сервера приведет к необходимости помнить обо всех связях сервера с другими активами – только так можно правильно оценить ущерб и последствия таких ситуаций для других активов. Между тем, Vsrisk обладает достаточно простым и интуитивно понятным пользовательским интерфейсом.

На первом этапе анализа и оценки рисков идет выбор масштаба воздействия и шкалы вероятности для каждой комбинации угроза/уязвимость. Далее устанавливаются критерии принятия риска в соответствии с требованиями, назначаются владельцы активов, определяются группы и подгруппы активов. Далее указывается возможность доступа к каждому активу, приводящая к нарушению конфиденциальности, целостности или доступности. В Vsrisk можно производить работу с помощью программы-мастера для ускорения процесса оценки рисков (Рис. 5). Встроенные угрозы, уязвимости и контрольные списки проверяются на соответствие стандарту ISO 27001:2005. Далее производится регистрация угроз, уязвимостей и мер контроля. На последнем этапе по результатам анализа формируется Положение о применимости и подробный отчет по всем недочетам.

Рис. 5. Программа «Мастер анализа рисков»

3. MSAT

Средство для оценки безопасности MSAT (Microsoft Security Assessment Tool), как и Vsrisk обладает смешанной шкалой оценивания. Программный инструментарий MSAT подходит организациям, в которых число сотрудников не превышает 1000 человек [7]. Эта методика с целостным подходом к измерению уровня безопасности направлена на определение и устранение угроз ИБ, а также на изучение инфраструктуры, персонала, процессов и технологий (Рис. 6). Методика включает более 200 вопросов, наряду с которыми относящиеся к ним решения и рекомендации выводятся из общепринятых практических рекомендаций, стандартов ISO 17799 и NIST-800.x, указаний от группы надежных вычислений Microsoft и других источников по информационной безопасности. Заполненные пользователем ответы на вопросы методики могут быть отправлены на защищенный веб-сервер MSAT, где результаты будут конфиденциально обработаны, выполнена оценка рисков и предоставлены рекомендации по повышению эффективности системы обеспечения ИБ.

MSAT предоставляет инфраструктуру эшелонированной защиты (технический, организационный и рабочий контроль), которая соответствует отраслевым стандартам, систематические отчеты по сопоставлению базовых показателей с полученными результатами, проверенные рекомендации и упорядоченные в соответствии с приоритетами корректирующие меры по улучшению.

Перед началом использования программного инструментария MSAT необходимо создать профиль, который включает несколько основ-

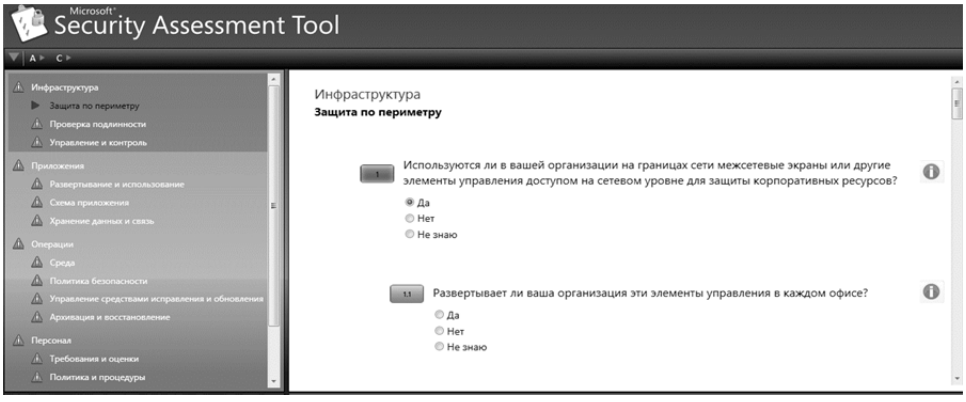

Рис. 6. MSAT. Вопросы по разделам

ных вопросов о компании и полную оценку профиля риска для бизнеса (ПРБ). Первые вопросы в методике связаны с основными сведениями о компании (параметры компании), далее следуют вопросы по безопасности инфраструктуры, приложений, операций, безопасности персонала, вопросы, касающиеся среды (рабочих процедур, процессов и рекомендаций, примененных к среде), которые формируют профиль риска для бизнеса. Вторая часть вопросов помогает получить комплекс мер ИБ, формирующих уровни защиты, которые вносят вклад в комбинированную стратегию глубокой защиты. Сумма уровней защиты носит название – индекс глубокой защиты (DiDI). Профиль риска для бизнеса сопоставляется с индексом глубокой защиты для распределения угроз по анализируемым четырем сферам, помогая лучше изучить персонал, процессы, ресурсы и технологии компании, которые направлены на обеспечение эффективного планирования мероприятий по безопасности и внедрение методов снижения риска в компании. На выходе получаем как сводный отчет (с диаграммой «Сравнение риска и защиты» по параметрам ПРБ и DiDI), так и полный отчет с подробным разбором по всем разделам с пояснениями, что в компании является неудовлетворительным и что требует усовершенствования. Полный отчет дает подробную оценку по всем четырем основным областям, предоставляя рекомендации в приоритетном порядке по значимости. Также предоставляется доступ к возможности сопоставления двух полученных оценок – прошлой и текущей для контроля прогресса изменений уровня риска.

Итак, данная методика анализа рисков ИБ включает этап планирования (формирование основы для проведения успешной оценки рисков), этап координированного сбора данных о рисках, ранжирование рисков. Однако MSAT не рассчитывает эффективность используемых мер ИБ, и рекомендации, полученные по итогу, применимы именно в качестве первичной, предварительной инструкции, которая дает возможность сделать акцент на конкретных, требующих более глубокого изучения, областях.

4. Сравнение ПО для анализа рисков ИБ

На Рис. 7 представлена лепестковая диаграмма сравнения Ra2, Vsrisk и MSAT по таким критериям, как «Стоимость», «Поддерживаемые стандарты», «Простота использования», «Функционал», «Риски», «Использование элементов риска», «Способы измерения величин рисков» и «Применение мониторинга рисков ИБ».

Сравнение рассмотренных выше методик анализа риска представлено в Табл.1.

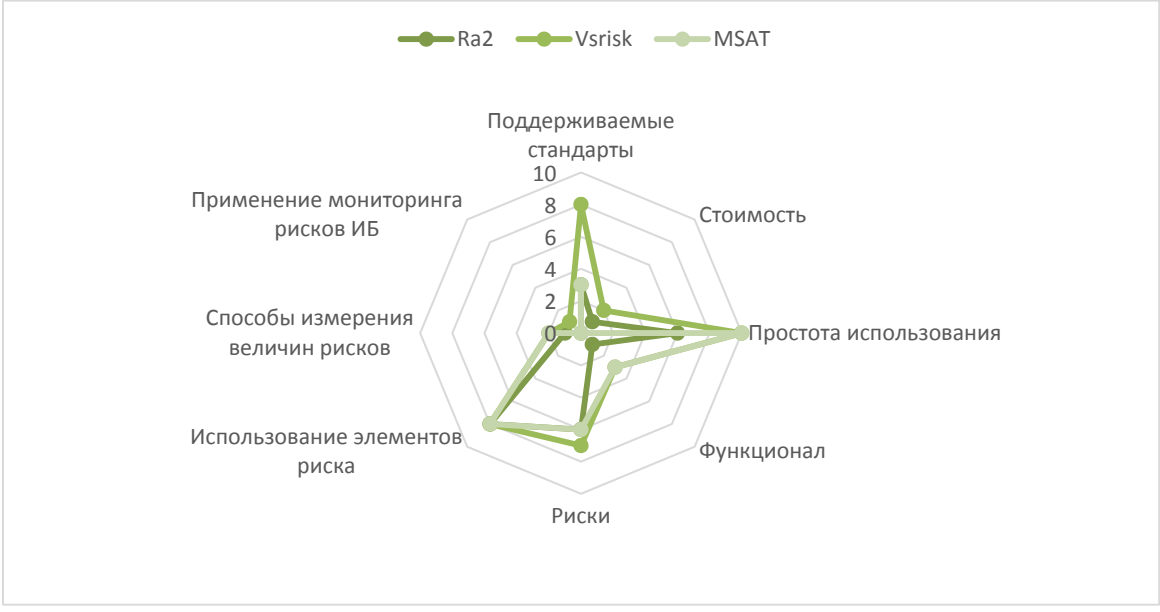

Рис. 7. Диаграмма сравнения Ra2, Vsrisk и MSAT по базовым критериям оценки

Табл. 1. Сравнение ПО для анализа рисков ИБ

Критерии сравнения	Ra2	Vsrisk	MSAT
Стоимость	1500$	2000$	бесплатно
Поддержка стандартов	ISO 27001 (BS 7799-2), ISO 17799	ISO 27001:2005, ISO 27001:2013, ISO 27032:2012, NIST 800-53, CSA CCM v3, PCI DSS v3, Cyber Essentials	ISO 17799, NIST-800.x
Соответствие ГОСТ Р ИСО/МЭК 27005-2010	+	+	+
Применимость к компаниям малого и среднего бизнеса	+	+	+
Простота использования	60 %	100 %	100 %
Операционная совместимость	ОС Windows	ОС Windows	ОС Windows
Функционал			
Наличие демоверсии	+	+	-
Обновляемая база угроз и уязвимостей	-	+	+
Экспорт отчетов	-	+	+
Поддержка русского языка	-	-	+
Наличие программы «Мастер анализа рисков»	-	+	-
Риски			
Использование категорий рисков	+	+	+
Использование понятия максимально допустимого риска	+	+	+
Подготовка плана мероприятий по снижению рисков	-	+	+
Оценка бизнес-рисков/операционных рисков/ИТ-рисков	+	+	-
Оценка рисков на организационном уровне	+	+	+
Перенос риска	+	-	-
Снижение риска	+	+	+
Сохранение риска	+	+	+
Процессы			
Использование элементов риска			
Материальные активы	+	+	+
Нематериальные активы	+	+	+
Угрозы	+	+	+
Ценность активов	+	+	+
Уязвимости	+	+	+
Меры безопасности	+	+	+
Потенциальный ущерб	+	+	+
Вероятность реализации угроз	+	+	+
Способы измерения величин рисков			
Качественная оценка	+	+	+
Количественная оценка	-	+	+
Мониторинг рисков			
Применение мониторинга эффективности мер ИБ	+	+	-

Заключение

В настоящее время необходимость проведения процедуры анализа и оценки рисков ИБ не вызывает сомнения. Компаниям необходимо получать не только результаты первоначальной оценки рисков ИБ, рекомендации по их снижению, но и простой в использовании инструмент такой оценки. Вопрос упирается, в основном, в необходимость инвестиций, как в проведение самой процедуры анализа и оценки рисков, так и в приобретение программного инструмента-

рия для этих целей и наличие квалифицированных специалистов для проведения процедуры.

Сравнительный анализ комплексов Ra2, Vsrisk, MSAT показал, что они применимы для всех типов компаний и направлены на соблюдение рыночных требований непрерывности и безопасности деятельности организации.

Ra2 является эффективной системой поддержки принятия решений по управлению информационными рисками для современного бизнеса. Данный программный инструментарий в отличие от Vsrisk и MSAT имеет демоверсию, но не имеет обновляемой базы угроз и уязвимостей.

Инструмент оценки безопасности Vsrisk ограничен качественными шкалами, задаваемыми пользователем, так как в нем отсутствуют средства для количественной оценки риска. Между тем, у Vsrisk достаточно простой и понятный пользовательский интерфейс, как и у MSAT.

MSAT – простое, экономичное средство для повышения эффективности ИБ вычислительной среды компании. В отличие от Vsrisk и Ra2, MSAT поддерживает русскоязычную версию. MSAT разработан для среднего размера организаций, которые содержат от 50 до 1500 настольных систем, и предназначен для большого диапазона областей потенциального риска в среде, а не для обеспечения глубокого анализа определенных технологий или процессов. Данный инструментарий рекомендуется к использованию в качестве предварительного руководства.

Таким образом, все три методики представляют собой достаточно эффективные, полезные инструментарии, являющиеся качественными помощниками в управлении рисками. Выбор конкретного программного средства зависит, в первую очередь, от потребностей, финансовых возможностей компании и ее инфраструктуры. Проведенный сравнительный анализ поможет компаниям упростить процедуру выбора методики анализа рисков.

Литература

1. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. №1 (9). С. 73-79.
2. Баранова Е. К. Особенности подхода к анализу рисков информационной безопасности в малом и среднем бизнесе // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. 2016. № 7-8. С. 146-152.
3. Бабаш А. В., Баранова Е. К. Актуальные вопросы защиты информации: Монография. М. : ИНФРА-М, РИОР, 2017.
4. RA2 art of risk. Искусство управления информационными рисками. Обзор методов и инструментальных средств управления рисками [Электронный ресурс]. – Режим доступа: http://анализ-риска.рф/content/ra2-art-risk. – (Дата обращения: 16.03.2019).
5. Луцкий М.Г. Современные средства управления информационными рисками // Защита информации. 2012. №1. С. 11-23.
6. vsRisk. Искусство управления информационными рисками. Обзор методов и инструментальных средств управления рисками [Электронный ресурс]. – Режим доступа: http://анализ-риска.рф/content/vsrisk. – (Дата обращения: 18.03.2019).
7. Годла А.С., Губенко Н.Е. Оценка рисков информационной безопасности на примере малых предприятий // Секция 8. Компьютерные технологии информационной безопасности. 2013. №1. С. 221-222.

Баранова Елена Константиновна. Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ), г. Москва, Россия. Доцент кафедры информационной безопасности. Количество печатных работ: 93 (из них 2 монографии). Область научных интересов: управление информационной безопасностью, защита информации. E-mail: ekbaranova@hse.ru

Мурзакова Александра Андреевна. Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ), г. Москва, Россия. Магистрант кафедры информационной безопасности. Количество печатных работ: 2. Область научных интересов: управление информационной безопасностью, защита информации. E-mail: aamurzakova@edu.hse.ru

Мурзакова Екатерина Андреевна. Национальный исследовательский университет «Высшая школа экономики» (НИУ ВШЭ), г. Москва, Россия. Магистрант кафедры информационной безопасности. Количество печатных работ: 2. Область научных интересов: управление информационной безопасностью, защита информации. E-mail: eamurzakova@edu.hse.ru

Modern software tools for information security risks management ISO/IEC 27005

E. K. Baranova[I], A.A. Murzakova[II], E.A. Murzakova[II]

[I] Financial University under the Government of the Russian Federation, Moscow, Russia; National Research University "Higher School of Economics", Moscow, Russia
[II] National Research University "Higher School of Economics", Moscow, Russia

Abstract. Information security risks analysis methods are considered in accordance with GOST R ISO / IEC 27005-10. A comparative analysis of Ra2 software, Vsrisk software and MSAT software are carried out based on the selected criteria.

Keywords: information security, analysis and risk management, Ra2, Vsrisk, MSAT, threats, vulnerabilities, control mechanisms.

DOI 10.14357/20718632190208

References

1. Baranova E.K. Metodiki analiza i ocenki riskov informacionnoj bezopasnosti // Obrazovatel'nye resursy i tekhnologii. 2015. №1 (9). S. 73-79.
2. Baranova E. K. Osobennosti podhoda k analizu riskov informacionnoj bezopasnosti v malom i srednem biznese // Voprosy oboronnoj tekhniki. Seriya 16: Tekhnicheskie sredstva protivodejstviya terrorizmu. 2016. № 7-8. S. 146-152.
3. Babash A. V., Baranova E. K. Aktual'nye voprosy zashchity informacii: Monografiya. M. : INFRA-M, RIOR, 2017.
4. RA2 art of risk. Iskusstvo upravleniya informacionnymi riskami. Obzor metodov i instrumental'nyh sredstv upravleniya riskami [Elektronnyj resurs]. – Rezhim dostupa: http://analiz-riska.rf/content/ra2-art-risk. – (Data obrashcheniya: 16.03.2019).
5. Luckij M.G. Sovremennye sredstva upravleniya informacionnymi riskami // Zashchita informacii. 2012. №1. S. 11-23.
6. vsRisk. Iskusstvo upravleniya informacionnymi riskami. Obzor metodov i instrumental'nyh sredstv upravleniya riskami [Elektronnyj resurs]. – Rezhim dostupa: http://analiz-riska.rf/content/vsrisk. – (Data obrashcheniya: 18.03.2019).
7. Godla A.S., Gubenko N.E. Ocenka riskov informacionnoj bezopasnosti na primere malyh predpriyatij // Sekciya 8. Komp'yuternye tekhnologii informacionnoj bezopasnosti. 2013. №1. S. 221-222.

Baranova E. C. National Research University "Highest School of Economics" (HSE), Moscow, Russia**.** Information security department Associate Professor. Associate Professor**.** Number of printed paper: 93 (of them there are 2 monographs)**.** Research interests: information security management, information protection**.** E-mail: ekbaranova@hse.ru

Murzakova A. A. National Research University "Highest School of Economics" (HSE), Moscow, Russia. Information security department undergraduate. Number of printed paper: 2**.** Research interests: information security management, information protection**.** E-mail: aamurzakova@edu.hse.ru

Murzakova E. A. National Research University "Highest School of Economics" (HSE), Moscow, Russia. Information security department undergraduate. Number of printed paper: 2**.** Research interests: information security management, information protection**.** E-mail: eamurzakova@edu.hse.ru