УДК 004.056

Головкова Елена Александровна,
к.т.н., доцент, Ангарский государственный технический университет,
e-mail: temnikova_ea@bk.ru
Аксёнова Полина Александровна,
обучающаяся группы ИВТ-21-1, Ангарский государственный технический университет
Соловьева Софья Сергеевна,
обучающаяся группы ИТБ-21-1, Ангарский государственный технический университет

ВЫБОР ИНСТРУМЕНТАРИЯ ДЛЯ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Golovkova E.A., Aksenova P.A., Solovieva S.S.

THE CHOICE OF TOOLS FOR ASSESSING INFORMATION SECURITY RISKS

Аннотация. Сформулированы основные требования к системам управления рисками информационной безопасности, осуществлен сравнительный анализ систем, в результате которого выявлены их основные достоинства и недостатки.

Ключевые слова: информационная безопасность, управление рисками, программные продукты.

Abstract. The basic requirements for information security risk management systems are formulated, a comparative analysis of the systems is carried out, as a result of which their main advantages and disadvantages are revealed.

Keywords: information security, risk management, software products.

Существует большое разнообразие коммерческих программных продуктов для оценки рисков информационной безопасности (ИБ). Однако, возникает ряд вопросов: какой из них выбрать; существуют ли отечественные аналоги; стоит ли разрабатывать свой программный продукт.

Опираясь на требования стандартов ГОСТ Р ИСО/МЭК 27001, BS 7799-3 и другие, связанные напрямую или косвенно с управлением в области ИБ, можно сформулировать ряд требований, которым должен соответствовать программный продукт для оценки рисков: охватывать все составляющие риска и их отношения; иметь в составе модули сбора, анализа и вывода данных; использовать алгоритмы, основанные на общепринятых подходах и методах к оценке рисков; формировать структурированные, полные и понятные отчеты; хранить историю сбора и анализа данных; обеспечивать доступ к актуальной документации по управлению рисками ИБ; быть совместимым с широким кругом современного программного и аппаратного обеспечения; иметь возможность сопровождения после внедрения, а также обучения пользователей.

Выделим достоинства и недостатки наиболее популярных программ: Cramm, RiskWatch, Кондор+.

1. RiskWatch. Достоинства: методология анализа рисков; сочетание качественной и количественной оценок рисков; обширная база данных по уязвимостям, угрозам, контрмерам; возможностью введения новых категорий; наличие русскоязычного интерфейса. Недостатки: анализ рисков только на программно-

техническом уровне защиты; не учитывает комплексный подход к ИБ; только на английском языке; дорогая лицензия.

2. CRAMM. Достоинства: идентификация элементов риска (нематериальных и материальных активов, их ценность, угрозы, величина потенциального ущерба, мер безопасности и вероятность реализации угрозы); обширная БД для оценки рисков и выбора контрмер; умелое использование метода позволяет экономить средства, избегая неоправданных расходов. Недостатки: использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора; только на английском языке; дорогая лицензия.

3. КОНДОР+. Достоинства: существует возможность отслеживать исполнение рекомендаций, связанных с политикой безопасности; наличие русскоязычного интерфейса; приемлемая стоимость лицензии. Недостатки: отсутствие возможности установки пользователем критерия значимости требования ИБ; отсутствие возможности внесения комментариев пользователя; какие-либо рекомендации или выводы частично отсутствуют, что снижает эффективность принятия управленческих решений.

Заключение. В результате проведенного сравнительного анализа наиболее популярных программных продуктов управления рисками ИБ выявлены общие недостатки (ограничения): частичное соответствие международным и государственным стандартам, например, очень мало продуктов разработано специально для ISO 27001; неполный охват активов, так как большинство функций программ направлены на работу с информационно-техническими активами; сложность в изучении и использовании; сокрытие от пользователя алгоритмов, автоматизированного расчета рисков, что приводит к сложностям в процессе осознания и оценке степени рисков; проблемы с русификацией, свойственные большинству импортных программных продуктов.

Обнаружить продукт, лишенный недостатков, достаточно сложно. Не говоря уже о том, что многие продукты, позиционируемые разработчиками как средства для оценки или управления рисками, на самом деле таковыми не являются, так как не реализуют ни методологии оценки рисков, ни алгоритма их вычисления, а предоставляют лишь средства представления и хранения данных о рисках, возлагая анализ и оценивание рисков на пользователей.

ЛИТЕРАТУРА

1. **Темникова, Е. А.** Сравнительный анализ программных систем управления рисками информационной безопасности / Е. А. Темникова, Е. А. Павлова – Текст : непосредственный // Транспортная система Сибирского региона. – 2017. – С. 412-417.