Дамир Фаритович Файзулаев, Борис Борисович Морозов
Астраханский государственный университет,
ул. Татищева, 20а, г. Астрахань, 414056, Россия
e-mail:rapzone@inbox.ru, ORCID 0000-0001-5121-1842;
e-mail:boris.coldman@gmail.com, ORCID 000-0002-4628-3355

МЕТОДЫ И СРЕДСТВА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

DOI: http://dx.doi.org/10.26583/bit.2017.3.09

Аннотация. Рассмотрены методы и средства оценки рисков информационной безопасности. Показаны основные проблемы, возникающие в процессе выполнения анализа защищенности предприятия в сфере ИБ. Приведен краткий обзор существующих инструментальных решений проблем оценки рисков ИБ организаций, занятых в различных сферах деятельности. Проанализированы основные достоинства и недостатки методов оценки рисков и программных средств, базирующихся на данных методиках. Представлены результаты обзора, сделаны выводы касательно недостатков методов и средств, а также рассмотрен вопрос оптимального соотношения таких понятий, как широта применимости методов и программных средств и надежность, точность и адекватность оценки рисков информационной безопасности. Предложены новые дополнительные этапы анализа рисков, которые позволять усовершенствовать уже имеющиеся методы и устранить выявленные в ходе обзора недостатки.

Ключевые слова: CORAS, CRAMM, Microsoft Security Assessment Tool (MSAT), OCTAVE, RiskWatch, ГРИФ, анализ защищенности информации, анализ и оценка рисков ИБ, информационная безопасность, методы и средства оценки рисков ИБ.

Для цитирования. **ФАЙЗУЛАЕВ, Дамир Фаритович; МОРОЗОВ, Борис Борисович.** МЕТОДЫ И СРЕДСТВА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ. Безопасность информационных технологий, [S.l.], v. 24, n. 3, p. 72-77, july 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/267>. Дата доступа: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.09.

Damir Faritovich Fayzulayev, Boris Borisovich Morozov
Astrakhan State University,
20a Tatischev Street, Astrakhan 414056 Russia
e-mail:rapzone@inbox.ru, ORCID 0000-0001-5121-1842;
e-mail:boris.coldman@gmail.com, ORCID 0000-0002-4628-3355

Methods and means of analysis of risks of the information security of the enterprise

DOI: http://dx.doi.org/10.26583/bit.2017.3.09

Abstract. Methods and means of assessing information security risks are considered. The main problems that arise in the process of performing the analysis of the security of an enterprise in the field of information security are shown. A brief review of the existing instrumental solutions to the problems of assessing the risks of information security organizations engaged in various fields of activity is given. The main advantages and disadvantages of methods for risk assessment and software based on these techniques are analyzed. The results of the review are presented, conclusions are made regarding the shortcomings of methods and tools, and the question of the optimal correlation of such concepts as the breadth of applicability of methods and software tools and reliability, accuracy and adequacy of information security risk assessment are considered. We propose new additional stages of risk analysis that allow improving existing methods and eliminating the shortcomings identified during the review.

Keywords: CORAS, CRAMM, Microsoft Security Assessment Tool (MSAT), OCTAVE, RiskWatch, GRIF, information security analysis, analysis and assessment of IS risks, information security, methods and means of IS risk assessment.
For citation. **FAYZULAYEV, Damir Faritovich; MOROZOV, Boris Borisovich.** Methods and means of analysis of risks of the information security of the enterprise. IT Security, [S.l.], v. 24, n. 3, p. 72-77, july 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/267>. Date accessed: 01 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.3.09.

Введение

Информационная безопасность (ИБ) предприятия – это состояние защищенности информации от НСД, разрушения, модификации, раскрытия и задержек при поступлении [1].

Для создания надежной системы защиты информации (СЗИ) необходимо выработать политику ИБ, провести анализ рисков, составить план мер по обеспечению ИБ и план мероприятий в чрезвычайных ситуациях, выбрать программные, технические и программно-технические средства обеспечения ИБ.

Поскольку на основе данных полученных в ходе анализа защищенности предприятия строится вся система защиты информации, этап анализа рисков является одним из основных, а также одним из сложных этапов построения СЗИ. Сложность данного процесса заключается в том, что для определения оценки рисков защищенности предприятия необходимо проанализировать большой объем входных данных различного формата: текст, числовые значения, схемы, диаграммы и т.п. В ходе этого возникает сложность в их обработке: значительные затраты времени и человеческих ресурсов. Решением этой проблемы является автоматизация данного процесс, с целью ускорить и облегчить задачу анализа защищенности предприятия для специалистов в области информационной безопасности.

Краткий обзор существующих инструментальных решений проблем анализа рисков

На сегодняшний день многими иностранными компаниями, которые специализируются в решении комплексных проблем ИБ, разработаны и предложены собственные методики управления информационными рисками. Эти методики различаются, прежде всего, по уровню и совершенству используемых математических методов, положенных в основу процедур оценивания рисков. В зависимости от этого они обладают разными возможностями адекватного учета реальных факторов, что в свою очередь, предопределяет точность и надежность полученных оценок риска.

Программные средства и методики анализа рисков

CORAS. Метод CORAS – это компьютеризированный инструмент, позволяющий документировать, создавать отчеты о результатах анализа путем моделирования риска.

Достоинства и недостатки метода CORAS. В методе CORAS не предусмотрена периодичность проведения оценки рисков и обновление их величин. CORAS не позволяет оценить эффективность инвестиций, вложенных во внедрение мер безопасности. Так же как не дает возможности найти необходимый баланс между мерами, направленными на предотвращение, выявление, исправление или восстановление информационных активов. Положительной стороной метода CORAS является то, что программный продукт,

реализующий эту методологию, распространяется бесплатно и не требует значительных ресурсов для установки и применения [3].

CRAMM. Метод CRAMM (CCTA Risk Analysis and Management Method) был разработан компанией Insight Consulting по требованиям Центрального Агентства по Компьютерам и Коммуникациям Великобритании.

Достоинства и недостатки метода CRAMM. Метод использует комплексный подход к оценке рисков, применяет технологии оценки угроз и уязвимостей по косвенным факторам с возможностью верификации результатов, имеет обширную базу знаний по контрмерам и обладает универсальностью и адаптируемостью под профили разных организаций. Однако использование метода CRAMM требует специальной подготовки и высокой квалификации аудитора. Аудит по данному методу – процесс достаточно трудоемкий и может потребовать месяцев непрерывной работы аудитора. Он не позволяет создавать собственные шаблоны отчетов или модифицировать имеющиеся. Программное обеспечение существует только на английском языке [4].

RiskWatch. Программное обеспечение RiskWatch, разрабатываемое американской компанией RiskWatch, Inc., является мощным средством анализа и управления рисками.

Достоинства и недостатки метода RiskWatch. В методе RiskWatch в качестве критериев для оценки и управления рисками используются «предсказание годовых потерь» и оценка «возврата от инвестиций».Он подходит, если требуется провести анализ рисков на программно-техническом уровне защиты, без учета организационных и административных факторов. Полученные оценки рисков (математическое ожидание потерь) далеко не исчерпывает понимание риска со системных позиций – метод не учитывает комплексный подход к информационной безопасности [4].

ГРИФ. ГРИФ - комплексная система анализа и управления рисками информационной системы компании, разработанная российской компанией «Digital Security»[5].

Достоинства и недостатки метода ГРИФ. Метод не требует специальных знаний в области ИБ, предоставляя подробный, дающий полную картину возможного ущерба от инцидентов документ, готовый для представления руководству компании, формирует полную модель информационной системы с точки зрения ИБ с учетом реального выполнения требований комплексной политики безопасности. Однако в методе отсутствует привязка к бизнесс-процессам, возможность сравнения отчетов на разных этапах внедрения комплекса мер по обеспечению защищенности и добавления специфичные для данной компании требования политики безопасности [5].

OCTAVE. Метод OCTAVE — это метод оперативной оценки критических угроз, активов и уязвимостей.

Достоинства и недостатки метода OCTAVE. Метод предусматривает регулярное проведение оценки рисков и обновление их величин, как части процесса оценки рисков. В нем не используется такой способ управления рисками, как обход (исключение). Метод OCTAVE не дает количественной оценки рисков, однако качественная оценка может быть использована в определении количественной шкалы их ранжирования [3].

Microsoft Security Assessment Tool (MSAT). Данное средство безопасности разработано для помощи в определении и устранении угроз безопасности в вычислительной среде и базируется на методике Microsoft.

Достоинства и недостатки метода Microsoft. MSAT оценка предназначена для широкого охвата областей потенциального риска в среде, а не для предоставления глубокого анализа конкретных технологий или процессов. Как следствие, средство не может оценивать эффективность примененных мер безопасности [6].

Обобщение результатов обзора

Проанализировав средства и методики, можно сделать вывод о том, что представленные методы не предполагают расчета рационального соотношения различных способов контроля, не производят оценки качества процесса реагирования на инциденты в области ИБ, не предусматривают составление плана проведения повторных оценок рисков и обновления их значений, не рассматривают вопросы постоянного или периодического аудита рисков ИБ.

Прежде чем проводить анализ рисков, необходимо определить цель, которую нужно достичь, и в зависимости от её значимости, выбрать метод оценки рисков. Важно понимать, что универсальные методики, которые применимы для анализа рисков в различных организациях, дают менее точную и адекватную оценку рисков ИБ предприятия, чем узкоспециализированные, которые в свою очередь применимы только для определенных видов деятельности и разрабатываются непосредственно самой организацией. Поэтому, разрабатывая собственную, усовершенствуя или дополняя существующую методику, нужно учитывать, какое оптимальное соотношение широты применения методики и точности оценки рисков ИБ на предприятиях необходимо достичь.

Поскольку на данный момент существующие методики получили широкое применение в различных сферах деятельности, то вопрос о точности и адекватности оценки рисков на основе их алгоритмов встает очень остро. Каждому предприятию, каждой организации или компании необходимо иметь возможность управлять рисками ИБ, чтобы вести успешную и выгодную деятельность, то есть получать точную оценку рисков ИБ, благодаря глубокому и подробному анализу защищенности информации. Это возможно благодаря разработке собственной методики, адаптированной под конкретный вид деятельности, но данный процесс затрачивает большой объем времени и человеческих ресурсов. Поэтому, учитывая результаты анализа приведенных методик, возникает необходимость усовершенствовать и доработать их.

Дополнение и усовершенствование методов

Предприятию необходимо использовать не только методику, которая предоставляет результаты первичной оценки рисков и рекомендации по их снижению, но и простое и понятное в использовании программное средство проведения этой оценки. Ведь в организации не всегда имеются квалифицированные специалисты в сфере ИБ или отделы ИБ.

Учитывая вышесказанное и недостатки рассмотренных методов, необходимо выполнять постоянный или периодический аудита ИБ (мониторинг), проводить регулярное обновление баз знаний и значений оценки рисков, проверять компетенции персонала и тестировать его, планировать проведение повторных оценок рисков ИБ, разработать меры по обеспечению безопасности самих систем оценки рисков ИБ.

Для того чтобы оценить эффективность работы методики, необходимо знать насколько объект информатизации был подвержен различным угрозам до её использования и после применения мер по их устранению, разработанных на основе данной методики. Постоянный или периодический аудит ИБ позволяет выявить угрозы и документально подтвердить случаи их возникновения. Для проведения мониторинга, нужно фиксировать и записывать в журнал событий любые манипуляции пользователя с ИС. Это в последующем поможет быстрее выявить угрозы и их инициатора.

Регулярное обновление баз знаний позволит получить более точную и адекватную оценку рисков ИБ. После обнаружения новой угрозы и применения разработанных мер по её ликвидации, база знаний должна обновляться. В базу записываются сведения об угрозе, мерах её устранения и результат применения таких мер.

Основным источником угроз является человек. Человеческий фактор играет огромную роль при работе с конфиденциальной информацией, различными информационными системами, поэтому от компетентности сотрудников в вопросах информационной безопасности зависит уровень защищенности информации предприятия. Этап проверки компетенций и проведения тестов, является одним из основополагающих этапов методики. Персонал организаций необходимо регулярно проверять на знания вопросов информационной безопасности предприятия, на котором они работают, моделировать для них различные ситуации, проводить экзаменационные тесты, с целью выявить потенциально опасных сотрудников, создающих угрозу информационной безопасности.

Проведение повторной оценки рисков ИБ позволяет выявить уязвимости и угрозы, которые не удалось устранить применением разработанных методикой мер. Исходя из этого, создаются новые меры или дорабатываются старые.

В меры по обеспечению безопасности программных средств оценки рисков ИБ необходимо включить ограничение прав доступа к системным фалам и файлам баз данных, ведение журнала аудита, установка режима работы пользователя с системой, централизованное хранение данных, физическое размещение системы на выделенном сервере, регулярное осуществление резервного копирования, на отдельный жесткий диск.

Заключение

Предложенные варианты дополнения рассмотренных методов позволят достичь оптимального баланса между такими аспектами анализа рисков, как универсальность, то есть широта применимости метода для различных профилей организаций, точность, надежность и адекватность оценки рисков ИБ. Также данные этапы обеспечат простоту использования программных инструментов, в будущем разработанных на основе данной усовершенствованной методики, прозрачность выполняемых процедур и ясность полученных результатов. Соответственно будут выполнены требования предприятия, предъявляемые к инструментам и методам оценки рисков ИБ.

СПИСОК ЛИТЕРАТУРЫ

1 Садердинов, А.А. Информационная безопасность предприятия: учеб. Пособие А.А. Садердинов, В.А. Трайнев, А.А. Федулов. – М.: Дашков и К , 2005. – 336 с.
2 Bjorn A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems — Model-based Risk Analysis Targeting Security, 2002.
3 Красникова, Т.В., Невежин, В.П. Моделирование оценки при аудите безопасности информационных систем. Т.В. Красникова, В.П. Невежин VII Международная студенческая электронная научная конференция "Студенческий научный форум 2015".
4 Медведовский, И. Современные методы и средства анализа и контроля рисков информационных систем компаний. И. Медведовский, www.dsec.ru, Digital Security.
5 Куканова, Н. Современные методы и средства анализа и управление рисками информационных систем компаний. Н. Куканова, www.dsec.ru, Digital Security.
6 Средство оценки безопасности Microsoft Security Assessment Tool – URL: https://technet.microsoft.com/ru-ru/security/cc185712.aspx

REFERENCES:

[1] Saderdinov AA, Trinev VA, Fedulov AA Informational security of the enterprise: Textbook.-2-e izd.- M., Publishing-trading corporation "Dashkov and K °", 2005 .- 336 p. (in Russian).

[2] Bjorn A.G. CORAS, A Platform for Risk Analysis on Security Critical Systems - Model-based Risk Analysis Analysis Targeting Security, 2002.
[3] Krasnikova, TV, Nevezhin, V.P. Modeling the assessment in the audit of information systems security / T.B. Krasnikov, V.P. Nevezhin VII International Student Electronic Scientific Conference "Student Scientific Forum 2015". (in Russian).
[4] Medvedovsky, I. Modern methods and means of analysis and control of risks of information systems companies. I. Medvedovsky, www.dsec.ru, Digital Security. (in Russian).
[5] Kukanova, N. Modern methods and means of analysis and risk management of information systems companies. N. Kukanova, www.dsec.ru, Digital Security. (in Russian).
[6] Microsoft Security Assessment Tool - URL: https://technet.microsoft.com/en-us/security/cc185712.aspx (in Russian).