УДК 004.056

Иерархический метод оценки активов для анализа рисков информационной безопасности

Шергазиева Майрам Сабырбековна
Иссык-Кульский государственный университет им. К.Тыныстанова
Преподаватель
Приамурский государственный университет им. Шолом-Алейхема
Магистрант

Аннотация
В этой статье предлагается метод оценки активов на основе иерархии. Метод предназначен для минимизации распространенных ошибок, которые были допущены в ходе проектов по управлению информационной безопасностью. Применение метода еще не было выполнено, однако считается, что он может облегчить процессы и уменьшить количество ошибок.
Ключевые слова: Анализ рисков информационной безопасности, оценка активов.

A hierarchical asset valuation method for information security risk analysis

Shergazieva Mayram Sabyrbekovna
Issyk-Kul State University named after K. Tynystanova
Lecturer
Sholom-Aleichem Priamursky State University
Master's student

Abstract
In this paper, a hierarchy-based asset valuation method is proposed. Our method is intended to minimize the common mistakes that were done during Information Security Management Projects. The application of the method has not been performed yet; however, it is thought that it can ease the processes and reduce the number of errors.
Keywords- Information security risk analysis, asset valuation

Научный руководитель:
Баженов Руслан Иванович
Приамурский государственный университет имени Шолом-Алейхема
к.п.н., доцент, зав. кафедрой информационных систем, математики и правовой информатики

Информационные технологии сегодня стали неотъемлемой частью ведения бизнеса. Информационные технологии эволюционировали от автономных пакетных приложений до современных взаимосвязанных

мобильных систем. Эта эволюция привела к широкому использованию информационных технологий всеми видами бизнеса. Более двадцати лет назад, в каждой организации, большинство бизнес-процессов были задокументированы на бумаге. В настоящее время, практически каждый бизнес-процесс зависит от информационных технологий. Поэтому, хотя информационные системы начинались как инструменты повышения операционной эффективности, позже они приобрели незаменимую роль для существования организации [1, 2].

Идентификация и оценка активов - важнейший процесс, который необходимо выполнять при анализе рисков. Без правильно идентифицированных и оцененных активов результаты анализа рисков приводят к неправильным решениям. Неправильные решения в области информационной безопасности могут напрямую повлиять на соответствующие бизнес-процессы. В литературе есть некоторые готовые и применяемые методы идентификации и оценки активов; однако эти методы сложны и не подходят для практических проектов по управлению информационной безопасностью.

Широкое использование информационных технологий непрерывно и быстро трансформирует бизнес. Информационные технологии также представляют новые угрозы для организаций. Анализ рисков является важным инструментом для принятия правильных решений и борьбы с киберугрозами.

Параллельно с общим использованием информационных систем в организациях, угрозы и атаки на информационные системы также быстро увеличивались. Быстрое изменение вычислительной среды предоставляет множество возможностей для злоумышленников.

Например, а) широкое использование распределенных систем связи, дает злоумышленникам возможность скрыться после удаленного взлома системы [3]. б) Мобильное оборудование привлекает внимание хакеров из-за его широкого использования. Мобильные системы также уязвимы для атак [4].

Количество инцидентов и угроз безопасности растет день ото дня [4]. Поскольку большая часть бизнес-операций зависит от информационных технологий, угроза информационным технологиям означает угрозу самому бизнесу. Помимо финансового воздействия, инциденты с безопасностью могут оказывать влияние на нематериальные активы, такие как:

- Имидж бренда, общественная репутация и деловая репутация на рынке;
- Финансовая стоимость деловых операций;
- Доверие общественности и клиентов к точности деловых операций;
- Доверие общественности и клиентов к устойчивости деловых операций к мошенничеству;
- Способность своевременно поддерживать денежный поток выручки;
- Способность разрешать споры вне разумных сомнений;

- Способность соответствовать требованиям регулирующих органов [6].

Инцидентов информационной безопасности могут быть потеря доверия и денежный ущерб [5]. Поскольку информационные технологии важнее, чем когда-либо, и организации в значительной степени полагаются на информационные системы, ответственность за защиту этих систем лежит на руководстве высшего уровня, а не на руководителе отдела обработки информации [7]. Информационная безопасность стала одним из главных приоритетов высшего руководства [5]. В стандарте ISO/IEC 27001:2005 руководство демонстрирует свою приверженность информационной безопасности организации, определяя критерии принятия рисков и приемлемый уровень риска [8].

Информационная безопасность направлена на обеспечение контроля в целях снижения рисков, влияющих на информацию организаций. Критически важно, что существует опасность тратить деньги на риски, которые могут быть не очень опасными, игнорируя при этом другие серьезные угрозы [9]. Методы управления рисками оказывают организациям помощь в выявлении угроз и выборе экономически эффективных мер безопасности для минимизации общей ожидаемой стоимости потерь [3, 10].

Метод анализа иерархий (МАИ) состоит в декомпозиции проблемы на более простые составные части и дальнейшей обработке последовательности суждений эксперта по парным сравнениям. Метод анализа иерархий служит для обоснования принятия решений в условиях определенности и многокритериальности.

Простейшая полная иерархия проблемы многокритериального выбора включает в себя три уровня (рис.1): актив, уязвимость, угроза. Хотя в литературе они имеют разные значения, анализ рисков, оценка рисков и иногда управление рисками используются взаимозаменяемо. Риск определяется как вероятностная функция угрозы, успешно атакующей актив через определенную уязвимость [3], [10-13].

Функция риска, имеет три переменные: активы, уязвимость и угроза. Первый вход функции риска, актив, определяется как все, что имеет ценность для организации в стандарте ISO/IEC 27001:2005. Определение стоимости актива является важнейшей частью анализа рисков.

$$\text{Риск} = f(\text{актив, уязвимость, угроза}) \quad (1)$$

Рис.1- Иеарархия проблемы

Уязвимость - это дефект в активе, который может быть использован угрозой для атаки на информационную систему. Компании, производящие программное и аппаратное обеспечение, пытаются адаптировать быстрые темпы изменений в информационных технологиях для поддержания своей конкурентоспособности, однако быстрое изменение технологий может привести к пренебрежению требованиями безопасности, которые замедляют производственный процесс. Каждый день внедряются новые технологии, и злоумышленники через некоторое время находят уязвимость, чтобы воспользоваться ею. Для успешного анализа рисков аналитик по безопасности должен получать и обмениваться информацией о новых технологиях, продуктах, угрозах или уязвимостях и поддерживать себя в курсе событий. Угрозы информационным системам могут повлиять на конфиденциальность, целостность или доступность активов. Угрозы могут действовать несколькими способами, такими как уничтожение (актив не подлежит восстановлению), модификация (изменение представления актива), раскрытие (нарушение необходимости знать) и отказ в обслуживании (ресурсы недоступны авторизованным пользователям) [3].

Общие угрозы информационной безопасности перечислены ниже [14]:

1. Акт человеческой ошибки или неудачи (несчастные случаи, ошибки сотрудников);
2. Посягательства на интеллектуальную собственность (пиратство, нарушение авторских прав);
3. Преднамеренные акты шпионажа или вторжения (несанкционированный доступ или сбор данных);
4. Преднамеренные акты вымогательства информации (шантаж раскрытия информации);
5. Преднамеренные акты саботажа или вандализма (уничтожение систем или информации);
6. Преднамеренные акты кражи (незаконная конфискация оборудования или информации);
7. Преднамеренные программные атаки (вирусы, черви, макросы, отказ в обслуживании);
8. Силы природы (пожар, наводнение, землетрясение, молния);
9. Отклонения в качестве обслуживания от Поставщиков услуг (проблемы с питанием и обслуживанием глобальной сети);
10. Технические сбои или ошибки оборудования (отказ оборудования);
11. Технические сбои или ошибки программного обеспечения (ошибки, проблемы с кодом, неизвестные лазейки);
12. Технологическое устаревание (устаревшие или устаревшие технологии).

Методы анализа рисков делятся на два основные группы как качественные, так и количественные методы. Методы количественного анализа рисков используют математические инструменты (например, байесовские сети, нечеткую логику) для оценки риска [12]. Количественные методы пытаются рассчитать ожидаемый годовой убыток в денежном

выражении для каждой угрозы и определить стоимость возможного ущерба [1], [3].

Важная специфическая особенность качественного анализа рисков состоит в его количественном результате. Это значит, что процесс проведения качественного анализа рисков должен включать не только чисто описательный аспект определения тех или иных конкретных видов рисков данного проекта, выявление возможных причин их возникновения, анализ предполагаемых последствий их реализации и предложения по минимизации выявленных рисков, но и стоимостную оценку всех мероприятий, минимизирующих риск конкретной компании (таб. 1).

Таблица 1- Качественный анализ рисков

Актив	**Угроза**	**Уязвимость**	**Риск**
Цифровой документ	Поломка жесткого диска	Нет резервной копии документа	Потеря доступности и целостности информации
	Вредоносный код	Антивирусная программа не обновляется должным образом	Потеря конфиденциальности, целостности и доступности
	Несанкционированный доступ	Схема контроля доступа не определена должным образом	Потеря конфиденциальности, целостности и доступности
		Доступ был предоставлен слишком многим людям	

Методология анализа рисков Livemore (LRAM), метод анализа рисков информационной безопасности (ISRAM) и ALE с использованием метода анализа оценки программ (PERT) являются примерами методов количественного анализа рисков [1], [7]. Количественные методы требуют солидной математической базы для оценки рисков информационной безопасности, и реализация этих методов требует больше времени и усилий, чем качественные методы [3], [12]. Методы качественного анализа рисков утверждают, что использование денежных значений для выражения возможных последствий угрозы не является хорошим методом [1]. Как правило, эти методы основаны на суждениях и представлениях эксперта по безопасности, который проводит анализ рисков, и используют несколько методов, таких как анкетирование, анализ сценариев и нечеткие показатели для оценки пригодности мер защиты от выявленных угроз [1], [3]. Ни один из этих методов не доказал своего превосходства над другим. Организация может выбрать любой из этих методов, который ей подходит, например, для

анализа рисков общественных организаций предлагаются качественные методы [12].

Недостатки, несоответствие стоимости денежных активов - грубая детализация. Несоответствие общей статистики, невозможность принятия решения о затратах и выгодах, отнимает много времени, требует большой предварительной работы. Субъективные результаты зависят от качества команды управления рисками. Какая бы методология ни использовалась при анализе рисков, существуют желаемые свойства метода анализа рисков. Основные свойства метода анализа рисков перечислены ниже [10]:

• Общее согласие всех связанных сторон (например, руководства, пользователей, ИТ-отдела);
• Обработка новых технологий, угроз и уязвимостей;
• Логически обоснованный;
• Воспроизводимый;
• Обеспечение оптимальной защиты по стоимости;
• Быть открытым для постоянной оценки со всех сторон;
• Сопровождаться четкой документацией;
• Быть циклическим, периодически повторяющимся.

Мы рассматривали два входных параметра функции анализа рисков, а именно уязвимость и угрозу. Третий ввод, актив, подробно описан в следующем разделе документа.

Идентификация и оценка активов являются важнейшим шагом для обеспечения объективного, воспроизводимого и логически обоснованного процесса анализа рисков. Процесс идентификации и оценки активов также влияет на полноту и эффективность возможного процесса анализа рисков. Поэтому идентификация и оценка активов не является простой задачей. Идентификация и оценка информационных активов усложняется, когда актив является нематериальным, таким как репутация организации. Существует не так много исследований по методам оценки активов для процессов анализа рисков, информационной безопасности. Оскарсон и Карлссон предлагают национальную модель классификации информации. Их модель основана на двух аспектах: аспекте безопасности информационной системы и уровнях/типах серьезности. В аспекте безопасности информационных систем существуют два документа для определения конфиденциальности, целостности и доступности. Эти документы относятся к серии ISO 27000 (ISO/IEC 27001:2005 и ISO/IEC 27002:2005), Справочнику SIS 550 "Терминология для информационной безопасности".

Прежде всего, иерархический метод имеет некоторые недостатки. Он имеет дело только с цифровыми активами. Например, он не распространяется на печатные книги. Активы, которые не являются оборудованием, программным обеспечением или цифровой информацией, следует рассматривать отдельно. Иерархический метод может эффективно использоваться в процессах анализа рисков, где в основном используются информационные технологии. Аналитики рисков должны быть осторожны при работе с оборудованием, таким как жесткие диски. На жестких дисках

нет явного программного обеспечения (например, операционных систем, прикладных программ). Они запускают специальное программное обеспечение, называемое прошивкой; но прошивка обычно не рассматривается как самостоятельный ресурс. Это рассматривается с аппаратным обеспечением в целом. Поэтому аналитики рисков должны пропустить средний уровень пирамиды оценки активов и должны непосредственно идентифицировать информационные активы на жестких дисках.

Важный вопрос заключается в следующем: "Какие ценности среди конфиденциальности, целостность и доступность должны приниматься во внимание в процессе анализа рисков?" Является ли использование среднего арифметического хорошей идеей? Для предлагаемого метода ответ связан с типом связанного с этим риска. Если риск связан с доступностью информации, следует учитывать значение доступности. Например, наводнение может повлиять на доступность сервера, но не влияет на конфиденциальность и целостность. Таким образом, при оценке риска следует использовать значение доступности соответствующего оборудования, но не значения конфиденциальности и целостности. Предлагаемый метод может облегчить процессы оценки активов и анализа рисков. Этот практический подход может помочь организациям, которые пытаются улучшить свои процедуры информационной безопасности.

Библиографический список

1. Хан И. Анализ рисков на основе бизнес-модель // Информация и управление. 2003. Т. 41. № 2. С.149-158.
2. Доэрти, Н.Ф., Анастасакис Л., Фулфорд Х. Информационная безопасность Политика распакована: Критическое исследование содержания университетской политики // Международный журнал по управлению информацией. 2009. Т. 29. № 6. С. 449-457.
3. Уилсон Дж. Л., Тюрбан Е., Звиран М. Безопасность информационных систем: Управленческая перспектива // Международный журнал управления информацией. 1992. Т. 12. № 2. С. 105-119.
4. Фосси М., Иган Г., Хейли К., Джонсон Э., Мак Т., Адамс Т., Дрозд И.И., Лоу М. К., Мазурек Д., Маккинни Д., Вуд П. Тенденции в отчете Symantec об угрозах интернет-безопасности за 2010 год. 2011. Компания Symantec.
5. Булгурчу Б., Чавушоглу Х., Бенбасат И.: Политика информационной безопасности Соответствие // Эмпирическое исследование убеждений, основанных на рациональности и осведомленность об информационной безопасности. 2010. Т. 34. № 3. С. 523-548.
6. Фараманд Ф., Навате С.Б., Шарп Г.П., Энслоу П.Х. Управленческий взгляд на риск угроз, системы информационной безопасности. Информационные технологии и управление. 2005. Т. 6. № 2-3. С. 203-225.
7. Карабаджак Б., Согукпинар И. ISRAM: Метод анализа рисков информационной безопасности // Компьютеры и безопасность. 2005. Т. 24.

№ 2. С.147-159.
8. Международная организация по стандартизации. Международная электротехническая комиссия (ISO/IEC): ISO/IEC 27001:2005, Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. 2005. Издание 1.
9. Солмс, Б., Солмс, Р. 10 смертных грехов информации Управление безопасностью. Компьютеры и безопасность. 2004. Т. 23. № 5. С. 371-376.
10. Райнер-младший Р.К., Снайдер К.А., Карр, Х.Х.: Анализ рисков для информации технологий // Журнал информационных систем управления. 1991.Т. 8. № 1. С. 129-147.
11. Треок Д., Тробек Р., Павесик Н., Тасич Дж.Ф. Безопасность информационных систем и поведение человека // Поведение и информационные технологии. 2007.Т. 26. № 2. С. 113- 118.
12. Озкан. С., Карабасак. В. Метод совместного риска для практики управления информационной безопасностью: Контекст дела в Турции // Международный журнал по управлению информацией. 2010. Т. 30. № 6. С.567-572.
13. Чен-п., Катария Г., Кришнан Р. Коррелированные сбои. Диверсификация и Управление рисками информационной безопасности. Неверный расчет. 2011. Т. 35. № 2. С. 397-422.
14. Уитмен М.Э. В защиту Королевства: Понимание угроз для информационной безопасности // Международный журнал по управлению информацией.2004. Т. 24. № 1. С.43-57.
15. Оскарсон П., Карлссон Ф. Национальная информационная модель Классификации. Объединение информационных систем // SIGSEC Семинар по информационной безопасности и конфиденциальности. 2009. Финикс, Аризона, США.