УДК 004.67 **DOI: 10.18413/2518-1092-2019-4-1-0-5**

Маслова М.А.

АНАЛИЗ И ОПРЕДЕЛЕНИЕ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Севастопольский государственный университет: ул. Университетская д. 33 г. Севастополь, 299053, Россия

e-mail: info@sevsu.ru

Аннотация
Любая информация требует эффективной системы защиты и является обеспечением устойчивого развития и функционирования объекта. Затраты необходимые для защиты информации не всегда оправданы. Поэтому важным условием обеспечения информационной безопасности является задача нахождения соответствующего уровня защиты при допустимых затратах. Значение выявления рисков в различных областях имеет ключевое значение для развития и стабильности предприятий, что дает возможность понять и оценить возможные опасные события, выявить их причины и последствия, вероятности возникновения и принятия решений, что является одной из сложных задач. Для этого необходимо провести анализ рисков информационной безопасности, с помощью которого можно будет оценить существующий уровень защищенности ресурсов любой организации. Существуют различные подходы, методы и средства оценки рисков информационной безопасности, приводящие к конечному результату, как с плюсами, так и с недостатками управления. Проведем оценку и анализ этих методов и выделим более приемлемые, эффективные и менее затратные.
Ключевые слова: информационные риски; информационная безопасность; угроза; ущерб; уязвимость; качественный метод; количественный метод; оценка уровня риска.

UDC 004.67

Maslova M.A.

ANALYSIS AND DEFINITION OF INFORMATION SECURITY RISKS

Sevastopol state University, 33 Universitetskaya St, Sevastopol, 299053, Russia

e-mail: info@sevsu.ru

Abstract
Any information requires an effective system of protection and is to ensure the sustainable development and functioning of the object. The costs necessary to protect the information are not always justified. Therefore, an important condition for information security is the task of finding the appropriate level of protection at an acceptable cost. The importance of identifying risks in different areas is crucial for the development and stability of enterprises, which makes it possible to understand and assess possible dangerous events, to identify their causes and consequences, the probability of occurrence and decision-making, which is one of the challenges. To do this, it is necessary to conduct an analysis of information security risks, with which it will be possible to assess the existing level of security of resources of any organization. There are various approaches, methods and tools for assessing information security risks, leading to the end result, both with advantages and disadvantages of management. We will evaluate and analyze these methods and identify more acceptable, effective and less costly.
Keywords: information risks; information security; threat; damage; vulnerability; qualitative method; quantitative method; risk assessment.

ВВЕДЕНИЕ

Происхождение термина «риск» берет свое начало с французского языка слова risqué или итальянского risico и обозначает возможность или вероятность наступления данного события с определенными последствиями с конечными конкретными решениями или действиями, где рассматривается не только отрицательный тип эффекта, но и положительный. В СССР риск-менеджмент начал развиваться после второй мировой войны и только в направлении страхования, который считался дорогим и неполным инструментом защиты от воздействия риска. Свое начало по работе с рисками считается статья аспиранта Чикагского университета Гарри Марковица «Диверсификация вложений» («Portfolio Selection»), в которой была представлена математически обоснованная стратегия диверсификации инвестиционного портфеля, что помогало грамотно распределить вложения и минимизировать отклонения доходности от ожидаемого показателя. В 1990 году Г.Марковицу была присуждена Нобелевская премия за то, что он вложил фундаментальные основы в развитии и изучении понятия риска.

Изначально работа с рисками применялась только к финансовой сфере, а вот уже во второй половине двадцатого века появились все ныне общеизвестные и применяемые на данный момент методы определения рисков в различных областях науки. Хотя до сих пор многие предприятия изначально не разрабатывают собственную концепцию рисков при «зарождении» предприятия и только столкнувшись с трудностями, приходят к этому [4, 8].

ОСНОВНАЯ ЧАСТЬ

Так как суть любого явления, процесса или объекта является деятельность, которая ведет к формированию результатов и различаются как: косвенные, прямые, конструктивные, деструктивные, псевдослучайные, объективные и субъективные виды результатов и т.д. Тогда объективный результат есть следствие определенного выполнения процесса, который непосредственно связан с его сутью, а субъективный результат есть выполнение процесса с недостаточным уровнем определенности и полноты информации. Преобладающее количество существующих рисков встречающихся на практике связанно именно с субъективными результатами осуществления и выполнения процесса. Поэтому можно сказать, что практически все риски есть субъективный результат выполнения процесса, и они имеют недостаток как количественной, так и качественной информации об определенном рассматриваемом процессе.

На данном этапе развития области рисков в информационных технологиях существует множество типизации рисков. Информационные риски, которые возникают в рассматриваемых процессах и проектах, отличаются между собой, как по совокупности внутренних и внешних факторов, так и по времени и месту их возникновения. При этом они влияют на их уровень, на способ анализа и методы первичного и последующего описания. Т.к. все виды рисков взаимосвязаны, следовательно, они оказывают влияние на осуществляемую деятельность, как по отдельности, так и в совокупности между собой. Необходимо классифицировать множество рисков по критериям и признакам, с помощью которых их можно объединить в общие понятия, такие как: характер, время и факторы возникновения, последствия и т.д. [8]

В свою очередь риски по характеру подразделяются на внешние и внутренние; по времени возникновения на прошлые или ретроспективные и будущие или перспективные; по фактору возникновения такие, как проектные, операционные риски, процессные, организационные; по последствиям на чистые и спекулятивные.

Так же выделяется подклассификация рисков по степени последствий возникновения рисков и состоит из: допустимого риска, критического риска и катастрофического риска. Эта классификации является важной при принятии решений по осуществлению какой-либо деятельности, связанной с рисками.

Важным этапом является идентификация риска – это одна из стадий анализа рисков позволяющая выявить, оценить и понять предпосылки, которые ведут к появлению риска и

которую необходимо проводить перед осуществлением классификации рисков. От ее правильности проведения и будет зависеть результат выбранного метода для устранения ущерба.

Информационный риск является опасное для объекта или субъекта информатизации событие, при реализации которого возможно нанести ущерб, как для информационной сферы, так и для информационного обслуживаемого объекта в целом. Информационные риски, связанные с информационной безопасностью (ИБ) с помощью современных методик анализа и управления рисками.

Определение рисков в сфере ИБ – это вероятность того, что предприятие или организация могут понести убытки из-за нарушения безопасности информационной системы (ИС). При этом часто понятие риска рассматривается с понятием угрозы, где угроза ИБ – это потенциально возможное происшествие, которое может быть совершенно преднамеренно или случайно, но при этом оказывает нежелательное воздействие как на компьютерную систему, так и на информацию, которая находится и обрабатывается и в ней. Основное отличие риска от угрозы состоит в том, что риск имеет как количественную оценку возможных потерь, так и оценки вероятности реализации угрозы.

Если рассматривать обеспечение ИБ к ИС для каких-либо проектов требующих финансовых затрат на их реализацию необходимо четко сформулировать задачу и поставить конкретную цель которую необходимо достичь. Существуют различные способы обоснований проектов подсистем обеспечения безопасности, но на практике свою реализацию получили в основном два подхода: первый заключается в проверке соответствия уровня защищенности ИС требованиям стандартов в данной области, второй – в построении системы обеспечения ИБ, которая производит как оценку, так и управление рисками.

Для того, чтобы риск описывать, необходимо определить актив (ресурс) – это элемент ИС, который имеет ценность и подлежит защите, и тогда риски можно идентифицировать по угрозе (с помощью которой вызван данный риск), ресурсу (для которого реализована данная угроза) и уязвимости (благодаря которой может быть реализована данная угроза в отношении данного ресурса). Т.е. при оценке риска, обязательно необходимо оценить: с какой частотой происходит нежелательное событие, какая вероятность данному ресурсу нанести вред, а также, сколько будет составлять потери от нанесенного ущерба [4]. Проведение оценки рисков есть очень длительной и трудоемкой задачей, при этом нет стандартных общепринятых подходов и методик для оценки рисков в конкретной ситуации. В основном факторы риска, такие как угроза, уязвимость, ущерб рассматриваются и анализируются с помощью эвристических подходов и методов за счет проведения экспертизы разными экспертами, за счет этого результаты могут отличаться друг от друга [7] и при этом возникать следующие проблемы:

- информация о риске очень часто не полная и имеет неоднозначные свойства;
- для достижения улучшения оценок необходимо назначать не менее двух специалистов в данной области;
- существует определенная сложность построения модели ИС и оценки ее уязвимости;
- сложность объединить элементы в одну систему из различных источников;
- требуется длительное время на оценку рисков, при этом потеря актуальности результатов наступает очень быстро.

Т.е. необходимо перебрать множество методов оценки риска ИБ, который будет обеспечивать наилучший результат с максимальной вероятностью оценки [3].

Сейчас на практике применяется множество разнообразных методик для анализа информационных рисков. Отличие существующих методик состоит в том, как они оцениваются: количественно, качественно или с помощью шкал оценки уровня риска. Рассмотрим данные методики.

Для оценки уровня риска организациями используется шкалы оценки, который в большей степени несут в себе описательный характер и делятся на: от 0 до 1 и разбивки на уровни: «очень низкий», «низкий», «средний», «высокий», «очень высокий» (таблица) [2].

Таблица

Уровни шкалы для оценки факторов риска

Table

Scale levels in risk assessment

Уровни шкалы		Угрозы	Ущерб	Уязвимости (У)
Очень низкий	от 0 до 0,2	Событие практически никогда не происходит	Незначительные потери материальных средств и ресурсов	У, которой можно пренебречь
Низкий	от 0,2 до 0,4	Событие случается редко	Более заметные потери материальных активов	Незначительная У, которую можно легко устранить
Средний	от 0,4 до 0,6	Событие вполне возможно при определенном стечении обстоятельств	Достаточные потери материальных активов или ресурсов	Умеренная У
Высокий	от 0,6 до 0,8	Скорее всего, событие произойдет при организации атаки	Значительный урон репутации и интересам, что может представлять угрозу для продолжения деятельности	Серьезная У, ликвидация возможна, но связана со значительными затратами
Очень высокий	от 0,8 до 1	Событие, вероятнее всего, произойдет при организации атаки	Разрушительные последствия и невозможность ведения деятельности	Критическая У, малая доля возможности ее устранения

Каждая организация разрабатывает шкалу оценки самостоятельно, поэтому могут встречаться различные градации в виде присвоения данным последствиям цифровых значений, которые могут быть как линейными, так и нелинейными, при этом смысл оценки остается прежним.

Если необходимо получить комбинации вероятности и воздействий, то используя шкалу уровней воздействия, строится матрица вероятностей, которая дает возможность присвоения ранга рискам: низкий, средний или высокий [9].

Количественный метод – включает в себя количественную оценку рисков, которая используется для исследуемых угроз. При этом связанные с ними риски можно будет сопоставить с конечными количественными значениями (в денежном эквиваленте, человекоресурсах или процентах и т.д.) и позволит получить результат в виде конкретных значений объектов оценки риска при реализации угроз ИБ [1, 5].

При количественном анализе риска используются различные методы оценки: аналитический метод; метод анализа целесообразности затрат; метод экспертных оценок; статистический метод; метод использования аналогов.

Количественная оценка рисков производиться с помощью различных факторов: необходимо определить ценность информационного актива; произвести количественную оценку потенциального ущерба от реализации каждой угрозы для каждого рассматриваемого информационного актива; определить вероятность реализации каждой из угроз ИБ; определить потенциальный ущерб для каждой угрозы и актива за определенный установленный период времени. Далее для каждой угрозы провести полученный анализ ущерба. После проведения

количественной оценки принимается решение, что делать с риском: принять, снизить или перенести [10].

Качественный метод не использует в своей оценке денежных измерений, а используется присвоение показателя по шкалам (пятибалльная шкала от 0 до 5 или десятибалльная от 0 до 10 или трехбалльная: низкая, средняя, высокая). Данный метод проводится сотрудниками (компетентными в области проведения оценки рисков и угроз) с помощью различных методов: анкетирование, тренинги, личные встречи, групповые встречи, опросы, интервьюирование и после сбора информации уже проводиться качественная оценка рисков, в которой необходимо определить:

- ценность информационных активов;
- вероятность реализации угрозы для информационного актива;
- возможность достижение положительного результата реализации угрозы в зависимости от данного состояния ИБ и внедренных средств защиты и мер;
- по каждой угрозе провести анализ конечных результатов и уровень риска.

Конечным результатом проведения качественной оценки должен быть конкретный результат для снижения рисков до минимального или приемлемого уровня, а также составлен список мер безопасности и определенный набор правил и действий [6].

Рассмотрев методы анализа информационных рисков можно сделать вывод, что с помощью всех методов можно определить перечень актуальных угроз, выбрать эффективные контрмеры и средства защиты. Главное определиться, что надо получить в результате – оценку в денежном эквиваленте и затратить на это больше времени, но получить конкретные цифры по затратам и возможному ущербу, использовав количественный метод оценки рисков. Либо выбрать более простой и быстрый путь – получив субъективный ответ на затраты и выгоды от внедрения средств защиты информации и ущерб, использовав качественный метод или метод шкалы оценки уровня риска [9, 11].

Следовательно, управление ИБ все в большей степени становиться не только необходимым, но и обязательным элементом в функционировании и управлении любого предприятия, организации. При этом ИБ имеет значение не только для сбора, обработки и хранения информации, но и для контроля: своевременного выявления угроз ИБ, уязвимостей информационной системы и меры по их устранению и предупреждению, используя существующие методы оценки уровней рисков и внедрения новых, использовав основные законы международных стандартов управления ИБ, законов ФСТЭК РФ.

ЗАКЛЮЧЕНИЕ

В данной статье было рассмотрено: общая характеристика рисков; информационные риски, связанные с информационной безопасностью; оценка рисков с помощью существующих методик. Из этого выяснили, что в ходе оценки риска можно оценить, как частоту возникновения нежелательных событий и вероятность того, что какое-то данное событие может нанести вред ресурсу, так и самое главное – стоимость данного ущерба. При оценке рисков ИБ можно выделить недостатки: оценка носит практически всегда формальный характер; оценивается без расследования на случайной, а не постоянной основе. Это влияет на то, что существующие важные данные остаются неучтенными и осведомленность лиц, которые принимают, какое-либо решение по ликвидации рисков во многих организациях будет недостаточной. Необходимо так же помнить, что главный риск – это человек, который предоставляет для ИБ наибольшую опасность в преднамеренной или не преднамеренной человеческой ошибке. Так как отсутствуют общепринятые подходы и методики для оценки рисков и в каждом конкретном случае необходимо тщательно просчитывать и продумывать все факторы риска, проводить анализ и расчет, что

является очень трудоемкой задачей, кроме того еще и существует вероятность получить ошибочный результат. Можно сделать вывод, что из всех приведенных методов оценки рисков необходимо применять совокупность методов анализа, обработки информации и только после этого оценивать риски ИБ, и осуществлять управление ИБ. Так же необходимо уменьшать «ручной труд», использовать существующие современные методологии оценки рисков, и все более переходить к оценке рисков с помощью интеллектуального анализа данных нейронных сетей [12].

Список литературы

1. Билозерова А.А., Микова С.Ю., Нестеренко М.А. Оценка рисков ИБ при использовании ERP-систем // М.: Молодой учены. 2016. №15. С. 152-155.
2. Булдакова Т.И., Миков Д.А. Реализация методики оценки рисков информационной безопасности в среде Matlab // М.: Вопросы кибербезопасности. 2015. №4(12). С. 53-61.
3. Вопросы управления информационной безопасностью / Курило А.П., Милославска Н.Г., Сенаторов М.Ю., Толстой А.И. М.: Горячая линия – Телеком, 2015. 234 с.
4. Герасименко В.А., Малюк А.А. Основы защиты информации. М.: Инкомбук, 1997.
5. Львова А.В. Методы анализа и управления рисками безопасности защищено информационной системы: Автореф. Дис. Канд. Тех. Наук. М., 2009. 198 с.
6. Методика определения угроз безопасности информации в информационных системах, 2015г. URL: https://fstec.ru/component/attachments/download/812 (дата обращения 07.01.2019).
7. Сибикина И.В. Анализ рисков информационной безопасности с использованием системы нечеткого вывода // Научный вестник НГТУ Science Bulletin of the NSTU том 65, 2016. № 4. С. 121–134
8. Хоффман Л.Дж. Современные методы защиты информации. М: Советское радио, 1980.
9. International Standard ISO/IEC 27000, 2009 y. URL: http://pqm-online.com/assets/files/lib/std/iso_iec_27000-2009.pdf (дата обращения 15.11.18)
10. Information security risks assessment: a case study / Samuel C.A., Bonaventure N, Olasunkanmi A., RobinLlal Khoshi, Samarappulige I.M. // P 13 [Электронный ресурс]: file:///D:/англоязычные%20стаатьи/1812_04659.pdf
11. Information security risk management: an intelligence-driven approach // Jeb Webb, Sean Maynard, Atif Ahmad, Graeme Shanks. Australasian Journal of Information Systems. Volume 18 Number 3, 2014
12. Reversible Recurrent Neural Networks // Matthew MacKay, Paul Vicol, Jimmy Ba, Roger Grosse, University of Toronto, Vector Institute [Электронный ресурс]: https://arxiv.org/pdf/1810.10999.pdf

References

1. Bilozerova A.A., Mikova S.Yu.. Nesterenko M.A. Risk assessment of is when using ERP-systems // M.: Molodoy ucheny 2016. №15. p. 152-155.
2. Buldakova T.I., Mikov D.A. Implementation of information security risk assessment methodology in Matlab environment M.: Voprosy kiberbezopasnosti // Voprosy kiberbezopasnosti 2015. №4(12). p. 53-61.
3. Information security management issues Kurilo A.P., Miloslavska N.G., Senatorov M.Yu., Tolstoy A.I. Goryachaya liniya – Telekom, 2015. 234 p.
4. Gerasimenko V.A., Malyuk A.A. Framework for the protection of information by information protection M.: Inkombuk. 1997.
5. Lvova A.V. Methods of analysis and management of security risks protected information system: Avtoref. Dis. Kand. Tekh. Nauk. M.: 2009. 198 p.
6. Methodology for determining information security threats in information systems, 2015 y. URL: https://fstec.ru/component/attachments/download/812 (data obrashcheniyaya 07.01.2019).
7. Sibikina I.V. Information security risk analysis using fuzzy inference system // Nauchnyy vestnik NGT Science Bulletin of the NSTU tome 65, 2016. № 4. p. 121–134.
8. Khoffman L.Dzh. Modern methods of information security. M: Sovetskoye radio. 1980.

9. International Standard ISO/IEC 27000, 2009 y. URL: http://pqm-online.com/assets/files/lib/std/iso_iec_27000-2009.pdf (data obrashcheniyaya 15.11.18)

10.Information security risks assessment: a case study / Samuel C.A., Bonaventure N, Olasunkanmi A., RobinLlal Khoshi, Samarappulige I.M. // P 13 [Electronic resource]: file:///D:/англоязычные%20стаатьи/1812_04659.pdf

11.Information security risk management: an intelligence-driven approach // Jeb Webb, Sean Maynard, Atif Ahmad, Graeme Shanks. Australasian Journal of Information Systems. Volume 18 Number 3, 2014.

12.Reversible Recurrent Neural Networks // Matthew MacKay, Paul Vicol, Jimmy Ba, Roger Grosse, University of Toronto, Vector Institute [Electronic resource]: https://arxiv.org/pdf/1810.10999.pdf

Маслова Мария Александровна, старший преподаватель, аспирант Севастопольского государственного университета
Maslova Maria Aleksandrovna, senior lecturer, postgraduate, Sevastopol state University