Научная статья
Original article
УДК 368

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ДЛЯ СОЗДАНИЯ МЕТОДИКИ ОЦЕНКИ УЩЕРБА ОТ РЕАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СФЕРЕ СТРАХОВАНИЯ

DEVELOPMENT RECOMMENDATIONS FOR THE CREATION OF A METHODOLOGY FOR ASSESSING DAMAGE FROM THE REALIZATION OF THREATS INFORMATION SECURITY IN THE INSURANCE INDUSTRY

Бурзунов Данил Денисович, магистрант, Московский государственный технический университет им. Н.Э. Баумана, г. Москва daniel.burzunov@mail.ru

Burzunov Danil Denisovich, undergraduate, Bauman Moscow State Technical University, Moscow daniel.burzunov@mail.ru

Аннотация: Управление риском является одним из инструментов повышения стабильности бизнеса. Оценка ущерба, наряду с вероятностной оценки возможных негативных событий (угроз) является одной из двух ключевых задач управления риска. В тех случаях, когда копания оценивает собственные риски, доступность информации об объекте защиты делает оценку простой задачей. Однако в случаях, когда оценку проводит внешний агент, которым может выступать страховая компания, информационная асимметрия и конфликт интересов сторон страховых отношений значительно повышает сложность проведения достаточно точной для безопасности выгодоприобретателя оценки. В статье проводится анализ существующих подходов к оценке ущерба, которые можно использовать для определения финансовых потерь, вызванных

нарушениями информационной безопасности и которые используются отечественными компаниями различных отраслей. Статья выделяет ключевые аспекты, которые необходимо учитывать при создании методики оценки ущерба, включая определение вероятности и влияния угроз, а также расчет экономических последствий. Рекомендации, разработанные в статье, направлены на разработку надежной и точной методики оценки ущерба рисков информационной безопасности. Такая методика может способствовать более прозрачной и точной оценке ущерба заказчика для определения корректной страховой премии, а также подбора других параметров предлагаемых на рынке страховых продуктов.

Annotation: Risk management is one of the tools for increasing business stability. Damage assessment, along with probabilistic assessment of possible negative events (threats) is one of the two key tasks of risk management. When a company assesses its own risks, the availability of information about the object of protection makes the assessment a simple task. However, in cases when the assessment is carried out by an external agent, which can be an insurance company, information asymmetry and conflict of interests of the parties to insurance relations significantly increases the complexity of carrying out an assessment accurate enough for the safety of the beneficiary. The article analyzes existing damage assessment approaches that can be used to determine financial losses caused by information security breaches and that are used by domestic companies in various industries. The article highlights the key aspects to be considered when creating a damage assessment methodology, including determining the probability and impact of threats, as well as calculating the economic consequences. The recommendations developed in the article aim to develop a reliable and accurate damage assessment methodology for information security risks. Such a methodology can contribute to a more transparent and accurate assessment of the customer's damage to determine the correct insurance premium, as well as the selection of other parameters of insurance products offered in the market.

Ключевые слова: оценка ущерба, страхование риска, угрозы информационной безопасности, управление рисками в коммерческой организации

Keywords: damage assessment, risk insurance, information security threats, risk management in a commercial organization

Оценка риска за последние десятилетия стала ключевым направлением развития сферы информационной безопасности. Концепция обеспечения безопасности за счёт анализа рисков выходит далеко за пределы области ИБ, повсеместно совершенствуются инструменты для защиты от рисков. В сфере информационной безопасности это связано в первую очередь с тем, что объём реализованных угроз в сфере ИБ растёт с каждым годом вне зависимости от сферы человеческой деятельности. Ущерб от реализации таких угроз также становится только больше.

Сложившаяся ситуация стимулирует развитие новых методик оценки риска для коммерческих организаций. Акцент в таких методиках должен выделяться не только вероятности возникновения рисковых событий, но и количественной оценке последствий от их реализации. Сейчас оценке ущерба, как показано в работе, уделяется гораздо меньше внимания, чем оценке вероятности реализации угрозы.

Методики оценки ущерба не являются принципиально новым инструментом: уже много лет отечественные организации разрабатывают собственные методики, которые применяются в различных сферах деятельности. Особенностью таких методик является их внутренняя направленность: предполагается, что методика применяется «изнутри» объекта оценки. Таким образом, оценщик обладает полной информацией о системе.

Однако для рынка страхования важно уметь проводить оценку возможного ущерба, исходя из информационной асимметрии между страховщиком и заказчиком. Такая методика должна обладать нужной гибкостью, позволяя получить оценку в условиях ограниченной информации.

Одним из хрестоматийных примеров методических указаний является документ компании РЖД, описывающий оценку ущерба от случая реализации угрозы транспортных происшествий. В документе рассматриваются случаи

оценки события уже после его свершения (реализации риска и причинению ущерба). Такой подход актуален при необходимости подготовки отчётности о произошедшем событии (в том числе для регулятора), а также для расчёта выплат пострадавшим сторонам, однако не предполагает предиктивного подхода к рассмотрению ещё не реализовавшихся рисков и оценки из потенциального ущерба.

Согласно документу, расчет реального ущерба осуществляется по следующей формуле (1):

$$Y_{\text{тп}} = \sum_{i=1}^{15} Y_i \qquad (1)$$

, где в качестве Y_i представлены различные составляющие ущерба, разделённые между возможными объектами угрозы. Приводится описание каждого из типов ущерба, также типовые формы для сбора необходимой информации и её структурирования, а также рекомендации по её дальнейшей обработке.

В некоторых случаях приводятся дополнительные формулы, описывающие корректный расчёт затрат на определённые (в основном – восстановительные) действия, стоимость которых должна быть включена в одну или несколько составляющих ущерба. Однако наличие конкретных формул скорее является исключением, чем правилом. Формулы раскрывают расчёт промежуточных узкопрофильных показателей низкой сложности и приведены скорее в качестве «подсказки» к корректному расчёту.

Схожую структуру имеют большинство методик оценки ущерба для нарушений работы крупных узкопрофильных систем, разрабатываемых крупными отечественными организациями. В методических рекомендациях расчета ущерба от несанкционированных подключений к сетям газораспределения и газопотребления и несанкционированных вмешательств в работу приборов учета газа выдержаны все положения из методики РЖД. Также в методики присутствуют следующие особенности:

- Отсутствует градация между возможными аварийными ситуациями.
- Описаны источники получения информации для проведения оценки.
- Описан порядок действий для проведения оценки в случае реализации события.
- Для различных подвидов нарушения работы системы приведены разные формулы расчёта (имеют место повышение точности оценки и гибкости методики).
- Экологический ущерб не рассматривается в методике, приводится ссылка на НПА, описывающий порядок проведения расследования в случае причинения вреда экологии.
- Помимо затрат на восстановление и прямых потерь, в методике также описан экологический ущерб (косвенно), регуляторные штрафы, потери от упущенной выгоды.

Методические рекомендации по проведению количественного анализа риска аварий на опасных производственных объектах магистральных нефтепроводов и нефтепродуктопроводов описывают аналогичный процесс оценки для ещё одной сферы тяжёлой промышленности. В отличие от предыдущих документов, в методике федеральной службы по экологическому, технологическому и атомному надзору имеет место разделение типов негативных событий в зависимости от этапа цикла, на котором произошло событие, а также по его тяжести. Ещё одной особенностью является рассмотрение типовых сценариев, в которых описывается применение методики, что делает инструмент оценки более доступным и наглядным.

Ещё одним отличием методики является её абстрактность. Большой приоритет отдан общим параметрами и коэффициентам, которые характеризуют конкретное происшествие. На основе оценённых экспертным образом значений таких параметров описывается инцидент, ущерб от которого впоследствии будет оценен. Это ключевой элемент данной методики, поскольку опосредованность оценки каждого из событий позволяет использовать методику в качестве

инструмента предсказывания возможного ущерба, вместе его фактической оценки.

К другим особенностям инструмента относятся следующие её отличия от предыдущих рассмотренных методик:

- В формулах используются параметры и коэффициенты, которые предполагают статистическую оценку. К ним не приводятся значения по умолчанию или расчётные формулы.
- Для перечня возможных причин реализации рискового события описывают т.н «Дерево событий», благодаря которому проще определить конфигурацию и тип реализовавшегося рискового события.
- Методика имеет огромное количество факторов, требующих точной и детальной оценки, что подразумевает наличие у агента-оценщика полной информации о системе-объекте оценки. Наличие такого количества информации у внешнего агента (аудитора, страховой компании) не позволяет в краткие сроки и с относительно небольшими затратами получить нужный объём информации для применения методики.

Здесь раскрывается ключевой фактор проектируемой методики: цель работы предполагает разработку инструмента, которым сможет пользоваться внешний агент. Таким образом инструмент должен учитывать эффект информационной асимметрии между владельцем объекта защиты и его оценщиком, чего мы не наблюдаем в последней методике.

На основе проанализированных документов можно сделать следующий вывод о структуре методических указаний по оценке ущерба, применяемых в РФ:

- Методика должна содержать в себе ограничения к собственному применению и приводить указания к действиям в случае, если методику применить нельзя ввиду наложенных ограничений.
- В случае, если методика предполагает учёт специфичного типа ущерба, высокую точность оценки которого невозможно получить в рамках имеющегося инструмента, тип ущерба рассматривается отдельно. Приводятся

ссылки на нормативные документы, регулирующие (описывающие) порядок оценки такого ущерба.

- Для повышения гибкости методики следует приводить различные значения по умолчанию для различных исходных конфигураций системы, где это приведёт к повышению точности оценки.
- Использование экспертного метода оценки риска допускается, однако подразумевает более подробное описание алгоритма обработки исходных данных и пограничных случаев.

Методика также должна содержать ограничения. Прежде всего, к ним относится утверждение о гарантии покрытия ущерба от рискового события, которое получает заказчик. Это требование является обязательным, поскольку именно при использовании этого подхода страхование риска зависит, в том числе, от ущерба от угрозы. В противном случае страховая организация управляет своим продуктом в зависимости от вероятности события и оценка ущерба как таковая теряет смысл – страховщик сам выставляет ту сумму страхования, которую готов покрыть без потерь для себя, а клиент соглашается на условия или отказывается от сделки.

Важно отметить, что такой подход не противоречит общей страховой практике в нашей стране. Страховое возмещение не может превышать размера прямого ущерба застрахованному имуществу страхователя или третьего лица при страховом случае, если договором страхования не предусмотрена выплата страхового возмещения в определенной сумме.

Естественными ограничением является потребность в сборе информации о компании-заказчике. Методика раскрывает индивидуальный подход к страхованию за счёт сбора сведений о конкретной компании вместо того, чтобы строить модели оценки за счёт статистических данных. Такой способ требует относительно высокого объёма затрат на формирование оценки, однако её точность будет значительно выше, чем использование статистических данных.

Для повышения гибкости методики и упрощения работы с ней по ряду параметров в методике будут предложены значения по умолчанию, а также

описаны правила, в соответствии с которыми это значение может формироваться. Однако использование только значений по умолчанию очень сильно снижает возможную точность оценки, что в том числе должно отражаться в точности итоговой оценки ущерба.

Отдельно также стоит оговорить исключение из методики ущерба, причинённого жизни или здоровью сотрудникам организации. Оценка такого ущерба является серьезным междисциплинарным вопросом, который в том числе находится в ведении области здравоохранения, а также особого медицинского страхования (в том числе и обязательного, которое может предоставлять работодатель).

Отдельно следует отметить ограничения, который на рекомендательной или обязательной основе приводятся к исполнению в НПА. В методике будут приведены ключевые ограничения, которые затрагивают этический вопрос страхования, а также вопросы, которые регулируют зоны соприкосновения страховой сферы деятельности с другими и разрешает возникающие там противоречия. Методика я обязательном порядке должна учитывать такие ограничения и исходить из них, чтобы не противоречить сложившимся юридическим практикам.

Литература

1. Мирзоян Наталия Витальевна Проблемы оценки реального ущерба в России // Имущественные отношения в РФ. 2018. №10 (205). URL: https://cyberleninka.ru/article/n/problemy-otsenki-realnogo-uscherba-v-rossii (дата обращения: 15.04.2024).

2. Об утверждении методических рекомендаций по расчету ущерба от транспортных происшествий и иных связанных с нарушением правил безопасности движения и эксплуатации железнодорожного транспорта Событий в ОАО "РЖД": Распоряжение ОАО "РЖД" n 681р [принято 03.04.2008] – Доступ из справочно-правовой системы Гарант. – Текст: электронный.

3. Об утверждении методических рекомендаций расчёта ущерба от несанкционированных подключений к сетям газораспределения и газопотребления и несанкционированных вмешательств в работу приборов учёта газа: Приказ Минэнерго России N 975 [утверждён 18.12.2015]. Доступ из справочно-правовой системы Гарант. – Текст: электронный.

4. Об утверждении Руководства по безопасности "Методические рекомендации по проведению количественного анализа риска аварий на опасных производственных объектах магистральных нефтепроводов и нефтепродуктопроводов": Приказ Ростехнадзора N 478 [утверждён 29.12.2022] Доступ из справочно-правовой системы Гарант. – Текст: электронный.

5. Оценка ущерба и страхового возмещения: метод. указ. по дисциплине для студентов напр. подгот. 38.02.02 Страховое дело (по отраслям) оч. и заоч. форм обучения / сост. : С.А. Буряков. – Шахты : ИСОиП (филиал) ДГТУ в г. Шахты, 2019. – 55 с.

6. Голубинский А.Н., Алехин И.В. Анализ распределений ущербов при реализации угроз в информационно-технических системах // Вестник ВИ МВД России. 2016. №3. С. 24–32.
URL: https://www.elibrary.ru/item.asp?id=26683939 (дата обращения: 01.03.2024).

7. Таныгин, Максим О. и др. Модель оценки ущерба от инцидентов информационной безопасности. Безопасность информационных технологий, [S.l.], v. 28, n. 2, p. 98–106, 2021. ISSN 2074-7136. Доступно на: . Дата доступа: 02.04.2024. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

8. Мартыненко Н. Э. Понятия «вред» и «ущерб» и их уголовно-правовая оценка // Труды Академии управления МВД России. 2020. № 2 (54). С. 103–109с.

References

1. Mirzoyan Natalia Vitalievna Mirzoyan Problems of real damage assessment in Russia // Property relations in the Russian Federation. 2018. №10 (205). URL: https://cyberleninka.ru/article/n/problemy-otsenki-realnogo-uscherba-v-rossii (date of reference: 15.04.2024).Kuznetsov Y.V., Bykova N.V. Efficiency of state support for small business in Russia // Finance: theory and practice. 2017. T. 21. № 6. C. 50-59.

2. On Approval of Methodological Recommendations for Calculating Damage from Transportation Accidents and Other Events in JSCo "Russian Railways" Related to Violation of the Rules of Traffic Safety and Operation of Railway Transportation: Order of JSC "Russian Railways" n 681r [adopted 03.04.2008] - Access from the reference and legal system Garant. - Text: electronic.

3. On approval of methodological recommendations for calculating damage from unauthorized connections to gas distribution and gas consumption networks and unauthorized interference in the operation of gas metering devices: Order of the Ministry of Energy of Russia N 975 [approved 18.12.2015]. Access from the reference and legal system Garant. - Text: electronic.

4. On Approval of the Safety Guidelines "Methodological Recommendations for Quantitative Analysis of the Risk of Accidents at Hazardous Production Facilities of Trunk Oil Pipelines and Oil Product Pipelines": Order of Rostechnadzor N 478 [approved 29.12.2022] Access from the reference and legal system Garant. - Text: electronic.

5. Estimation of damage and insurance compensation: method. instructions on the discipline for students of the field of training. 38.02.02 Insurance business (by branches) full-time and part-time forms of training / comp. S.A. Buryakov. - Shakhty : ISOIP (branch) DSTU in Shakhty, 2019. - 55 c.

6. Golubinsky A.N., Alekhin I.V. Analysis of damage distributions at realization of threats in information-technical systems // Vestnik VI of the Ministry of Internal Affairs of Russia. 2016. №3. C. 24-32. URL: https://www.elibrary.ru/item.asp?id=26683939 (date of access: 01.03.2024).

7. Tanygin, Maxim O. et al. Information security incident damage assessment model. Information Technology Security, [S.l.], v. 28, n. 2, p. 98-106, 2021. ISSN 2074-7136. Available at: . Access date: 02.04.2024. DOI: http://dx.doi.org/10.26583/bit.2021.2.09.

8. Martynenko N. E. Notions of "harm" and "damage" and their criminal-legal assessment // Proceedings of the Academy of Management of the Ministry of Internal Affairs of Russia. 2020. № 2 (54). С. 103-109с.