УДК 004.056.5

# 59. ОЦЕНКА РИСКОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МЕТОДЫ И ПОДХОДЫ

*Вегера Ю.С., студент гр.478104, Федюкович Т.В., ассистент кафедры ЭИ*

*Белорусский государственный университет информатики и радиоэлектроники г. Минск, Республика Беларусь,*

*Ефремов А.А. – канд. экон. наук, доцент каф. ЭИ*

**Аннотация.** В условиях стремительного развития цифровых технологий и увеличения количества киберугроз оценка рисков в области информационной безопасности становится критически важной для организаций. В данной статье подробно анализируются основные подходы к оценке рисков: количественный, качественный и комбинированный. Особое внимание уделяется сравнению популярных методик управления рисками (OCTAVE, CRAMM, MSAT, FRAP и другие) с учетом их применимости для различных типов организаций. Показано, что наиболее эффективным является комбинированный подход, сочетающий числовые и экспертные оценки для обеспечения комплексного анализа угроз. Подчеркивается важность анализа рисков как неотъемлемой части стратегического планирования и управления компанией, направленного на защиту информационных активов и минимизацию финансовых и репутационных потерь. Особое внимание уделено практическим аспектам внедрения системы управления рисками и минимизации потенциального ущерба.

**Ключевые слова:** информационная безопасность, оценка рисков, управление рисками, количественный анализ, качественный анализ, комбинированные методики, CRAMM, Risk Watch, ГРИФ, CORAS, MSAT, FRAP, OCTAVE, угрозы информационной безопасности, защита информации.

Информационная безопасность — это сложная система действий, методов и технических средств, предназначенная для защиты информации от различных опасностей, включая несанкционированный доступ, утечку данных, изменение или полное уничтожение. Главная цель — обеспечить ключевые характеристики информации: конфиденциальность, целостность и доступность. Конфиденциальность подразумевает, что доступ к информации имеют только уполномоченные пользователи, исключая несанкционированное получение данных. Целостность гарантирует сохранение точности и полноты данных, предотвращая несанкционированное внесение изменений, что может быть реализовано, например, посредством контрольных сумм или цифровых подписей. Доступность гарантирует возможность использования информации и связанных с ней сервисов всегда, когда это необходимо авторизованным пользователям, защищая системы от атак и поддерживая отказоустойчивость.

Информационная безопасность - одна из проблем, с которой столкнулось современное общество в процессе массового использования автоматизированных средств обработки информации [1].

В современном мире риски, связанные с информационной безопасностью, представляют собой одну из наиболее серьезных угроз для компаний. Оценка этих рисков является критически важной частью стратегического планирования каждой организации. Информационные риски включают в себя широкий спектр потенциальных опасностей и слабых мест, способных нанести вред информационным системам и корпоративным данным. Существует множество методик, разработанных для помощи организациям в проведении анализа рисков информационной безопасности. Использование этих методик приносит значительные выгоды, позволяя компаниям не только защищать свои ценности, но и успешно адаптироваться к быстро меняющейся цифровой среде [2]. Процесс оценки рисков информационной безопасности является неотъемлемой частью общего управления компанией, поскольку выявление и своевременное устранение неприемлемых рисков позволяет уменьшить вероятность репутационного и финансового ущерба.

Риск в области информационной безопасности – это возможность возникновения неблагоприятных последствий из-за воздействия угроз на информационные активы.

Для анализа рисков, касающихся защиты информации, используются различные подходы, включая количественный, качественный и комбинированный анализ.

Количественный подход подразумевает применение числовых значений для определения вероятности возникновения угроз и масштаба потенциального ущерба. Количественная оценка рисков уместна в ситуациях, когда исследуемые угрозы и сопутствующие им риски могут быть сопоставлены с конкретными числовыми показателями, такими как денежные суммы, процентные ставки или временные рамки. Данный метод позволяет получить точные значения для объектов оценки риска при реализации угроз информационной безопасности. Первым шагом является оценка всех информационных активов организации в денежном выражении для определения их значимости и

критичности. Затем определяется размер возможного ущерба в случае возникновения конкретных рисков для отдельных информационных активов. Следующим этапом является вычисление вероятности наступления каждой возможной угрозы для активов. Далее рассчитывается общий потенциальный ущерб для каждого вида угроз с учетом определенного временного периода. В заключение проводится анализ полученных данных и определяется количественное значение ущерба, связанного с конкретной угрозой [2].

Ввиду значительной неопределенности, точное количественное определение объекта оценки не всегда возможно. В таких ситуациях используется качественный метод.

При качественном подходе к оценке объекта не используются численные или финансовые показатели. Вместо этого риску присваивается определенный уровень согласно системе оценивания: баллы, ранги. Сначала оценивается ценность информационных активов. Затем вычисляется вероятность возникновения угрозы для актива. Далее определяется вероятность реализации угрозы с учетом существующих мер защиты. После этого делается заключение о величине риска, основываясь на ценности актива и вероятности возникновения риска. В завершение проводится анализ и выставляется оценка для каждой угрозы и размера риска. Также разрабатываются защитные меры для снижения ущерба от каждой угрозы. Для сбора данных при качественной оценке рисков используются опросы, анкетирование, личные беседы с целевыми группами. Анализ рисков информационной безопасности качественным методом должен выполняться с привлечением опытных специалистов в соответствующей области.

Оба способа оценивания рисков – количественный и качественный – имеют свои плюсы и минусы.

Часто продуктивнее применять комбинированный метод, совмещая количественные и качественные техники оценки рисков. Это предоставит наиболее всеобъемлющий и целостный подход к решению проблемы управления рисками.

К комбинированным методикам управления рисками относятся методики CRAMM, Risk Watch, ГРИФ.

Методика CRAMM не учитывает сопроводительной документацию, такой как описания бизнес-процессов или отчетов по проведенным оценкам рисков. В отношении стратегии работы с рисками CRAMM предполагает использование только методов их снижения. Такие способы управления рисками, как обход или принятие, не рассматриваются. В методике отсутствуют: процесс интеграции способов управления и описание назначения каждого метода, мониторинг эффективности применяемых методов управления и методов работы с остаточными рисками, процесс реагирования на инциденты [3]. Практическое использование CRAMM требует привлечения специалистов высокой квалификации, трудозатрат и продолжительности процесса оценки рисков. Также следует учесть высокую стоимость лицензии.

Методика Risk Watch основывается на количественных и качественных подходах для оценивания рисков. Объем работ по анализу рисков с применением данного метода сравнительно невелик. Этот метод подходит, если нужно проанализировать риски на программно-техническом уровне защиты, не принимая во внимание организационные и административные аспекты. Важным преимуществом Risk Watch считается интуитивно понятный интерфейс и высокая гибкость метода, обеспечиваемая возможностью добавления новых категорий, описаний, вопросов.

Методика ГРИФ комплексно оценивает риски, применяя как количественные, так и качественные методы, и определяет критерии, при которых их приемлемость для компании может быть обоснована. В ее состав входит расчет возврата инвестиций на внедрение мер безопасности. В отличие от других подходов к анализу рисков, ГРИФ предлагает исчерпывающий набор стратегий их снижения: обход, снижение и принятие. При этом методика берет во внимание сопроводительную документацию, например, описания бизнес-процессов или отчеты по ранее проведенным оценкам информационной безопасности.

Комбинированные методы позволяют учесть, как объективные финансовые показатели, так и экспертные оценки, что делает процесс управления рисками более гибким и адаптивным.

К качественным методам оценки рисков относятся методики CORAS, MSAT, FRAP, OCTAVE.

В CORAS не предусмотрено регулярное обновление оценок рисков, что указывает на его пригодность для разовых задач, но не для периодических. Преимуществом CORAS является бесплатное распространение программы, реализующей эту методику, а также отсутствие необходимости в значительных ресурсах для её установки и использования.

При MSAT оценке ключевыми параметрами для программного обеспечения являются: профиль рисков для бизнеса (степень изменения рисков в зависимости от бизнес-условий, значимый фактор, не всегда учитываемый при оценке защищенности системы в организациях разных областей) и индекс эшелонированной защиты (обобщенная оценка уровня защищенности). MSAT не предоставляет количественной оценки уровня рисков, но кыачественные оценки можно соотнести с ранговой шкалой.

MSAT позволяет оценить эффективность вложений в меры безопасности, но не позволяет определить оптимальный баланс между мерами по предотвращению, обнаружению, исправлению или восстановлению информационных активов.

Модель FRAP- заключается в качественной оценке рисков. При этом акценты делаются в пользу детального анализа информационной системы посредством автоматизированных инструментов, тщательной идентификации угроз с составлением подробного перечня. В процессе оценки рисков информационной безопасности осуществляется их градация сообразно вероятности наступления и размеру урона.

Методика OCTAVE описывает способ качественной оценки рисков. Данная методология предназначена для формализации и оптимизации процесса выявления рисков информационной безопасности в организации и обеспечения возможности достижения необходимых организации результатов с минимальными расходами времени и ресурсов. Методология рассматривает людей, технологии, информационные системы, приложения, и прочие объекты в контексте их взаимосвязи с информацией и бизнес - процессами и услугами, которые они обеспечивают. Методика OCTAVE в наибольшей мере подходит организациям, осуществляющим первичное внедрение процессов управления рисками, не располагающим ресурсами для внедрения процессов анализа и управления рисками информационной безопасности на всю организацию разом и имеющим потребность в постепенной декомпозиции рисков информационной безопасности от наиболее важных рисков верхнего уровня к рискам нижнего уровня. Метод позволит итеративно распространять процессы управления рисками на всю организацию [4].

Для проведения разовой оценки уровня рисков в компании среднего масштаба рекомендуется применять методику CORAS. В сфере управления рисками, основанным на периодических технических оценках, наилучшим решением выступает методика CRAMM. Для крупных организаций, стремящихся внедрить управление информационной безопасностью с регулярными оценками не ниже организационного уровня и разработкой планов мероприятий по снижению рисков, предпочтительна методика Risk Watch.

Целью качественного, количественного и комбинированного методов является осознание действительных рисков ИБ компании, выявление списка угроз, выбор средств защиты.

Каждый способ оценки рисков имеет свои достоинства и недостатки. Количественный способ даёт наглядное представление в денежном эквиваленте по объектам оценки, однако он более трудоёмок и в ряде случаев не применим. Качественный способ позволяет произвести оценку рисков быстрее, однако оценки и результаты носят более субъективный характер и не дают наглядного понимания ущерба.

Выбор способа следует делать исходя из специфики конкретной компании и задач, поставленных перед экспертом.

Не существует универсального метода оценки рисков. Выбор подходящего метода зависит от конкретной ситуации. Важно учитывать все факторы и использовать все доступные инструменты для более полной и точной оценки рисков.

Оценка рисков безопасности и управление ими – фундамент любой стратегии информационной безопасности, поскольку они предоставляют детальное представление об угрозах и уязвимостях, способных повлечь финансовые потери, и о способах их устранения. Четкая оценка уязвимостей и понимание ценности информационных активов позволяют усовершенствовать политику и методы обеспечения безопасности, чтобы обезопасить важные активы.

Важно подчеркнуть, что оценивание рисков – не одноразовая процедура, а непрерывно развивающийся процесс. Угрозы, как и технологии, эволюционируют: возникают новые слабые места и приёмы атак. Регулярная переоценка рисков – необходимое условие для поддержания защиты на должном уровне. Более того, подобная оценка предоставляет организациям возможность принимать взвешенные решения о распределении ресурсов, внедрении инноваций и улучшении текущих процессов. В конечном итоге, это способствует созданию более надежной и защищенной информационной инфраструктуры, снижая вероятность инцидентов и их воздействия на бизнес.

В статье был рассмотрен и проанализирован процесс оценки рисков. Акцентировалась потребность и значимость применения системы оценки рисков при разработке системы защиты информации. Были также описаны и проанализированы основные методы управления рисками. Проведён анализ нескольких доступных программных продуктов для управления рисками. У каждого из продуктов есть свои преимущества и недостатки, однако область их использования зависит от особенностей конкретного предприятия.

Статья знакомит с подходами к качественной, количественной и комбинированной оценке рисков. Ввиду их ограничений, как качественные, так и количественные методы считаются неидеальными, субъективными, содержащими долю случайности и сложными для обновления или повторного применения. Поэтому наиболее эффективно использовать подход, сочетающий в себе как качественную, так и количественную оценку рисков.

***Список использованных источников:***
*1. Баранова Е.К., Бабаш Л.В. Информационная безопасность и защита информации. – М.: ИНФРА-М_РИОР, 2014.*
*2. Wikipedia [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/.*
*3. Баранова Е.К. Методики и программное обеспечение для оценки рисков в сфере информационной безопасности // Управление риском. 2009.*
*4. Методики управления рисками информационной безопасности и их оценки [Электронный ресурс]. – Режим доступа: https://safe-surf.ru/specialists/article/5194/587935/.*

UDC 004.056.5

# RISK ASSESSMENT IN THE FIELD OF INFORMATION SECURITY: METHODS AND APPROACHES

*Vegera J.S., student gr. 478104, Fedziukovich T.V., assistant of the Department of EI*

*Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus*

*Efremov A.A. – Candidate of Economic Sciences, Associate Professor*

**Annotation.** In the context of rapid development of digital technologies and increase in the number of cyber threats, risk assessment in the field of information security is becoming critical for organizations. This article analyzes in detail the main approaches to risk assessment: quantitative, qualitative and combined. Particular attention is paid to the comparison of popular risk management methods (OCTAVE, CRAMM, MSAT, FRAP and others) taking into account their applicability to different types of organizations. It is shown that the most effective is a combined approach combining numerical and expert assessments to ensure a comprehensive analysis of threats. The importance of risk analysis as an integral part of strategic planning and company management aimed at protecting information assets and minimizing financial and reputational losses is emphasized. Particular attention is paid to the practical aspects of implementing a risk management system and minimizing potential damage.

**Keywords:** information security, risk assessment, risk management, quantitative analysis, qualitative analysis, combined methods, CRAMM, Risk Watch, GRIF, CORAS, MSAT, FRAP, OCTAVE, information security threats, information protection.