ORES

Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056

ОСОБЕННОСТИ СОВРЕМЕННОГО МЕХАНИЗМА УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ В БАНКОВСКОЙ СФЕРЕ

Гобозов В. В.,
Магистр прикладной информатики; бакалавр информационной безопасности, Российский государственный гуманитарный университет
vova.gobozov01@mail.ru

Аннотация

В настоящей статье приводятся некоторые особенности процесса управления рисками в банковской сфере в нынешних условиях. Дается краткая характеристика современного подхода к управлению рисками, а также вариантов реагирования на риск, этапов, принципов и уровней управления рисками. Основываясь на этом, автор анализирует особенности современного механизма управления информационными рисками в деятельности банков. В статье содержится развернутая характеристика системе управления информационными рисками (СУИР) и принципам, которые лежат в основе ее создания и деятельности. Автор особо подчеркивает важность системного подхода в процессе управления рисками в банковской сфере, а также необходимость учета особенностей данной сферы.

Ключевые слова: риск, управление рисками, информационные риски, банковская сфера, современный механизм, СУИР, информационная безопасность.

FEATURES OF THE MODERN INFORMATION RISK MANAGEMENT MECHANISM IN THE BANKING SECTOR

Gobozov V. V.,
Master of Applied Informatics; Bachelor of Information Security
Russian State University for the Humanities
vova.gobozov01@mail.ru

ABSTRACT

This article presents some features of the risk management process in the banking sector in the current conditions. It provides a brief description of the modern approach to risk management, as well as the options for responding to risk, the stages, principles, and levels of risk management. Based on this, the author analyzes the features of the modern mechanism for managing information risks in the banking sector. The article provides a detailed description of the information risk management system (IRMS) and the principles that underlie its creation and operation. The author emphasizes the importance of a systematic approach to risk management in the banking sector, as well as the need to consider the specific features of this sector.

Keywords: risk, risk management, information risks, banking sector, modern mechanism, IRMS, information security

Управление рисками – это, прежде всего, процесс разработки, принятия и исполнения решений, а также применения средств и методов, направленных на уменьшение вероятности возникновения неблагоприятных событий и их результатов, способных помешать достижению поставленных целей. Реализация мероприятий по управлению рисками направлена на то, чтобы оценить размер рисков, выработать максимально эффективные и экономически оправданные меры по их снижению, а затем убедиться, что в результате размер рисков находиться в приемлемых рамках. Измерение (оценка и переоценка) и нейтрализация (выбор защитных средств) рисков представляют собой два взаимосвязанных и циклически чередующихся вида деятельности в процессе управления рисками.

У предприятия есть следующие возможные варианты реагирования на риск: уменьшение риска, ликвидация риска, уклонение от риска, принятие риска и переадресация (передача) риска. Каждому из вариантов присущи свои методы. Уровень риска, который остается после применения специальных методов реагирования, называется остаточным риском. Он может быть приемлемым или неприемлемым. У разных предприятий различная толерантность к риску: одни готовы рисковать в надежде на большие дивиденды, другие шарахаются от любых рискованных действий [1].

Управление рисками, согласно современному подходу, является непрерывным процессом, в ходе которого происходит перманентное выявление, анализ и измерение рисков, поиск способов работы с ними, оценка действенности применяемых мер

Этапы процесса управления рисками условно можно разбить на три группы: предварительные, основные и заключительные этапы [2].

К предварительным можно отнести следующие этапы:

- выбор объектов для анализа и определение степени детализации их рассмотрения. Он зависит во многом от величины предприятия. На небольшом предприятии объектом для анализа может быть вся информационная система; а на крупном – наиболее важные ее элементы, риски для которых либо заведомо велики, либо вообще пока неизвестны, так как всеобъемлющая оценка может оказаться слишком затратной и по времени, и в плане финансов;

- выбор методологии оценки рисков. Разумная методология должна дать ответ не только на вопрос о том, насколько приемлемы или неприемлемы существующие риски, но и определить защитные средства с учетом приемлемости для предприятия размеров возможных расходов на новые регуляторы безопасности;

- идентификация активов. В данном случае стоит учитывать, что защите подлежат не только компоненты информационной системы, но и поддерживающая инфраструктура (персонал, репутация и т.д.), необходимая для основных направлений деятельности предприятия. Надо описать внешний интерфейс предприятия, учитывать аппаратные и программные активы, классифицировать данные в плане конфиденциальности и т.д.

К основным этапам процесса управления рисками относятся:

- анализ угроз и их последствий, а также выявление уязвимых мест в защите – необходимо, в первую очередь, идентифицировать угрозы, исходя из здравого смысла, определить наиболее опасные для предприятия виды угроз, выявить источники их возникновения, по определенной шкале оценить вероятность их осуществления и определить потенциальный размер ущерба;

- оценка рисков – для определения величины риска стоит умножить вероятность осуществления угрозы на предполагаемый ущерб. Риск может быть низким, средним и высоким. Если он недопустимо высок, надо принимать дополнительные меры для его нейтрализации;

- выбор защитных мер – осуществляется предприятием в зависимости от собственных возможностей и от стоимости оборудования (программ) и его внедрения, а также обучения персонала. Новые средства должны быть совместимыми с имеющейся структурой и сложившимися на предприятии традициями.

Завершающими этапами процесса управления рисками можно считать:

- реализацию и проверку выбранных мер – эти меры необходимо запланировать заранее, с учетом наличия необходимых финансовых средств, сроков переподготовки персонала, необходимости тестирования программно-технических средств;

- оценку остаточного риска – проводится после реализации новых мер защиты, чтобы убедиться в приемлемости для предприятия остаточных рисков.

Современный подход к управлению рисками предполагает не только определение этапов этого процесса, но и уровней функционирования системы управления рисками. Обычно выделяют три таких уровня: стратегический, тактический и оперативный.

На стратегическом уровне происходит выработка принципов управления рисками. Для этого очерчиваются рамки управления рисками, формируются принципы принятия решений, управления процессами противодействия рискам, определяется толерантность предприятия к риску.

Тактический уровень представляет собой собственно систему управления рисками. Осуществляется общее руководство процессами, выбор и совершенствование методов управления рисками. Принимаются концепция и план управления рисками. Концепция управления рисками – это официально принятый документ, в котором зафиксированы решения высшего руководства предприятия об основных принципах и направлениях деятельности в управлении рисками, отражаются цели, приоритеты и обязательства различных должностных лиц в сфере риск-менеджмента. План управления рисками – это схема (краткое описание) конкретных мероприятий в ходе деятельности по управлению рисками, с указанием основных ответственных работников и необходимых ресурсов.

Оперативный уровень представляет собой процесс управления рисками, в ходе которого осуществляется основная работа с рисками (идентификация, анализ, оценка, мониторинг, реагирование).

Отметим, что отнюдь не в всегда возможно управление рисками. Для этого необходимо наличие ряда условий, таких как определенный уровень прогнозируемости внешних и внутренних условий и событий, влияющих на деятельности предприятия, культура, готовность, возможность, наличие времени и ресурсов для противодействия рискам и т.д.

Все вышесказанное справедливо и в отношении информационных рисков, которые являются одной из разновидностей рисков. В то же время у них имеются свои, характерные им особенности [3]. В любом случае, главным в процессе управления информационными рисками является системный подход, который и лежит в основе создания и функционирования системы управления информационными рисками (СУИР). [4]. Другими принципами деятельности СУИР являются:

1. Постоянное функционирование системы. Это означает, что СУИР (и средства управления, и органы управления) должна работать непрерывно.

2. Равная защищенность всех звеньев системы. Информационная система банковского предприятия в современных условиях является многоуровневой структурой, в различных звеньях которой получается, накапливается, обрабатывается, хранится и

передается информация в различных формах. А значит, надо обеспечивать ее качество на всех этих стадиях.

3. Многоуровневая защита. Эффективность деятельности СУИР увеличивается создания т.н. «рубежей защиты».

4. Адаптивная система. Она обеспечивает устойчивость предприятия к воздействию информационных рисков. Адаптивность обеспечивается, прежде всего, определенной избыточностью ресурсов и механизмов.

6. Централизованно-иерархическое управление. Позволяет создать оптимальную систему, в которой решение концептуальных проблем сосредоточенно на высшем уровне, при этом потоки информации формируются в соответствии с уровнем компетентности и полномочий органа управления, а к высшему руководству информация поступает после обработки и обобщения на более низких уровнях.

7. Дружественный интерфейс. Под этим термином понимается создание благоприятных условий (безопасность, комфорт и т.д.) для взаимодействия человека и системы, что положительно влияет на производительность труда.

8. Открытость системы. Обеспечивает возможность своевременно вносить изменения в СУИР в зависимости от характера новых рисков, а «блочная» структура системы позволяет осуществлять ее быструю модернизацию.

Рассмотрим более подробно функционирование СУИР на примере деятельности кредитных предприятий. Выбор именно банковской сферы в данной ситуации обусловлен ее особенностями.

Во-первых, риск является одним из основополагающих факторов банковской деятельности. Если это разумный и выверенный риск, банк добивается успеха, если нет – может даже обанкротиться. Банковский риск означает, что кредитное предприятие всегда стоит перед вероятностью понести ущерб из-за неблагоприятных событий, вызванных внутренними и/или внешними причинами (угрозами). Основными из них являются угрозы, приводящие к нарушению своевременности поступления, целостности, конфиденциальности и доступности информации.

Во-вторых, в информационных системах банков вероятны почти все варианты информационных рисков, так как в основе всех основных банковских рисков лежат информационные факторы. Вместе с тем, информационные риски обычно не считают отдельным видом банковских рисков, хотя они напрямую влияют на такие риски банковской деятельности, как стратегический, правовой, операционный и репутационный.

Информационные риски – это, во многом, экономические риски, так как они наносят ущерб предприятию. В свою очередь, основой любого экономического риска является информационная составляющая. Информационными являются такие виды экономических рисков, как управленческий, валютный, инвестиционный, ликвидности, кредитный и т.д.

Возможным следствием реализации информационных рисков в банковской сфере являются несанкционированный доступ к конфиденциальной информации или ее утрата; незаконное использование информационных ресурсов кредитного предприятия; кража, сбой банковской информационной системы, распространение в ней вируса, разглашение данных о банке и/или о третьих лицах [5].

В контексте создания и функционирования механизма управления информационными рисками предприятия в банковской деятельности следует учитывать ряд особенностей информационных процессов в данной сфере.

В первую очередь, банки обычно выстраивают максимальную защиту внутреннего контура своей информационной системы, что обеспечивает ее устойчивость и хорошее качество информации. При этом кредитные организации связаны с открытыми системами и большим числом некорпоративных пользователей (операции через банкоматы, интернет-

платежи), действия которых трудно контролировать. Банки стараются постоянно расширять сеть своих клиентов и территорию охвата, что усложняет защиту информации. Отметим и особую привлекательность данной сферы для кибермошенников.

Наконец, слабым местом банковской системы является довольно слабая защищенность от человеческого фактора, то есть беспечности клиентов и сотрудников организации, а также халатности и умышленных незаконных действий банковских служащих. По статистике именно этот фактор является причиной четырех из пяти инцидентов, которые имеют место в информационных системах банковских предприятий.

Ограничить возможности служащих по доступу к информации, а значит – максимально нейтрализовать влияние «человеческого фактора», позволит широкое применение современных программных, криптографических и аппаратно-технических средств. Вместе с соответствующими нормативно-правовыми и организационно-методическими механизмами они максимально затруднят возможность несанкционированного доступа к банковской информации.

Управление информационными рисками является основным направлением деятельности структур, обеспечивающих информационную безопасность. Под информационной безопасностью в банковской деятельности понимают такую степень защищенности в информационной сфере целей и интересов банков, при которой достигается приемлемый для них уровень информационных рисков. Соответственно, обязательным элементом ее является механизм управления информационными рисками [6].

Большое значение в этом аспекте имеют статус и влияние службы информационной безопасности в структуре банка. Совсем недавно вопросами информационной безопасности занимались отделы и службы автоматизации, но в последнее время банки идут по пути создания отдельных служб со своими организационно-кадровыми и финансовыми возможностями.

Еще одним определяющим фактором является отношение банка к остаточным информационным рискам. Так как невозможно создать идеальную систему, гарантирующую стопроцентную защиту от рисков, руководители (собственники) банка должны определить допустимый уровень остаточных рисков, выбирая с учетом возможностей предприятия, в том числе и финансовых, варианты защиты информации. При этом надо учитывать, что для банков, как для любых финансовых структур, информация – чрезвычайно важный ресурс и представляет немалую ценность.

Таким образом, усложнение и все более широкое внедрение информационных технологий в банковские процессы вкупе с человеческим фактором неизбежно усиливают вероятность информационного риска. В любом случае, очевидно, что в банковской сфере эффективный механизм управления информационными рисками может быть создан только с учетом особенностей данной области и происходящих в ней информационных процессов.

Список литературы:

1. Грабовой П.Г. Риски в современном бизнесе. – М.: Аланс, 2004. – 240 с.
2. Боков В. В., Забелин П. В., Федцов В. Г. Предпринимательские риски и хеджирование в отечественной зарубежной экономике. – М.: ПРИОР. – 2000.
3. Исаев Г.Н. Информационные технологии: учебное пособие М: Омега-Л, 2012, 464 с.
4. Поляков В.П. Экономическая информатика [Электронный ресурс] Режим доступа: URL: https://studme.org/207049/informatika/

printsipy_postroeniya_sistemy_obespecheniya_informatsionnoy_bezopasnosti (дата обращения: 18.07.2025).
5. Криворучко Д.С. Информационные риски в банковской сфере и их решение // Материалы XIII Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2021/article/2018024934 (дата обращения: 18.07.2025).
6. Мовсесян Е. Л. Информационная безопасность в банковских системах [Текст] / Е. Л. Мовсесян, М. В. Перова // Перспективы развития информационных технологий. – 2014. – № 21. – С. 145–150.

References:

1. Grabovoy P.G. Risks in modern business. Moscow: Alans, 2004. 240 p.
2. Bokov V. V., Zabelin P. V., Fedtsov V. G. Entrepreneurial risks and hedging in the domestic foreign economy. Moscow: PRIOR. – 2000.
3. Isaev G.N. Information technologies: a textbook Moscow: Omega-L, 2012, 464 p.
4. Polyakov V.P. Economic informatics [Electronic resource] Access mode: URL: https://studme.org/207049/informatika / printsipy_postroeniya_sistemy_obespecheniya_informatsionnoy_bezopasnost (accessed: 07/18/2025).
5. Krivoruchko D.S. Information risks in the banking sector and their solution // Proceedings of the XIII International Student Scientific Conference "Student Scientific Forum" URL: <a href="https://scienceforum.ru/2021/article/2018024934">https://scienceforum.ru/2021/article/2018024934 (date of reference: 07/18/2025).
6. Movsesyan E. L. Information security in banking systems [Text] / E. L. Movsesyan, M. V. Perova // Prospects for the development of information technology. - 2014. – No. 21. – pp. 145-150.