ОБЗОР ПОДХОДОВ К УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ РИСКАМИ

КИСЕЛЕВА Тамара Васильевна
доктор технических наук, профессор
профессор кафедры прикладных информационных технологий и программирования
МАСЛОВА Елена Владимировна
кандидат технических наук
доцент кафедры прикладных информационных технологий и программирования
ФГБОУ ВО «Сибирский государственный индустриальный университет»
г. Новокузнецк, Россия

Обзорно рассмотрены различные подходы к управлению информационными рисками, включая традиционные и современные методики. Освещены основные этапы управления информационными рисками, ключевые принципы и рекомендации для повышения защиты информационных ресурсов организации.
Ключевые слова: информационные риски, защита информации, информационная безопасность, риск-менеджмент.

Управление рисками входит в общую систему управления организацией и использует ту же модель процессов, что и другие стандарты управления. Эта модель включает четыре группы процессов: Планирование, Реализация, Проверка и Действие (ПРПД), отражающие стандартный цикл управления. При внедрении информационных технологий на предприятиях важно учитывать управление ИТ-деятельностью, используя модель жизненного цикла ИТ-сервиса, проектные и процессные подходы, а также обеспечивать информационную безопасность и контроль рисков.

Для объяснения процессов управления рисками в организации используется та же модель, что и в других стандартах систем управления [1].

На любом этапе развития организации могут возникать различные риски, включая информационные. Для их снижения или предотвращения рекомендуется проводить регулярный анализ и оценку, на основе которых можно разработать защитные меры.

Управление рисками в информационной области включает в себя ряд действий, направленных на выявление, анализ и устранение недостатков в системах информационной безопасности, связанных с созданием, эксплуатацией и удалением информационных комплексов. Это означает, что информационные риски представляют потенциальную угрозу возникновения убытков и ущерба из-за использования информационных технологий в организации [2].

На этапе планирования определяются правила, контекст и методы управления рисками, происходит инвентаризация (идентификация) активов и определение их стоимости, формулируются характеристики угроз и уязвимостей, происходит оценка эффективности мер по защите, а также осуществляется обработка рисков. Руководство организации принимает соответствующие решения и утверждает план по обработке рисков.

Согласно стандарту ISO 27001, оценка рисков информационной безопасности необходима для понимания требований информационной безопасности и рисков, связанных с бизнес-активами организации [2]. Она включает в себя следующие мероприятия:

– идентификация активов;

– идентификация требований законодательства и бизнеса, применимых к идентифицированным активам;

– оценивание активов с учетом идентифицированных требований законодательства и бизнеса, а также последствий нарушения конфиденциальности, целостности и доступности;

– идентификация значимых угроз и уяз-

вимостей для активов;

– оценка вероятности возникновения угроз и величины уязвимостей;

– вычисление рисков;

– оценивание рисков по заранее определенной шкале риска.

На следующем этапе управления рисками требуется определить наиболее подходящие способы обработки каждого выявленного риска. Для этого могут быть использованы такие механизмы контроля, как предотвращение и обнаружение, тактика избегания, страхование и принятие (сохранение) риска. После оценки рисков необходимо принять соответствующие бизнес-решения. В любом случае эти решения должны быть экономически обоснованы и ясны для руководства и собственников компании, которые могут поддержать или оспорить принятые решения [3].

Как уже отмечалось, наиболее рискованными этапами процесса являются проектирование и ввод в эксплуатацию. Это фазы, когда могут возникать недоработки в проектировании, инфраструктурные сбои, отказ оборудования, человеческие ошибки из-за недостаточной квалификации персонала и другие причины.

На каждом этапе управления рисками присутствует механизм обеспечения непрерывности, который тесно связан с управлением рисками. Поставщик услуг должен обеспечивать работоспособность своих услуг даже в случае серьезных сбоев, для этого могут использоваться методы устойчивости к отказам и восстановление активов.

Непредвиденные катастрофы могут произойти в любой момент, и в таких случаях важным средством защиты является страхование. Организация получает гарантию того, что будут доступны средства на восстановление после разрушений. Размер страхового взноса зависит от стоимости услуг, вероятности разрушений и стоимости восстановления потерь.

Процесс управления рисками информационной безопасности включает определение контекста, оценку и обработку рисков, принятие решений, коммуникацию, а также мониторинг и пересмотр рисков.

Процесс оценки и/или обработки рисков может иметь циклический характер. Это позволяет сделать оценку более глубокой и детальной с каждым циклом. Однако необходимо найти баланс между временем и усилиями, затрачиваемыми на определение механизмов контроля, и обеспечением правильной оценки высоких рисков.

Сначала определяется контекст, после чего проводится оценка рисков. Если получено достаточно информации для эффективного определения необходимых мер по снижению рисков до приемлемого уровня, можно переходить к обработке рисков. В случае недостаточной информации проводится дополнительный цикл оценки рисков в пересмотренном контексте.

Руководство организации должно открыто принимать риски, особенно в случаях, когда необходимое контрольное оборудование не установлено из-за высоких затрат. В процессе управления рисками информационной безопасности необходимо информировать руководителей и сотрудников о рисках и их управлении. Даже перед началом управления рисками, информация о них может быть полезна для минимизации потенциального ущерба и управления инцидентами.

Для эффективного регулирования непредвиденных событий необходимо иметь информированных менеджеров и сотрудников, которые знакомы с возможными рисками и существующими механизмами контроля. Важно также документировать результаты всех шагов в управлении рисками информационной безопасности и места, где принимаются решения [4].

На этапе реализации необходимо внедрить меры безопасности и осуществить действия по обработке рисков, включая заключение страховых договоров, соглашений о качестве услуг и внесение изменений в бизнес-план.

После определения методов обработки рисков и внедрения механизмов контроля начинается управление рисками, включающее мониторинг рисков и эффективности системы управления информационной безопасностью, а также проведение аудитов и процедур контроля [5; 6].

На этапе выполнения улучшаются процессы управления рисками через анализ результатов, пересмотр определенных рисков и

методов их оценки [7].

Дальше цикл управления рисками начинается заново, проходя последовательно стадии планирования, реализации, мониторинга и совершенствования. Эти процессы функционируют параллельно и непрерывно, обеспечивая взаимодействие между ними.

После начала реализации плана обработки рисков необходимо осуществлять непрерывную деятельность по управлению рисками, которая включает в себя следующие процессы:

– сопровождение и мониторинг;
– анализ со стороны руководства;
– пересмотр и переоценка рисков;
– аудит;
– управление документами;
– корректирующие и превентивные меры;
– коммуникация рисков.

Большинство методов безопасности нуждаются в постоянном следовании и управлении на протяжении всего срока их существования. Разработанные механизмы проверки регулярно просматриваются и анализируются с целью гарантии их эффективной работы и предотвращения их обесценивания в результате изменений окружающей среды. Обычно любой сервис или механизм со временем становится менее эффективным. Мониторинг необходим для выявления этих проблем и принятия соответствующих мер.

Действия по мониторингу и сопровождению должны планироваться и выполняться на регулярной основе согласно расписанию. Таким образом могут быть минимизированы накладные расходы и сохранена эффективность механизмов безопасности [7].

Действия по сопровождению и мониторингу механизмов безопасности включают проверку журналов и отчетов, модификацию параметров контроля, анализ эффективности и обновление политик и процедур. Основная цель – обеспечить корректное и эффективное функционирование. Руководство должно регулярно анализировать систему управления информационной безопасностью (СУИБ) для обеспечения соответствия, адекватности и эффективности [8]. Анализ включает в себя изменение ситуации с рисками, переопределение области действия СУИБ, настройку системы в соответствии с целями и метриками, и определение потребностей в ресурсах. Анализ проводится на основе информации от пользователей СУИБ, результатов аудиторских отчетов, внутренних и внешних проверок, с целью выявления изменений и возможных улучшений.

Регулярная переоценка рисков необходима для учета возможных изменений, таких как появление новых бизнес-функций или угроз, изменение окружающей среды и обновление механизмов безопасности. После учета всех изменений и определения необходимых корректировок в решениях по обработке рисков, эти изменения должны быть задокументированы, согласованы с руководством и внедрены. Результаты переоценки рисков и новые решения должны быть отражены в реестре информационных рисков и плане их обработки. Рекомендуется устанавливать график проведения регулярных внутренних аудитов, которые включают идентификацию активов, угроз и уязвимостей, оценку уровня защиты и выработку рекомендаций по усилению защиты и устранению уязвимостей.

Для проведения аудита необходимы требования и критерии, выработанные в ходе оценки рисков. Для оценки рисков необходимо проведение мероприятий по аудиту. Это два параллельных процесса, обменивающихся информацией между собой. Один не может существовать без другого. Поэтому во многих случаях аудит включает в себя оценку и обработку рисков, а оценка рисков предполагает проведение аудита. Если же аудит не включает в себя оценку рисков, тогда речь идет либо об оценке соответствия конкретным нормативным документам, либо об узкой области аудита, когда, например, требуется оценить защищенность конкретной системы или приложения в отношении внешних угроз.

Для эксплуатации и сопровождения СУИБ необходима полная, доступная и корректная документация, а также контролируемый процесс управления документами; область действия и уровень детализации для разных организаций может варьироваться. Ответственность за осуществление надзора над процессом управления документацией должна быть четко определена и согласована [9].

Требования к управлению документами и записями содержатся в ISO 27001. Эти тре-

бования полностью соответствуют требованиям, предъявляемым к документации другими стандартами систем управления, такими как ISO 9001. Они помогают комбинировать различные системы управления и согласованно применять необходимые механизмы контроля документации.

Эффективный контроль документов способствует согласованному распространению информации, устраняя неразбериху в отношении состояния СУИБ.

Документация включает в себя политики, стандарты, руководства, процедуры, списки проверки, реестр рисков и другие документы, используемые для поддержки СУИБ

По результатам мониторинга, проверок со стороны руководства или аудитов должны приниматься соответствующие корректирующие и превентивные меры. В то время как корректирующие меры направлены на устранение существующих нарушений и несоответствий требованиям безопасности, превентивные меры направлены на устранение причин этих нарушений и несоответствий.

Для эффективной коммуникации о рисках важно иметь актуальный план, определяющий ключевых участников процесса управления рисками и порядок распространения решений. План также включает механизмы обновления информации о рисках и обучения сотрудников по информационной безопасности, а также процедуры связи с общественностью при обнародовании информации о нарушениях безопасности. Страхование также может быть одним из способов защиты от рисков, при котором страховой фонд позволяет возместить ущерб, но рекомендуется использовать его вместе с другими методами снижения или устранения риска [10].

Оценка рисков должна проводиться периодически, что помогает снизить риск и улучшить работу организации.

СПИСОК ЛИТЕРАТУРЫ

1. *Киселева Т.В., Маслова Е.В.* Анализ информационных рисков // Сборник докладов Всероссийской конференции по моделированию, программному обеспечению и наукоемким технологиям в металлургии. – Новокузнецк: изд. СибГИУ, 2011. – С. 75-81.
2. *Астахов А.* Как управлять рисками информационной безопасности? – IS027000 RU, 2006. – URL:http://www.iso27000.ru/chitalnyi-zai/upravlenie-riskaniiinformacionnoi-bezopasnosti/kak-upravlyat-riskami-informacionnoibezopasnosti/ (дата обращения: 10.11.2023).
3. *Астахов А.* Особенности обеспечения информационной безопасности промышленных систем. – IS027000 RU, 2006. – URL:http://www.iso27000.ru/chitalnyi-zai/kiberugrozy-i-kiberterrorizm/osobennosti-obespecheniyainformacionnoi-bezopasnosti-promyshlennyh-sistem/ (дата обращения: 10.11.2023).
4. *Астахов А.* Анализ защищенности корпоративных автоматизированных систем. – IS027000 RU, 2002. – URL:http://iso27000.ru/chitalnyi-zai/auditinformacionnoi-bezopasnosti/analiz-zaschischennosti-korporativnyhavtomatizirovannyh-sistem/ (дата обращения: 10.11.2023).
5. *Астахов А.* История стандарта BS 7799. – IS027000 RU, 2006. – URL:http://iso27000.ru/chitalnyi-zai/standarty-informacionnoi-bezopasnosti/istoriyastandarta-bs-7799 (дата обращения: 10.06.2023).
6. Кэтрин Уолш. Хаки, фрики и черви: события, которые изменили безопасность Интернет. – IS027000 RU. – URL:http://www.iso27000.ru/chitalnyi-zai/kiberugrozy-i-kiberterrorizm/haki-friki-i-chervi-sobytiya-kotorye-izmenilibezopasnost-intemet (дата обращения: 10.11.2023).
7. ISO/IEC 27001:2005 RU Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью. – Требования. – URL:http://gtrust.ru/show good.php?idtov= 1030 (дата обращения: 10.06.2023).
8. BS ISO/IEC 27005:2008 RU Информационные технологии – Методы обеспечения безопасности – Управление рисками информационной безопасности. – URL:http://gtrust.ru/show good.php?idtov=l 137. Библиография 239 (дата обращения: 10.11.2023).
9. *Симонов С.В.* Технологии и инструментарий для управления рисками // Jet Info. – 2003. – № 2. – С. 3-6.

REVIEW OF INFORMATION RISK MANAGEMENT APPROACHES

KISELEVA Tamara Vasilievna
Doctor of Sciences in Technology, Professor
Professor of the Department of Applied Information Technologies and Programming
MASLOVA Elena Vladimirovna
Candidate of Sciences in Technology
Associate Professor of the Department of Applied Information Technologies and Programming
Siberian State Industrial University
Novokuznetsk, Russia

Various approaches to information risk management, including traditional and modern techniques, are reviewed. The main stages of information risk management, key principles and recommendations for increasing the protection of an organization's information resources are covered.
Keywords: information risks, information protection, information security, risk management.