Оригинальная статья / Original article

УДК 004
http://doi.org/10.35854/1998-1627-2025-1-72-82

Управление рисками информационной безопасности

Виталий Анатольевич Мордовец[1], Александр Александрович Графов[2], Георгий Валерьевич Варламов[3]✉

[1, 2, 3] *Санкт-Петербургский университет технологий управления и экономики, Санкт-Петербург, Россия*

[1] *mordovets@mail.ru, https://orcid.org/0000-0002-8266-5537*

[2] *grafov_aa@mail.ru, https://orcid.org/0009-0003-6916-1451*

[3] *varlamovgeorge@mail.ru✉*

Аннотация

Цель. Изучить методы управления рисками информационной безопасности в условиях цифровой трансформации компаний.

Задачи. Рассмотреть существующие подходы к модернизации информационных систем, включая метод градуальной модернизации, реинжиниринг бизнес-процессов и технологии реинжиниринга; провести анализ современных методик оценки и контроля рисков, таких как метод CRAMM, модель FRAP, методика OCTAVE и методика управления рисками корпорации Microsoft; выделить преимущества и недостатки этих методов, а также предложить рекомендации по их адаптации и интеграции в современные производственные процессы.

Методология. В процессе исследования использованы общенаучные методы (дедукция, анализ и синтез), а также методы сравнительного анализа.

Результаты. Определены основные подходы к модернизации информационных систем и выявлены их отличия, рассмотрены современные методики оценки и контроля рисков (CRAMM, модель FRAP, методика OCTAVE и методика управления рисками корпорации Microsoft), а также сформулированы преимущества и недостатки каждого из них. Кроме того, выработаны рекомендации по адаптации рассмотренных методик и их дальнейшей интеграции в современные производственные процессы.

Выводы. Развитие современных цифровых технологий имеет ряд существенных преимуществ и вместе с тем рисков, которые вынуждены учитывать компании в условиях цифровой трансформации. Грамотное управление рисками информационной безопасности позволяет компаниям минимизировать ущерб и затраты на ликвидацию негативных последствий. Изученные в ходе исследования методы дают возможность существенно повысить эффективность управления рисками информационной безопасности компаний. Важным выводом стало признание необходимости регулярного мониторинга и обновления подходов к управлению рисками в ответ на изменения в технологической среде.

Ключевые слова: *менеджмент, цифровая трансформация, управление рисками, информационная безопасность, информационные системы*

Для цитирования: Мордовец В. А., Графов А. А., Варламов Г. В. Управление рисками информационной безопасности // *Экономика и управление.* 2025. Т. 31. № 1. С. 72–82. http://doi.org/10.35854/1998-1627-2025-1-72-82

Information security risk management

Vitaly A. Mordovets[1], Aleksandr A. Grafov[2], Georgij V. Varlamov[3]✉

[1, 2, 3] *St. Petersburg University of Management Technologies and Economics, St. Petersburg, Russia*

[1] *mordovets@mail.ru, https://orcid.org/0000-0002-8266-5537*

[2] *grafov_aa@mail.ru, https://orcid.org/0009-0003-6916-1451*

[3] *varlamovgeorge@mail.ru✉*

Abstract

Aim. The work aimed to study the methods of information security risk management in the context of digital transformation of companies.

Objectives. The work discusses existing approaches to the modernization of information systems, including the gradual modernization method, business process reengineering and reengineering technologies; it analyzes current risk assessment and control methods, such as the CRAMM method, the FRAP model, the OCTAVE technique, and the Microsoft risk management method; and highlights the advantages and disadvantages of these methods, as well as proposes recommendations for their adaptation and integration into modern production processes.

Methods. The study employed general scientific methods (deduction, analysis and synthesis), as well as comparative analysis methods.

Results. The work defines the main approaches to the modernization of information systems, reveals their differences, discusses modern methods of risk assessment and control (CRAMM, FRAP model, OCTAVE method, and Microsoft risk management method), and formulates the advantages and disadvantages of each of them. In addition, recommendations are developed for the adaptation of the considered methods and their further integration into modern production processes.

Conclusions. The development of modern digital technologies has a number of significant advantages and also risks that should be taken into account by companies in the context of digital transformation. Competent information security risk management enables companies to minimize damage and costs of eliminating negative consequences. The methods investigated in the course of the study enable to increase significantly the efficiency of information security risk management of companies. An important conclusion was the recognition of the need for regular monitoring and updating of risk management approaches in response to changes in the technological environment.

Keywords: *management, digital transformation, risk management, information security, information systems*

For citation: Mordovets V.A., Grafov A.A., Varlamov G.V. Information security risk management. *Ekonomika i upravlenie = Economics and Management.* 2025;31(1):72-82. (In Russ.). http://doi.org/10.35854/1998-1627-2025-1-72-82

Введение

Стремительное развитие цифровых технологий существенно повысило значимость адекватного управления рисками информационной безопасности (далее — ИБ) компаний в условиях цифровой трансформации. В современном мире информация стала одним из важнейших факторов производства, и ее защита требует комплексного подхода. Цифровая трансформация затрагивает все аспекты деятельности компаний, от производства до управления бизнес-процессами. Однако, наряду с возможностями, которые предоставляет цифровизация, возрастают и риски, связанные с утечкой данных, кибератаками, иными угрозами.

Актуальность исследования методов управления рисками ИБ обусловлена рядом факторов, описанных в ежегодном аналитическом отчете «Оценка ущерба от утечек информации и затрат на ликвидацию последствий» экспертно-аналитического центра группы компаний InfoWatch [1]. Приведем некоторые из них:

1. *Рост числа киберугроз*. Современные компании сталкиваются с возрастающим количеством сложных и изощренных кибератак, в том числе целевых атак (так называемых постоянных серьезных угроз или APT-атак). Без эффективных мер по управлению этими рисками организации подвергаются значительным финансовым и репутационным потерям. Результаты исследования

Таблица 1

Данные, украденные при последней утечке, согласно отчету

Table 1. Data stolen in the latest leakage, according to the report

№ п/п	Какие данные были украдены	Значение, %
1	Персональные данные	50
2	Платежная информация	30
3	Коммерческая тайна или иная конфиденциальная информация	27
4	Банковская тайна (кроме платежной информации)	23
5	Сведения о системе безопасности компании	17
6	Ноу-хау / секреты производства	10
7	Данные криптокошельков	2
8	Другое	3

Источник: составлено авторами на основе [2].

о потере чувствительных для компаний данных представлены в таблице 1.

По полученным количественным оценкам от организаций, столкнувшихся с утечкой информации, самыми дорогими категориями являются последствия кражи денег в криптовалюте, в том числе за счет кражи аутентификационной информации и/или носителей (до 400 тыс. руб.), увеличение страховых взносов (до 3 246 770 руб.), добровольные выплаты пострадавшим (до 700 тыс. руб.), судебные штрафы (до 5 370 000 руб.), сорванные сделки (до 5 млн руб.), проведение аудита ИБ и оценка рисков (до 5 млн руб.), выполнение компьютерно-технической экспертизы (до 3 400 000 руб.), оплата расследования, проведенного экспертными организациями (до 1 700 000 руб.), обучение персонала после утечки информации (до 5 млн руб.) [2].

Это целесообразно учитывать в рамках реализации компаниями принципа экономической целесообразности. Согласно данному принципу, выделять средства на защиту информации следует исходя из потенциального ущерба, который может быть нанесен компании злоумышленниками ввиду отсутствия должного уровня безопасности и осмотрительности. Дополним, что чаще всего при оценке ущерба считают недополученный доход от потери клиентов, оценивают репутационные убытки и сорванные сделки.

2. *Изменение бизнес-среды*. Цифровая трансформация изменяет традиционные бизнес-модели, требуя адаптации существующих информационных систем и внедрения инновационных технологий. Это создает новые вызовы и угрозы для управления рисками, связанными с модернизацией и интеграцией информационных систем.

3. *Необходимость соответствия нормативным требованиям (комплаенс*). Законодательство в области ИБ становится все более строгим и многочисленным. Вносят поправки в действующие законы, издают новые. Несоблюдение норм может привести к штрафам и санкциям, грозит лицензиатам лишением или приостановкой действующих лицензий со стороны регуляторов, что делает управление рисками важным элементом стратегического планирования.

4. *Глобализация и межсекторальное взаимодействие*. Компании работают в глобальном масштабе, границы все более размыты. Тем самым происходит взаимодействие с партнерами, клиентами и контрагентами в мире. Это повышает сложность управления рисками и требует унифицированных подходов к защите конфиденциальной информации (коммерческой тайны, персональных данных, ноу-хау и т. д.).

Таким образом, статья имеет высокую актуальность и практическую значимость, на наш взгляд. В ней мы предлагаем практические решения для организаций, стремящихся защитить свои активы в условиях быстро изменяющегося цифрового мира. Это предопределило цель, задачи и методы настоящего исследования.

Результаты и их обсуждение

Для успешного запуска цифровой трансформации нужен аудит IT-решений, которые сегодня встроены в производственный процесс. Аудит необходим для того, чтобы эффективнее управлять рисками цифровой трансформации. На практике применяют метод градуальной модернизации информационных систем, как показано на рисунке 1.

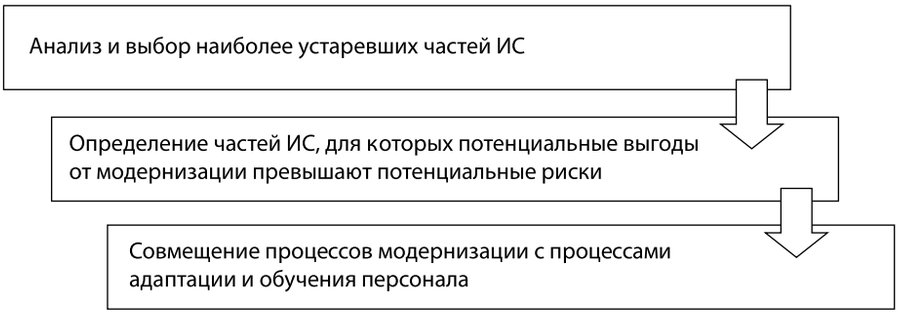

Рис. 1. Метод градуальной модернизации информационных систем (ИС)
Fig. 1. The method of gradual modernization of information systems (IS)

Источник: составлено авторами.

В его основе находится разделение процесса модернизации на ряд этапов. На каждом этапе обновляется тот или иной компонент информационных систем. Сведено к минимуму сопротивление у сотрудников новшеству, снижается социальная инерция и сокращается вероятность наступления технологических рисков.

Базисом рассматриваемого метода выступает процесс идентификации устаревших частей информационной системы, а затем выявления потенциальных рисков, которые могут возникнуть при их модернизации. После этого следует выбор тех, у которых риск минимален. Особенностью метода выступает совмещение двух процессов, в частности модернизации и одновременно с ней обучения сотрудников, чтобы снять проблему сопротивления новшествам.

В основе модернизации информационных систем должны находиться технологии реинжиниринга, и его необходимо четко распланировать. Только в таком случае можно ориентироваться на успех. Данная технология направлена на решение проблем, связанных с модернизацией применяемых ИС, которые требуют апгрейда, но при этом обеспечивают высокий уровень эффективности оцифрованных бизнес-процессов предприятия. Процесс реинжиниринга можно разделить на ряд этапов. Первый этап ориентирован на реализацию мониторинга действующей информационной системы, затем внимание разработчиков концентрируется на архитектуре. В центре внимания — обновленный функционал, который должна впоследствии выполнять информационная система, и исходя из этого выстраивают ее новую модель и структуру. Финишным этапом служат изменение действующих информационных компонентов и разработка новых [3]. Ключевыми преимуществами данного подхода выступают постепенный характер вносимых в информационные системы коррективов, а следовательно, снижение рисков, уменьшение расходов по сравнению с вариантом создания новой системы [4].

Метод CRAMM (CCTA Risk Analysis & Management Method — метод CCTA анализа и контроля рисков) позволяет сочетать не только количественные, но и качественные методы анализа. Его разработчики своей целью ставили создать действенный инструментарий, в основе которого находятся формализованные процедуры. Такие процедуры предоставляют возможность оценить, во-первых, все ключевые предписания относительно безопасности, проанализировать и запротоколировать их; во-вторых, минимизировать расходы, возникающие при отсутствии объективного подхода к данному вопросу; в-третьих, оптимизировать процесс планирования и запустить защитные механизмы на всех этапах разработки информационных систем; в-четвертых, снизить временные затраты; в-пятых, оптимизировать процесс в отношении требований безопасности за счет его автоматизации; в-шестых, иметь возможность проводить сравнительный анализ применяемых контрмер и выбирать наиболее эффективные; в-седьмых, в автоматическом режиме создавать отчеты.

Анализ рисков заключается в их идентификации и присвоении каждому из них определенного уровня в результате их оценки с точки зрения уязвимости ресурсов. Контроль рисков сводится не только к выбору контрмер, но и оценки их с точки зрения оптимальности, что в итоге приводит к их минимизации. Рассмотрим стадии

Таблица 2

Недостатки и достоинства CRAMM

Table 2. Disadvantages and advantages of CRAMM

Недостатки	Достоинства
1. Значительное количество сгенерированных отчетов. 2. Высокий уровень трудоемкости при применении метода	1. Активно применяемый метод. 2. Систематизированная база данных, в которой зафиксированы и набор контрмер, и оценки рисков. 3. Метод может быть использован как инструмент аудита

Источник: составлено авторами.

диагностики безопасности информационных систем в рамках применения метода CRAMM.

Первая стадия связана с регламентацией тестируемой информационной системы. На этой стадии — ее функционал, пользовательский срез, границы и персонал, который осуществляет обследование. Применяется десятибалльная шкала. Среди показателей, которые оценивают, отражены и количественные, и качественные. Например, финансовые потери — это количественный показатель, а потери репутации — качественный и т. д. Помимо указанных показателей, метод CRAMM рекомендует применять разного вида ущербы (для здоровья персонала, от разглашения коммерческой тайны и др.). Кроме того, оценивают финансовые потери, ориентированные и на возвращение ресурсов, и на дезорганизацию функционирования, а также ряд иных [5].

Вторая стадия напрямую нацелена на выявление «прорех» в безопасности информационных систем. Схема работы метода CRAMM сводится к тому, что посредством программного обеспечения формируется для 36 типов угроз и для всех групп ресурсов список вопросов. Ответы на них ранжированы. Ранг угроз варьируется от очень высокого до очень низкого, а ранг уязвимости имеет три значения: низкий, средний и высокий. Применяя семибалльную градацию (от 0 до 7), сформированный массив информации можно преобразовать в оценку ранга риска. Тем самым CRAMM формирует матрицу риска, в которой учтены показатели и уязвимостей, и угроз. Итогом становится оценка возможных потерь информационной системы по результатам работы за год. За основу взята следующая формула:

$$Р_{риск} = Р_{реализация} \times Ущерб. \quad (1)$$

Вероятность наступления рисковой ситуации ($Р_{риск}$) в данном случае напрямую зависит от ущерба и вероятности реализации. В свою очередь, вероятность реализации может быть определена по формуле:

$$Р_{реализации} = Р_{угрозы} \times Р_{уязвимости}, \quad (2)$$

где угроза — это какой-либо фактор, который может негативно отразиться на рассматриваемом процессе и привести к ущербу безопасности; уязвимость представляет собой неспособность в полной мере осуществить защиту ресурса либо группы ресурсов, и в результате может быть реализована угроза.

На третьей стадии происходит отыскание соответствующих контрмер. Фактически речь идет о выявлении востребованного варианта для нужд заказчика системы безопасности. CRAMM на данном этапе инициирует спектр вариантов контрмер, которые максимально противостоят соответствующим рискам. CRAMM способен переводить качественные показатели в количественный формат, применяя соответствующий математический аппарат при подсчете баллов. В таблице 2 систематизированы недостатки метода и его достоинства.

Как показывает опыт, применение метода приводит к высоким результатам. Прежде всего появляется возможность оценить расходы предприятия на сохранение безопасности информационной системы с учетом обеспечения целостности бизнес-процессов. Применение CRAMM снижает риск возникновения необоснованных расходов и тем самым приводит к экономии средств. На рисунке 2 представлен ранее описанный механизм функционирования метода CRAMM, в основе которого, как указано выше, находится комплексный подход по выявлению рисков, способный комбинировать методы анализа, создавая матрицу рисков, и выдавать варианты контрмер.

Основой разработки метода выступил стандарт ISO 27000, ориентированный на обеспечение управления ИБ. Особенность

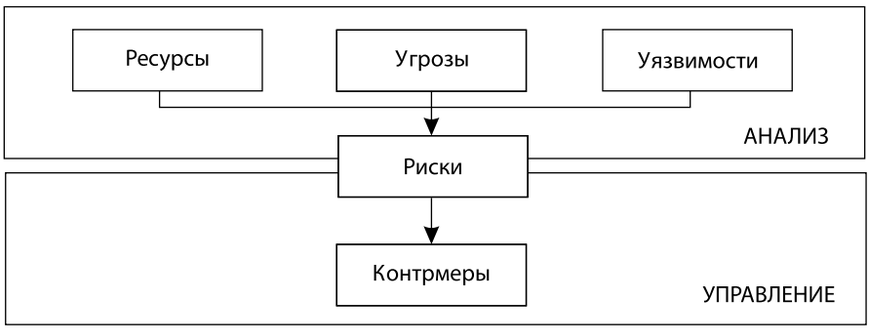

Рис. 2. Структурная схема метода CRAMM
Fig. 2. Structural diagram of the CRAMM method

Источник: составлено авторами.

метода заключается в его универсальности. Он подходит как для малого бизнеса, так и для крупных компаний.

Модель Facilitated Risk Analysis Process (FRAP) ориентирована на качественную оценку рисков. Основой ее служат механизмы управления рисками. Она предполагает детальное изучение информационной системы с помощью автоматизированных инструментов и тщательную идентификацию угроз с формированием подробного списка. Сформированный список выступает фундаментом, на базе которого осуществляется процесс принятия решений относительно обеспечения безопасности информационной системы. Особенность FRAP состоит в том, что основой оценки служит обусловленность затрат и приобретаемого эффекта. Ее роль сводится к выявлению необходимых средств защиты, ориентированных на доведение уровня риска до допустимых значений.

В модели принято допущение относительно того, что изначально информационная система не обладает механизмами и средствами защиты. Тем самым происходит оценка ее уровня риска, что в дальнейшем приводит к идентификации эффекта от ее применения. В качестве ключевой цели разработчики определили оценку и фиксацию состава рисков, которые могут быть связаны с обеспечением ИБ бизнес-процессов, информационных систем либо иной части информационного обеспечения предприятия.

Метод Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), разработанный Университетом Карнеги-Мелон в 2007 г., описывает подход к качественной оценке рисков. Метод OCTAVE базируется на своевременном мониторинге угроз, обладающих критичным характером, а также активов и уязвимостей. Метод строится на создании группы сотрудников, которые анализируют риски ИБ. В ее состав входят работники предприятия, осуществляющие эксплуатацию информационной системы, а также работающие в IT-отделе.

Среди недостатков метода на первое место ставят то обстоятельство, что реализуемый анализ риска не интегрирован в систему управления ИБ компании. Далее следует то, что возникают проблемы, связанные с мониторингом рисков, осуществлением их повторных оценок. Это исключает возможность управлять остаточными рисками, а также устранять из рассмотрения их. Анализ рисков в рамках исследуемого метода включает в себя восьмишаговую последовательность, как видно на рисунке 3.

При оценке рисков следует отработать восемь шагов. В частности, шаг 1 предназначен для того, чтобы сформировать систему критериального оценивания рисков ИБ. Речь идет о структуре качественных показателей, задачей которой выступает установление соответствия между оценкой риска и его реализацией. Оценить риск без сформированной системы его критериального оценивания не представляется возможным. Поэтому этот шаг крайне значим.

На шаге 2 не только формируется перечень информационных активов, но и каждому присваивают соответствующий профиль, содержащий информацию об особенностях актива и качествах, которыми он обладает, а также о стоимостной характеристике. Инструментарий по присвоению профилей предназначен для очерчивания границ актива и определения его уровня безопасности. Тем самым на данном шаге каждый актив получает свой профиль, который может

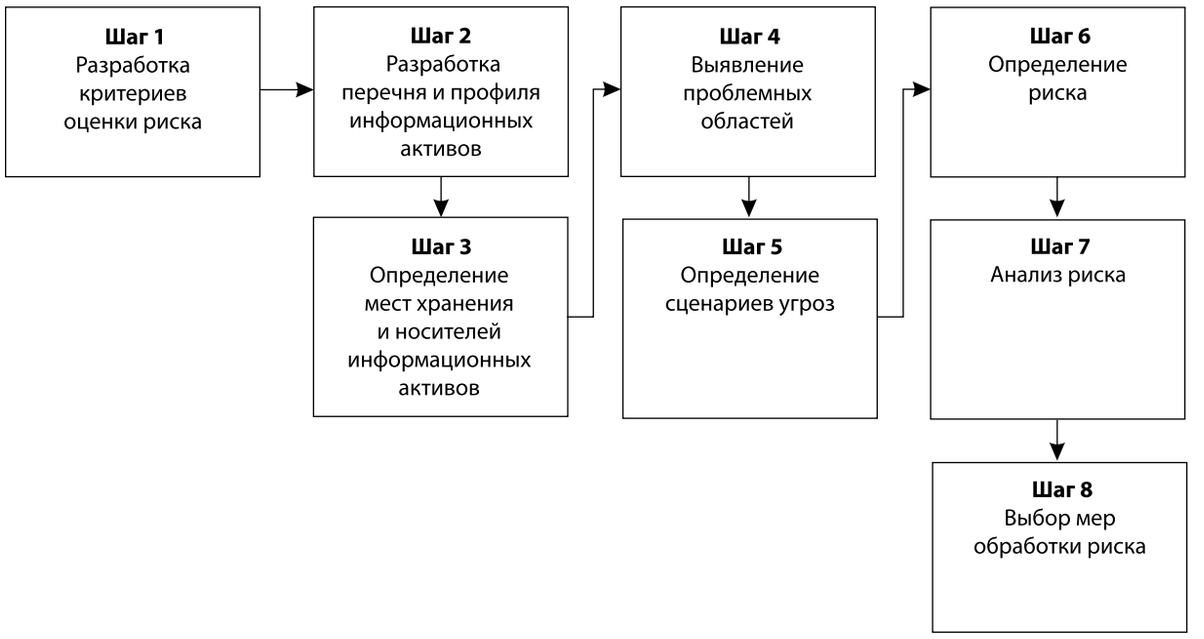

Рис. 3. Этапы анализа рисков по методике OCTAVE
Fig. 3. Stages of risk analysis using the OCTAVE technique

Источник: составлено авторами.

быть представлен в виде входных данных, дальнейших шагов. С его помощью можно будет оценивать риски и диагностировать угрозы.

Шаг 3 предназначен для того, чтобы прояснить ситуацию, связанную с местом хранения актива, способами его передачи и обработки. Это обусловлено тем, что часть активов может быть размещена вне предприятия. На этом шаге формируется карта актива. Ее основным наполнением служит конкретизация мест их хранения и обработки. Место хранения обладает разнообразной направленностью: в качестве него могут выступать сотрудник компании, печатный источник, программное обеспечение. Особое внимание в рамках алгоритма отведено сотрудникам, поскольку они приобретают статус «контейнера» актива при условии поступления им защищаемой информации. Такого рода риски требуют пристального внимания к себе и их следует оперативно выявлять.

Шаг 4 ориентирован на поиск и идентификацию проблемных сфер ИБ компании. В рамках этого шага аналитики выявляют угрозы.

Шаг 5 выступает продолжением предыдущего шага. Полученная на данном этапе информация о проблемных сферах преобразуется в сценарии угроз. При этом угрозы структурированы в виде дерева, а его ветви выявляют угрозы, которые возможны в конкретном информационном активе. Механизм реализации определен для каждой ветви в виде опросных листов, в которых отражены сценарии угроз. Кроме того, рассматриваемый шаг дает возможность учитывать вероятность наступления угроз, что ведет к минимизации риска на последующих шагах. Чтобы оптимизировать данный процесс, вводят уровни вероятности наступления негативной ситуации в виде низкого, среднего и высокого.

На шаге 6 выявляют риски ИБ, то есть происходит оценивание того, каким образом тот или иной риск может оказывать влияние на компанию или актив. Особенность шага прослеживается в том, что риск выявляется для каждого актива. Это сделано для того, чтобы своевременно определять его уровень приоритетности и для актива, и для компании. Формируется взаимосвязь, в которой каждому риску соответствует как минимум одно последствие.

Шаг 7 предназначен для того, чтобы измерить величину ущерба, который может возникнуть при неблагоприятных условиях проявления той или иной угрозы. На данном шаге все риски ранжируются. Например, если на деятельность компании влияет ее реноме, то этому виду риска будет присвоен

максимальный ранг, и все усилия будут направлены на минимизацию воздействия такого риска.

Шаг 8 предназначен для выбора уровня обработки выявленных рисков с учетом проведенного на предыдущем шаге ранжирования.

Методика управления рисками ИБ корпорации Microsoft предложена в 2006 г. Она нашла отражение в соответствующем корпоративном руководстве, ориентированном на управление рисками [2]. Методика в своей основе базируется на таком же принципе, что и методика CRAMM, объединяя качественный и количественный подходы. Качественный подход предназначен для эффективного структурирования рисков ИБ, а количественный — нацелен на углубленное исследование особенно существенных рисков. Это позволяет выявить комплект ключевых рисков, которые потребуют пристального внимания при изучении и концентрации усилий для их недопущения.

Microsoft ответственно относится к выстроенной в компании системе управления рисками. В этой связи мониторинг рисков структурирован в несколько этапов. На первом этапе осуществляется выработка планабазиса для успешной оценки рисков. Затем следует этап синхронизированного сбора информации относительно рисков и ее обсуждения. Завершающий этап ориентирован на иерархизацию рисков за счет присвоения рангов обнаруженным рискам. Процесс оценки базируется на сборе информации в отношении прежде всего активов компании, потенциальных уязвимостей и угроз безопасности, а также существующей системы контроля. Собранная информация выступает ключевым элементом в управлении безопасностью. Все активы обладают разным уровнем влияния на бизнес и распределяются от высокого до низкого, включая срединное значение.

Каждому виду угроз соответствует тот или иной уровень воздействия, создавая тем самым несколько уровней защиты. К ним отнесены защита на физическом уровне, на уровнях сетей, приложений и данных. Оценка рисков представляет собой очередной шаг, на котором формируется список рисков. Эти риски упорядочены по критериям их значимости. В первой итерации выстраивается обобщенный список, а затем вычленяются значимые риски, и происходит их детализация. При формировании списка учитывают такие факторы, как частоту проявления и степень влияния риска.

Процесс детализации рисков — завершающая задача при их оценке. Каждому оцениваемому риску присваивают денежный эквивалент. Затем риску присваивают соответствующий уровень его предрасположенности к воздействию, выраженный в процентах, что характеризует объем ущерба актива и величину влияния. Размер ущерба от предрасположенности к воздействию в Microsoft оценивают по линейной шкале, в диапазоне от 20 до 100 %. Представленный диапазон может быть изменен. Величина влияния приобретает соответственный качественный статус: высокий, средний и низкий.

Итоговое значение вероятности формируется в результате суммирования двух показателей. Один из них характеризует вероятность наличия уязвимости в окружении, другой оценивает такую же уязвимость, но не в окружении, а с точки зрения эффективности ее контроля. Диапазон значения расположен в интервале от 1 до 5. Оценочное суждение формируется посредством ответов на вопросы. Уровень риска вычисляют в соответствии с формулой:

$$\text{Уровень риска} = \text{Оценка уровня влияния} \times \text{Уровень вероятности}. \quad (3)$$

Оба показателя в представленной формуле имеют диапазон от 0 до 10. В итоге уровень риска может колебаться в интервале от 0 до 100.

На заключительном этапе осуществляется количественный анализ оценки рисков. Для того, чтобы это сделать, выполняют оценку активов с точки зрения их воздействия на бизнес. Иными словами, происходит аудит конкретного актива, и для него устанавливают денежную оценку, базирующуюся на его ценности для компании, учитывая и материальную, и нематериальную составляющие. Уровень вреда, которому может быть подвержен актив, устанавливается на базе значения предрасположенности к воздействию. Заключительный шаг выражен количественной оценкой воздействия риска. Ее получают в виде произведения предрасположенности к воздействию на стоимость актива.

Проведенный анализ разнообразных моделей, ориентированных на процесс управления рисками, показал, что единообразного подхода не существует. Фактически

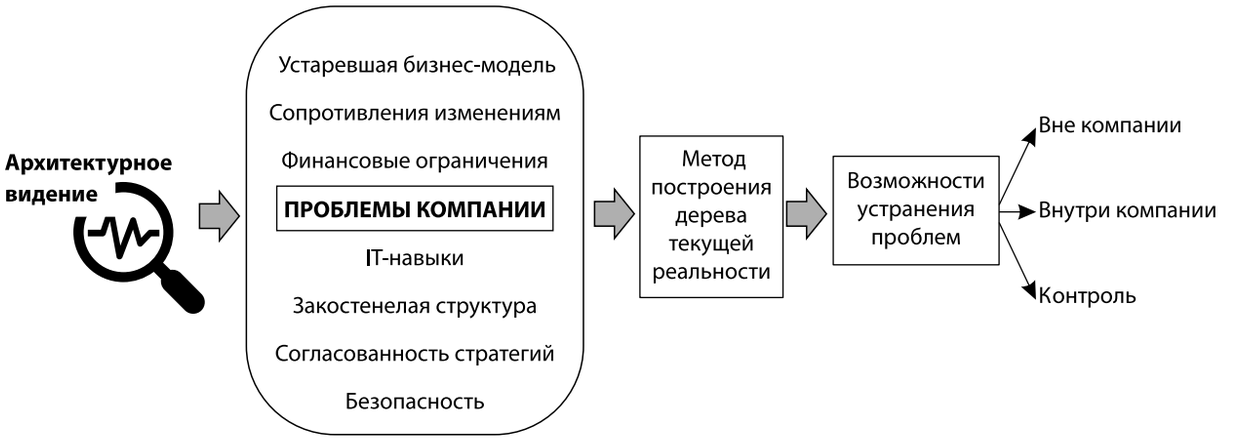

Рис. 4. Диагностика проблем цифровой трансформации организации
Fig. 4. Diagnostics of problems of the organization digital transformation

Источник: составлено авторами.

каждая компания вынуждена заниматься решением вопросов минимизации рисков самостоятельно. В основе функционирования рассмотренных моделей находится понимание того, что внешняя среда организации скрывает в себе множество негативных факторов, которые необходимо учитывать и пытаться нейтрализовать. Анализ также выявил, что все модели имеют те или иные недостатки. Условия цифровой трансформации требуют корректировки существующих моделей уровня риска, так как в обязательном порядке должна быть учтена цифровая составляющая в рамках трансформационных производственных процессов.

Ряд ученых придерживаются мнения о том, что цифровая трансформация способствует нивелированию корпоративных рисков посредством существенного роста гибкости компаний с одной стороны и возможности привлечь финансовые ресурсы — с другой. Эти два фактора существенно влияют на политику управления рисками, которую проводит компания [6]. В результате, чтобы конкретизировать данный процесс, необходимо детальнее оценивать внешнюю среду компании и выявлять факторы, которые могут стать в действительности проблемой и негативно влиять на компанию. Схема диагностики проблем цифровой трансформации компании приведена на рисунке 4.

Внедрение цифровых технологий будет проходить четко и без сложностей для компании только в случае, если руководство своевременно и правильно осознает проблемы, с которыми она столкнется на пути цифровой трансформации [7; 8]. Для разрешения потенциальных сложностей создают дорожную карту цифровой трансформации. В этом программном документе отражены ключевые проблемы, требующие разрешения.

Выводы

В процессе исследования изучены различные методы управления рисками ИБ в условиях цифровой трансформации. Установлено, что ни один из них не является универсальным, и каждая организация должна разрабатывать собственные стратегии управления рисками, учитывая специфику своей деятельности, особенности бизнес-процессов, внешнего окружения и факторов. Очевидным стало признание необходимости регулярного мониторинга и обновления подходов к управлению рисками в ответ на изменения в технологической среде.

Предлагаем ряд рекомендаций компаниям:

1. Проведение регулярного аудита IT-решений и процессов для выявления устаревших и уязвимых компонентов (например, ввиду отсутствия строгой политики периодических обновлений имеющихся компонентов), что поможет предотвратить возможные инциденты и минимизировать угрозы.

2. Проведение градуальной модернизации для постепенного обновления информационных систем, что позволит снизить сопротивление сотрудников (так называемая команда перемен) и социальные риски.

3. Планирование и реинжиниринг бизнес-процессов для повышения эффективности

и результативности информационных систем. Четкое планирование и поэтапное выполнение реинжиниринговых мероприятий поможет избежать ошибок и лишних затрат.

4. Внедрение методов CRAMM, FRAP, OCTAVE и Microsoft для комплексного анализа и контроля рисков. Это даст возможность сочетать количественные и качественные методы анализа как мощного инструмента оценки и минимизации рисков.

5. Обеспечение постоянного мониторинга внешних и внутренних угроз, а также регулярное обучение сотрудников основам ИБ для поддержания высокого уровня защиты (тренинги, деловые игры, мастер-классы).

6. Ведение подробной документации по всем предпринятым мерам и достигнутым результатам, что поможет отслеживать прогресс и принимать обоснованные решения в будущем (цикл Деминга).

Список источников

1. Сколько стоят утечки информации: аналитический отчет // Infowatch. 2025. 16 января. URL: https://www.infowatch.ru/analytics/analitika/skolko-stoyat-utechki-informatsii-analiticheskiy-otchet (дата обращения: 25.01.2025).
2. *Бычков А. К., Моисеенко А. С.* Методы оценки рисков в работе ИТ-подразделений // Молодой исследователь: вызовы и перспективы: сб. ст. по материалам CCCLVIII Междунар. науч.-практ. конф. (Москва, 20 мая 2024 г.). № 20. М.: Интернаука, 2024. С. 741–758.
3. *Щенников С. Ю.* Реинжиниринг бизнес-процессов. Экспертное моделирование, управление, планирование и оценка. М.: Ось-89, 2004. 288 с.
4. *Соколов Б. В., Зайчик Е. М., Иконникова А. В., Потрясаев С. А.* Комплексное планирование модернизации информационных систем: методологические и методические основы // Труды СПИИРАН. 2006. Т. 1. № 3. С. 265–278.
5. *Чернышева Т. Ю., Удалая Т. В.* Оценка риска проекта информатизации на основе продукционных правил // Научное обозрение. 2013. № 5. С. 169–172.
6. *Tian G., Li B., Cheng Y.* Does digital transformation matter for corporate risk-taking? // Finance Research Letters. 2022. Vol. 49. Article No. 103107. DOI: 10.1016/j.frl.2022.103107
7. *Идигова Л. М., Бишаев С. С.* Стратегические подходы в условиях цифровой трансформации менеджмента в современных компаниях // ФГУ Science. 2020. № 1. С. 97–103.
8. *Кузина Г. П., Мозговой А. И., Крылов А. Н.* Организация цифровой трансформации российских предприятий // Вестник МГПУ. Серия: Экономика. 2020. № 4. С. 69–82. DOI: 10.25688/2312-6647.2020.26.4.07

References

1. How much do information leaks cost: Analytical report. Infowatch. Jan. 16, 2025. URL: https://www.infowatch.ru/analytics/analitika/skolko-stoyat-utechki-informatsii-analiticheskiy-otchet (accessed on 25.01.2025). (In Russ.).
2. Bychkov A.K., Moiseenko A.S. Methods of risk assessment in the work of IT departments. In: Young researcher: Challenges and prospects. Proc. 368th Int. sci.-pract. conf. (Moscow, May 20, 2024). Moscow: Internauka; 2024:741-758. (In Russ.).
3. Shchennikov S.Yu. Business process reengineering. Expert modeling, management, planning and evaluation. Moscow: Os'-89; 2004. 288 p. (In Russ.).
4. Sokolov B.V., Zaychik E.M., Ikonnikova A.V., Potryasaev S.A. Comprehensive planning for modernization of information systems: Methodological and technical bases. *Trudy SPIIRAN = SPIIRAS Proceedings.* 2006;1(3):265-278. (In Russ.).
5. Chernysheva T.Yu., Udalaya T.V. Assessing the risk of informatization project based on production rules. *Nauchnoe obozrenie*. 2013;(5):169-172. (In Russ.).
6. Tian G., Li B., Cheng Y. Does digital transformation matter for corporate risk-taking? *Finance Research Letters*. 2022;49:103107. DOI: 10.1016/j.frl.2022.103107
7. Idigova L.M., Bishaev S.S. Strategic approaches in the conditions of digital transformation of management in modern companies. *FGU Science*. 2020;(1):97-103. (In Russ.).
8. Kuzina G.P., Mozgovoy A.I., Krylov A.N. Organization of digital transformation of Russian enterprises. *Vestnik MGPU. Seriya: Ekonomika = MCU Journal of Economic Studies.* 2020;(4):69-82. (In Russ.). DOI: 10.25688/2312-6647.2020.26.4.07

Сведения об авторах

Виталий Анатольевич Мордовец

кандидат экономических наук, доцент, заведующий кафедрой управления социально-экономическими системами

Санкт-Петербургский университет технологий управления и экономики

190020, Санкт-Петербург, Лермонтовский пр., д. 44а

Scopus Author ID: 57203782974

ResearcherID: AFC-7651-2022

AuthorID (РИНЦ): 851126

SPIN-код: 8553-8510

Александр Александрович Графов

кандидат экономических наук, доцент, заведующий кафедрой информационных технологий и математики

Санкт-Петербургский университет технологий управления и экономики

190020, Санкт-Петербург, Лермонтовский пр., д. 44а

Георгий Валерьевич Варламов

кандидат экономических наук, доцент кафедры международных финансов и бухгалтерского учета, начальник управления внешних коммуникаций

Санкт-Петербургский университет технологий управления и экономики

190020, Санкт-Петербург, Лермонтовский пр., д. 44а

Поступила в редакцию 27.01.2025
Прошла рецензирование 12.02.2025
Подписана в печать 21.02.2025

Information about the authors

Vitaly A. Mordovets

PhD in Economics, Associate Professor, Head of the Department of Socio-Economic Chain Management

St. Petersburg University of Management Technologies and Economics

44A Lermontovskiy Ave., St. Petersburg 190020, Russia

Scopus Author ID: 57203782974

ResearcherID: AFC-7651-2022

AuthorID (RSCI): 851126

SPIN: 8553-8510

Aleksandr A. Grafov

PhD in Economics, Associate Professor, Head of the Department of Information Technologies and Mathematics

St. Petersburg University of Management Technologies and Economics

44A Lermontovskiy Ave., St. Petersburg 190020, Russia

Georgij V. Varlamov

PhD in Economics, Associate Professor at the Department of International Finance and Accounting, Head of External Communications Department

St. Petersburg University of Management Technologies and Economics

44A Lermontovskiy Ave., St. Petersburg 190020, Russia

Received 27.01.2025
Revised 12.02.2025
Accepted 21.02.2025

Конфликт интересов: авторы декларируют отсутствие конфликта интересов, связанных с публикацией данной статьи.

Conflict of interest: the authors declare no conflict of interest related to the publication of this article.