Раздел 5. КЛАССИФИКАЦИЯ И УПРАВЛЕНИЕ РИСКАМИ

5.1 Классификатор рисков цифровой экономики

Политические риски

Макрополитические риски затрагивают все экономические субъекты данной страны без исключения и оценивается по политическим, социальным, экономическим, юридическим параметрам в каждой стране.

Макроэкономические риски делятся на:

– **Инфляционные риски** – это риски непрогнозируемого изменения темпов роста цен, при котором инвестор стремится получить доход, покрывающий инфляционное изменение цен;

– **Риски темпов экономического развития страны** связаны с цикличностью рыночной экономики, которая определяет необходимость учитывать при расчетах общее состояние экономического развития и ожидаемые темпы экономического роста на ближайшую перспективу;

– **Риски изменения величины ставки процента** связаны с движением процентной ставки, которая является реакцией на проводимые меры макроэкономического регулирования и может приводить как к стимулированию инвестиционной активности, так и сдерживать увеличение совокупных расходов в экономике;

– **Риски изменения валютного курса** – связаны с изменением валютного курса под влиянием экономических и политических факторов, который не точно отражает колебания розничных цен в стране;

– **Политические риски** – это угроза активам, вызванная политическими событиями. Факторы политического риска определяются, как правило, на основе экспертных оценок, проводимых крупными фирмами, аналитическими агентствами или государством;

– **Страновые риски** – это степень риска того, что действия суверенного правительства повлияют на способность должника, связан-

ного с данной страной, исполнить свои обязательства. Различают риски прямые и косвенные.

Микрополитические риски заключают в себе изменения, которые целенаправленно формируют угрозы лишь для определенных секторов экономики или даже отдельных предприятий. Касается только предприятий, обладающих определенными характеристиками, и его оценка производится для каждой операции в отдельности.

Микроэкономические (внутрифирменные) риски делятся на:

– **Производственные риски** связаны с отсутствием сырья и материалов, недостаточно квалифицированным управленческим и производственным персоналом, значительным числом ошибок при проектировании и планировании выполнения работ, несвоевременной поставкой материалов;

– **Финансовые риски** связаны низким уровнем управления финансовыми потоками, неквалифицированным персоналом в области финансового менеджмента, неправильным составлением смет и перерасходом средств;

– **Маркетинговые или рыночные риски** связаны с изменением потребительских настроений, усилением конкуренции, потерей позиций на рынке и несвоевременным выходом на целевой рынок;

– **Правовые риски** связаны с несоблюдением контрагентами условий и сроков контрактов и возможными судебными процессами;

– **Дефолтные риски на уровне предприятия** – связаны с банкротством предприятия или его краткосрочной неплатежеспособностью.

Риски потери собственности связаны с национализацией или экспроприацией без надлежащей компенсации.

Риски трансферта связаны с ограничением экспорта продукции или ресурсов, ограничениями относительно конвертации локальной валюты в иностранную и осуществлением расчетов по внешнеэкономическим контрактам.

Контрактные риски предполагают возможное расторжение контракта вследствие действий правительства страны, в которой находится компания-контрагент.

Риски изменения регулирующих норм связаны с возможными изменениями в законодательной базе, изменением торгового режима и таможенной политики, изменением в налоговой системе, валютном регулировании, регулировании внешнеполитической деятельности страны.

Финансовые риски

Финансовые риски – это вероятность возникновения непредвиденных финансовых потерь (снижение предусматриваемой прибыли, уменьшение ожидаемого дохода, потеря части или всего капитала) в ситуации неопределенности условий финансовой деятельности предприятия.

Финансовые риски подразделяются на:

– **Риски снижения финансовой устойчивости (или риски нарушения равновесия финансового развития) предприятия** – формируются несовершенством структуры капитала (чрезмерной долей используемых заемных средств), порождающим несбалансированность положительного и отрицательного денежных потоков предприятия по объемам.

– **Риски неплатежеспособности (или риски несбалансированной ликвидности) предприятия** обусловлены снижением уровня ликвидности оборотных активов, порождающим разбалансированность положительного и отрицательного денежных потоков предприятия во времени. По своим финансовым последствиям этот вид риска также относится к числу наиболее опасных.

– **Инвестиционные риски** характеризуют возможность возникновения финансовых потерь в процессе осуществления инвестиционной деятельности.

– **Риски снижения доходности** могут возникнуть в результате уменьшения размера процентов и дивидендов по портфельным инвестициям, вкладам и кредитам.

– **Селективные риски (от лат. selectio – выбор, отбор)** – это риски неправильного выбора способа вложения капитала, вида ценных бумаг для инвестирования в сравнении с другими видами ценных бумаг при формировании инвестиционного портфеля.

– **Инфляционные риски** – это риски того, что при росте инфляции получаемые денежные доходы обесцениваются с точки зрения реальной покупательной способности быстрее, чем растут. Этот вид риска характеризуется возможностью обесценения реальной стоимости капитала (в форме финансовых активов предприятия), а также ожидаемых доходов от осуществления финансовых операций в условиях инфляции.

– **Дефляционные риски** – это риски того, что при росте дефляции происходит падение уровня цен, ухудшение экономических условий предпринимательства и снижение доходов. И в том и в другом случае предприниматель несет реальные финансовые потери.

– **Валютные риски** – представляют собой опасность валютных потерь, связанных с изменением курса одной иностранной валюты по отношению к другой при проведении внешнеэкономических, кредитных и других валютных операций.

– **Депозитные риски (от англ. Deposit risk)** – риски возможного невозвращения полностью или частично депозитных вкладов в связи с банкротством банка или другого финансового учреждения.

– **Кредитные риски** имеют место в финансовой деятельности предприятия при предоставлении им товарного (коммерческого) или потребительского кредита покупателям, формой его проявления является риск неплатежа или несвоевременного расчета за отпущенную предприятием в кредит готовую продукцию.

– **Налоговые риски** – возможность понести финансовые и иные потери, связанные с процессом уплаты и оптимизации налогов, выраженной в денежном эквиваленте.

Цифровые риски

– **Риски быстрого устаревания техники** – переход к цифровой экономике, основанной на новых цифровых технологиях приведет к тому, что старая техника станет абсолютно не пригодной к использованию и будет отправлена на свалку.

– **Риски потери дохода –** автоматизация процессов на предприятиях и в сфере услуг может привести к росту безработицы, и далее в среде бедных конкуренция за рабочие места может стать сильнее, что приведет к стагнации зарплат, следовательно, и к риску того, что развитие цифровых технологий может усугубить социально-экономическое неравенство.

– **Риски роста потребительства (массовый консьюмеризм) –** риск, связанный с формированием через телевидение и интернет потребительского спроса. Вирусный маркетинг будет провоцировать совершать все новые и новые покупки, превращая в товар сам процесс потребления.

– **Риски свертывания массового производства –** риски, связанные со стремлением производителей к экономии на масштабах, сокращению объемов производства и свертыванию массового производства товаров широкого потребления в связи с индивидуализацией производства.

– **Риски роста безработицы и исчезновения многих профессий –** риски, связанные с высвобождением огромной массы неквалифицированных работников при цифровой революции, что приведет к росту безработицы и исчезновению многих специальностей.

– **Риски дефицита профессиональных кадров –** это вероятность возникновения дефицита профессиональных кадров при переходе к цифровой экономике.

– **Риски роста новых преступлений –** риски, связанные с возможным всплеском новых, ранее не наблюдавшихся преступлений, связанных с использованием преступных цифровых технологий в виде киберпреступлений.

Инвестиционные риски

Инвестиционные риски подразделяются по сферам применения:

Законодательно-правовые риски – риски, связанные с действующим законодательством, могут возникать в связи с несовершенством действующего законодательства, как в целом, так и в определенных его областях.

Экологические риски – риски, связанные с влиянием, которое окружающая среда может оказать на объекты инвестирования.

Подразделяются на три основных подпункта:

– **Техногенные риски** – риски, связанные с нештатными ситуациями и авариями на промышленных объектах, способными привести к существенному загрязнению окружающей среды (например, на предприятиях химической или атомной промышленности).

– **Природно-климатические риски –** риски, связанные с экстремальными погодными условиями (засухи, морозы), климатическими условиями, природными катаклизмами (землетрясения, цунами, наводнения и т.п.), отсутствием необходимых полезных ископаемых.

– **Социально-бытовые риски –** риски, связанные уровнем заболеваемости населения разного рода инфекционными заболеваниями, от которого может зависеть объект инвестирования.

Социальные риски - риски, зависящие от таких факторов, как сложившиеся традиции(нарушение которых чревато последствиями), уровня неудовлетворенности населения текущим положением (который может выливаться в забастовки и массовые беспорядки).

Политические риски – риски, связанные с влиянием текущей государственной политики на объект инвестирования: обострение в межгосударственных отношениях; уровень коррупции; смена политического курса в стране; уровень гласности и т.п.

Экономические риски – риски, включающие в себя факторы, связанные с экономической ситуацией в стране: дефолты; кризисы; различные потрясения в экономической жизни общества.

Технико-технологические риски – риски**,** связанные с технической стороной организации производства (являющегося объектом инвестирования): оборудование; технологические процессы производства; разработка конструкторской и технологической документации.

По формам проявления:

Риски финансового инвестирования – риски, связанные с непродуманным выбором финансовых инструментов. (т.е .выбрали плохие акции – получили убыток или недополучили прибыль) и с непредвиденными изменениями условий инвестирования (т.е. изменение ранее оговоренного процента получаемой прибыли может снизить доход инвестора).

Риски реального инвестирования – риски, связанные с перебоями в поставках материалов и оборудования (т.е. не привезли вовремя сырье по причине плохой логистики - не выпустили вовремя партию товара - как следствие понесли убытки), ростом цен на инвестиционные товары и с неправильным выбором подрядчика для инвестирования в разного рода строящиеся объекты (т.е. выбор некомпетентного или недобросовестного подрядчика может привести к существенной задержке в сдаче объекта).

По источникам возникновения:

Системные риски (рыночные) – риски, характерные для всех объектов инвестирования и всех участников рынка в целом, на них невозможно повлиять и они относятся к категории недиверсифицируемых.

Системные риски подразделяются на:

– **Инфляционные риски** – риски, возникающие в случае, когда темпы инфляции примерно сопоставимы с ростом доходов предприятия, как итог возможно перекрытие всего дохода от инвестиционной деятельности или убытка.

– **Риски изменения процентной ставки** – риски, связанные с возможным изменением ставки, установленной Центробанком страны, что, в свою очередь, может отразиться на увеличении стоимости кредитов для предприятий.

– **Валютные риски** – риски, возникающие при взаимосвязи объекта инвестирования и иностранной валюты, выражающееся в возможности неблагоприятного изменения курса иностранной валюты.

Несистемные риски (нерыночные) – риски, характерные для отдельного участника рынка (инвестора) и (или) для отдельного объекта инвестирования, для каждого отдельного объекта свои, и их можно минимизировать за счет диверсификации.

Несистемные риски подразделяются на:

– **Отраслевые риски** – риски, характерные для отрасли в целом, подвержены одновременно все предприятия относящиеся к определенной отрасли. Минимизация отраслевых рисков возможна путем

диверсификации, предполагающей выбор объектов инвестирования принадлежащих к разным отраслям, слабо коррелирующим между собой.

– **Деловые риски** – риски, возникающие при неграмотном или нерациональном управлении предприятием, следствием которого является снижение его прибыльности и рыночной стоимости.

– **Кредитно-инвестиционные риски** – риски, возникающие при использовании инвестором кредитных средств. Возникает риск непогашения задолженности по кредиту в том случае, если инвестиции не принесут запланированного дохода.

– **Страновые риски** – риски, возникающие при инвестировании в объекты, находящиеся на территории других стран и зависящие от стабильности политической и экономической обстановки в них.

– **Риски упущенной выгоды** – риски, связанные с различными причинами, по которым будет недополучена (или не будет получена вовсе) потенциально возможная прибыль.

– **Риски ликвидности** – риски, связанные со сложностями перевода активов в наличные средства. Чем проще и быстрее это можно сделать, тем выше ликвидность и, соответственно, тем ниже риск.

– **Селективно-инвестиционные риски** – риски, возникающие при возможном выборе инвестором из нескольких объектов того (или тех), который принесет потенциально меньшую прибыль (или не принесет прибыли вовсе, или причинит убыток).

– **Функционально-инвестиционные риски** – риски, связанные с неправильным подбором объектов инвестирования (инвестиционного портфеля) и неправильным (неэффективным) управлением этим портфелем.

– **Операционно-инвестиционные риски** – риски, возникающие при сбоях и ошибках при проведении операций по инвестированию денежных средств (т.е. в случае инвестирования на фондовом рынке операционные риски могут возникать по вине брокера).

Страховые риски

Страховые риски – ожидаемые благоприятные или неблагоприятные события в виде убытков (по рисковому страхованию) или доходов (по сберегательному страхованию).

Страховые риски подразделяются на:

Чистые риски – определяют возможность получения отрицательного или нулевого экономического результата (риски стихийных бедствий, природные, техногенные, экологические риски).

Спекулятивные риски – дают возможность получить все три экономические результата – отрицательный, нулевой и положительный (финансовые риски как часть рисков коммерческой деятельности).

Страхуемые риски – это риски, которые могут быть переданы в порядке внешнего страхования соответствующим страховым организациям или риски, которые могут быть захеджированы самим предприятием.

Нестрахуемые риски – это риски, по которым отсутствует предложение соответствующих страховых продуктов на страховом рынке.

Аномальные риски – это риски, размер которых не позволяет отнести соответствующие объекты к тем или иным группам страховой совокупности.

Катастрофические риски – риски, связанные с проявлением стихийных сил природы, а также с преобразующей деятельностью человека в процессе создания материальных благ (например, авария на энергоблоке АЭС).

Экологические риски

Природно-экологические риски – риски, обусловленные изменениями в окружающей природной среде.

Технико-экологические риски – риски, обусловленные появлением и развитием техносферы:

Риски устойчивых техногенных воздействий – риски, связанные с изменениями окружающей среды в результате обычной хозяйственной деятельности человека;

Риски катастрофических воздействий – риски, связанные с изменениями окружающей среды в результате техногенных катастроф, аварий, инцидентов.

Социально-экологические риски – риски, обусловленные защитной реакцией государства и общества на обострение экологической обстановки.

Эколого-нормативные риски – риски, обусловленные принятием экологических законов и норм или их постоянным ужесточением.

Эколого-политические риски – риски, обусловленные экологическими акциями протеста.

Экономо-экологические риски – риски экономических потерь и ущерба, которые могут быть у объектов различного уровня общественной организации вследствие ухудшения состояния (качества) окружающей среды (экологических нарушений). Такое ухудшение может иметь различный характер: относительно медленный {эволюционный) и быстрый (катастрофический).

Производственные риски

Производственные риски – это форс-мажорные обстоятельства, возникшие во время производственного процесса, лабораторных исследований, разработок, реализации услуг, в процессе обслуживания и транспортировки.

Производственные риски подразделяется на следующие категории:

– **Риски в процессе разработки стратегии** – риски, связанные с необоснованным определением приоритетов общей экономической и рыночной стратегии предприятия, неправильным прогнозом конъюнктуры на всех или отдельных рынках капитальных закупок и снабжения и неадекватной оценкой потребности сферы потребления и собственного производства.

– **Снабженческие риски** – риски, связанные с: ненахождением поставщиков ресурсов, необходимых для осуществления данного направления предпринимательской деятельности; ненахождением поставщиков при проектируемых ценах закупок; отказом поставщиков от заключения контрактов на поставку; необходимостью заключения контрактов на условиях, отличающихся от наиболее приемлемых или обычных для предприятия и отрасли; затягиванием кампании по орга-

низации закупок; заключением контрактов на объемы текущего снабжения производства, не обеспеченные сбытом готовой продукции.

– **Риски нарушения плановых сроков** – риски, связанные с несоблюдением запланированного графика расходов и намеченного графика доходов.

– **Риски конфликтов с интересами поддержания текущей деятельности предприятия и других ее направлений** заключаются в том, что в процессе хозяйственной деятельности предприятия, несмотря на наличие приоритетных направлений, может происходить перераспределение средств на финансирование текущих потребностей или иных видов деятельности.

Технические риски (риски НИОКР) – риски, связанные с наличием вероятности возникновения отклонений от ожидаемых результатов или неудачи в процессе выполнения этих работ, при этом отклонения могут быть как отрицательные, так и положительные.

Риски реализации – это риски, возникающие в процессе реализации товаров и услуг, произведенных или купленных компанией (предпринимателем).

Риски реализации подразделяются на:

– **Риски упущенной выгоды** – риски наступления косвенного финансового ущерба (неполученная прибыль) в результате неосуществления какого-либо мероприятия (например, страхование, инвестирование и т.д.).

– **Риски снижения доходности** – риски, связанные с тем, что результаты реализации проекта могут оказаться хуже ожидаемых средних результатов, проект может оказаться недостаточно рентабельным, для того чтобы заемщик смог вернуть кредит.

Инновационные риски

Инновационные риски – это вероятность потерь, возникающих при вложении предпринимательской фирмой средств в производство новых товаров и услуг, которые, возможно, не найдут ожидаемого спроса на рынке.

Инновационные риски подразделяются на:

Маркетинговый (рыночный) риск – связан с рисками востребованности нового продукта (услуги) потребителем в тех объемах, по тем ценам и в те сроки, на которые рассчитывает компания.

Технический (технологический) риск – связан с рисками несоответствия нового продукта или услуги ожиданиям его разработчиков.

Исполнительский риск (человеческий фактор) – способность человеческих ресурсов компании (государства) разработать, произвести, вывести на рынок и поддерживать новый продукт (услугу) в соответствии с графиком.

Финансовый риск – связан с рисками обеспеченности у компании (государства) достаточными финансовыми ресурсами для выполнения в соответствии с графиком всех работ по разработке, выводу на рынок и дальнейшей поддержки нового продукта (услуги).

Коммерческие риски

Коммерческие риски – риски связанные с возможной опасностью потерь в процессе финансово-хозяйственной деятельности. Они означают неопределенность результатов от данной коммерческой деятельности.

Виды коммерческих рисков:

– **Имущественные риски** – связаны с вероятностью потерь имущества предпринимателя по причине кражи, диверсии, халатности, перенапряжения технической и технологической систем и т.д.

– **Производственные риски** – риски, связанные с убытком от остановки производства, прежде всего с «гибелью» или повреждением основных или оборотных фондов (оборудование, сырье, транспорт и т.д.), а также риски, связанные с внедрением в производство новой техники и технологии.

– **Торговые риски** – возникают вследствие задержки платежей, отказа от платежа в период транспортировки товара, непоставки товара и т.д.

Риски человеческого фактора

Риски, связанные с человеческим фактором, – риски, причинами возникновения которых являются поступки конкретных людей,

действующих как самостоятельные биологические существа, наделенные волей и сознанием.

Риски человеческого фактора подразделяются на:

Физиологические риски – риски, причинами реализации которых являются физиологические реакции и свойства организма конкретного человека.

Поведенческие риски – риски, причинами реализации которых являются решения и поступки конкретных людей, действующих как самостоятельное лицо.

Виды поведенческих рисков:

– **Риски мотивированных решений и поступков** – риски, связанные с поступками человека, совершенные осознанно в своих интересах в виде краж или неуплаты взноса по кредиту.

– **Риски немотивированных поступков –** риски, связанные с совершением человеком действий, имеющих нежелательные последствия, как для других, так и для него самого, которое происходит непреднамеренно или случайно (ошибки и упущения в работе).

Транспортные риски

Риск нарушений производственного процесса связан с изношенностью подвижного состава и постоянных устройств, отсутствием резервов пропускных и провозных способностей, сбоями в снабжении топливом и другими видами ресурсов, низким качеством сырья, материалов, запасных частей и недостатками в организации труда.

Разновидности:

– технический;

– организационный;

– риск военных и террористических действий и гражданских беспорядков;

– риск форс-мажорных обстоятельств.

Риск разработки, внедрения и освоения новой техники и технологии связан с несоответствием расчетных параметров работы новой техники, отказами в работе новой техники, неэффективностью

инновационной деятельности, неточной оценкой лизинговых сделок и невозвратом кредита и процентов.

Разновидности:

– инвестиционный;

– кредитный;

– селективный;

– лизинговый.

Риск в процессе реализации продукции и осуществления коммерческих сделок связан с недобросовестностью партнеров (смежников), потерей имущества и снижением качества перевозимых грузов, непредставлением грузов к перевозке, отсутствием страхования грузов и транспортных средств и падением или неустойчивым спросом.

Разновидности:

– имущественный;

– риск невыполнения обязательств.

Риск при осуществлении финансовых сделок связан с колебаниями курсов валют, действием инфляции, изменением системы налогообложения и величины транспортных тарифов.

Разновидности:

– валютный;

– инфляционный;

– кредитный;

– процентный;

– налоговый;

– риск законодательных изменений.

Риск проведения внешнеэкономических операций связан с нестабильностью политической и экономической ситуации в отдельных странах, ошибками в маркетинговой стратегии, недостаточной надежностью партнеров и изменением курсов валют.

Разновидности:

– страновый;

– маркетинговый;

– риск выбора партнера;

– валютный.

Риск кадрового потенциала связан с нехваткой рабочей силы, профессиональной непригодностью, вредностью производства, травматизмом, скрытой безработицей, переходом компетентных и информированных сотрудников к конкурентам или в криминальные структуры.

Разновидности:

– профессиональный;

– риск необеспеченности кадрами;

– риск разглашения коммерческой тайны.

Риск негативного воздействия на природу связан с проявлением стихийных сил природы, происшествиями, авариями и катастрофами на объектах транспорта и несанкционированными выбросами загрязняющих веществ.

Разновидности:

– природно-естественный;

– техногенный.

Природные риски

Классификация природных рисков по генезису:

Космогенные риски связаны с гравитационными опасностями и вещественными (метеорными) потоками.

Космогенно-климатические риски связаны с климатическими циклами, длительными колебаниями мирового океана, современным потеплением климата и проблемами озоновых дыр.

Атмосферные риски связаны с метеогенными (атмосферные фронты, циклоны, западные ветры и вихри) явлениями, опасными

природными явлениями в атмосфере зимнего периода и опасными природными явлениями в атмосфере летнего периода.

Гидрологические и гидрогеологические риски связаны с гидрологическими опасностями во внутренних водоемах, ледовыми опасными явлениями (заторы, наледи, морские и горные ледники), ветровыми геологическими явлениями (тайфун, сильное волнение на море, ветровой нагон, волновая абразия морских волн) и подземными волнами и их воздействием.

Риски геологически опасных процессов связаны с эндогенными опасными природными процессами (извержение вулкана, землетрясение, разжижение грунта), экзогенными опасными природными процессами (оползни, осыпи, лавины, овражная эрозия, эрозия речных берегов) и ветровыми эрозиями почв.

Риски инфекционных заболеваний людей связаны с единичными случаями особо опасных инфекционных заболеваний, групповыми случаями опасных инфекционных заболеваний, эпидемией (массовое инфекционное заболевание людей), пандемией (эпидемия, охватывающая значительную часть населения инфекционным заболеванием не выясненного происхождения).

Риски поражения сельскохозяйственных растений связаны с болезнями сельскохозяйственных растений по невыявленным причинам, прогрессирующей эпифитотией (массовое заболевание растений).

5.2 Управление рисками и информационная безопасность

В настоящее время информация очень часто рассматривается как наиболее ценный ресурс. Это неудивительно, так как в современном компьютеризированном мире наиболее эффективные конкурентные преимущества фирма может получить в основном за счет обладания уникальной информацией, будь то новейшие технологические разработки, необходимые для успеха на развивающемся рынке мобильных устройств, или данные о предпочтениях интернет-пользователей, имеющие огромную ценность для эффективной целевой рекламы. Кроме того, информация ограниченного доступа

(например, персональные данные клиентов) всегда представляла ценность для ее обладателей и вызывала интерес со стороны злоумышленников.

Еще одной причиной актуальности проблемы обеспечения информационной безопасности является повсеместное использование автоматизированных средств хранения, передачи и обработки информации.

Именно поэтому информационной безопасности в последнее время уделяется все больше внимания: высший менеджмент предприятий различных сфер деятельности готов тратить все больше сил и средств на создание и развитие системы защиты информации, а также системы менеджмента информационной безопасности. Стоит заметить, что формирование режима информационной безопасности является комплексной задачей и осуществляется на трех уровнях: законодательно-правовом, административном (организационном) и программно-техническом. Для достижения поставленной цели требуется большое количество материальных и человеческих ресурсов.

Именно поэтому в настоящее время анализу рисков информационной безопасности уделяется все больше внимания. Этому есть несколько основных **причин**: безостановочный рост использования информационных технологий в процессе деятельности практически любой современной организации, увеличение ценности информации, обрабатывающейся и генерирующейся в процессе работы компании, а также интеграция различных информационных продуктов с целью покрытия всех нужд фирмы.

Теперь рассмотрим некоторые **основные понятия и определения**, необходимые для изучения этой проблемы.

Начнем с определения **информационная безопасность** (ИБ), под которым понимается сохранение конфиденциальности, целостности и доступности информации.

Конфиденциальность информации не может быть доступной или раскрытой для неавторизованного на то лица.

При этом д**оступность информации** определяется как доступность и используемость данных по запросу со стороны авторизованного логического объекта.

Целостность можно определить как свойство сохранения правильности и полноты информации.

Далее дадим также определения ситуаций, связанных с нарушением ИБ. Так, **событие информационной безопасности** определим как идентифицированное возникновение состояния системы, услуги или сети, указывающее на возможное нарушение политики информационной безопасности или аварию защитных мер (средств), а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью.

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий информационной безопасности, которые имеют значительную вероятность компрометации бизнес-операции и угрожают информационной безопасности.

Система информационной безопасности (СИБ) – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента информационной безопасности (СМИБ) – та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности.

Угроза информационной безопасности – это потенциальная возможность нарушения режима информационной безопасности. Преднамеренная реализация угрозы называется атакой на информационную систему.

Уязвимость ИС – это так называемое «слабое место» в информационной системе, которое является основанием для возникновения угрозы со стороны злоумышленников.

Активы – все, что имеет ценность для организации. В информационной системе главным активом является сама

информация – базы данных и другая ценная для организации информация, хранящаяся в цифровой форме.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации, находящаяся в распоряжении организации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.

Особого внимания относительно рисков информационной безопасности заслуживает **банковская сфера**, так как стоимость информации в компаниях, работающих в данной области, еще выше за счет превалирования персональных данных клиентов, обладание которыми дает возможность получить несанкционированный доступ к финансовым ресурсам.

Кроме того, существует такое понятие, как банковская тайна, суть которой заключается в обязанности каждого банка (или иной кредитной организации) защищать сведения о вкладах и счетах своих клиентов и корреспондентов, банковских операциях по счетам и сделках в интересах клиента, а также сведения клиентов, разглашение которых может нарушить право последних на неприкосновенность частной жизни (ФЗ «О банках и банковской деятельности» от 02.12.1990 N 395-1 (последняя редакция).

Таким образом, информация, задействованная в работе коммерческих банков, нуждается в особой защите от потери ее свойств, а именно конфиденциальности, целостности и доступности. В частности, особое внимание должно уделяться поиску уязвимостей в системе защиты информации и анализу и оценке рисков информационной безопасности.

Однако на данный момент не существует стандартизированной методики анализа и оценки рисков информационной безопасности для кредитных организаций, обязательной для применения банками России. Все разработанные и активно использующиеся методики являются довольно общими для организаций, работающих в различных секторах экономики, они не учитывают особенностей банковского законодательства и специфики деятельности кредитных организаций.

Между тем, изучение современных методик анализа и управления рисками, связанными с информационной безопасностью (ИБ), является необходимостью для любого пользователя информационных технологий, и не только в сфере банковской деятельности. При этом под рисками в сфере ИБ следует понимать потенциальную возможность понести убытки и потери из-за нарушения безопасности информационной системы (ИС). При этом отметим, что понятие риска отличается от понятия угрозы именно тем, что риск отличает наличие количественной оценки возможных потерь и оценки вероятности наступления нежелательного события.

Как известно, для любого проекта, требующего финансовых затрат на его реализацию, весьма желательно уже на начальной стадии определить, что следует считать положительным результатом проекта. Для задач, связанных с обеспечением ИБ, это тем более важно и актуально.

На практике наибольшее распространение получили два подхода к **обоснованию проекта подсистемы обеспечения безопасности**.

Первый из них основан на проверке соответствия уровня защищенности ИС требованиям одного из стандартов в области информационной безопасности. Это может быть класс защищенности в соответствии с утвержденными требованиями.

При этом основной недостаток данного подхода заключается в том, что в случае, когда требуемый уровень защищенности четко не задан (например, через законодательные требования), определить наиболее эффективный уровень защищенности ИС достаточно сложно.

Второй подход к построению системы обеспечения ИБ связан с оценкой и управлением рисками. Изначально он произошел из принципа разумной достаточности, примененного к сфере обеспечения ИБ.

Этот принцип может быть описан следующим набором утверждений: абсолютно непреодолимую систему защиты создать невозможно; необходимо соблюдать баланс между затратами на защиту и получаемым эффектом, в т.ч. и экономическим, заключающимся в снижении потерь от нарушений безопасности;

стоимость средств защиты не должна превышать стоимости защищаемой информации (или других ресурсов – аппаратных, программных); затраты нарушителя на несанкционированный доступ к информации должны превышать тот эффект, который он получит, осуществив подобный доступ.

К сожалению, на практике точные зависимости между затратами и уровнем защищенности определить не представляется возможным, поэтому аналитический метод определения минимальных затрат в представленном виде неприменим.

Поэтому, для того чтобы перейти к рассмотрению вопросов описания риска, введем еще одно определение. Ресурсом или активом будем называть именованный элемент ИС, имеющий (материальную) ценность и подлежащий защите.

Тогда риск может быть идентифицирован следующим **набором параметров**: угроза, с возможной реализацией которой связан данный риск; ресурс, в отношении которого может быть реализована угроза (ресурс может быть информационный, аппаратный, программный и т.д.); уязвимость, через которую может быть реализована данная угроза в отношении данного ресурса.

Важно также определить то, как мы узнаем, что нежелательное событие произошло. Поэтому в процессе описания рисков обычно также указывают события-триггеры, являющиеся идентификаторами рисков, произошедших или ожидающихся в скором времени (например, увеличение времени отклика web-сервера может свидетельствовать о производимой на него одной из разновидностей атак на «отказ в обслуживании»).

Исходя из сказанного выше, в **процессе оценки риска** надо оценить **стоимость ущерба** и частоту возникновения нежелательных событий и вероятность того, что подобное событие нанесет урон ресурсу. Размер ущерба от реализации угрозы в отношении ресурса зависит от стоимости ресурса, который подвергается риску, и степени разрушительности воздействия на ресурс, выражаемой в виде коэффициента разрушительности.

Далее необходимо оценить **частоту возникновения** рассматриваемого нежелательного события (за какой-то

фиксированный период времени, например, за год) и вероятность успешной реализации угрозы. Затем ожидаемый ущерб сравнивается с затратами на меры и средства защиты, после чего принимается решение в отношении данного риска.

Он может быть: принят; снижен (например, за счет внедрения средств и механизмов защиты, уменьшающих вероятность реализации угрозы или коэффициент разрушительности); устранен (за счет отказа от использования подверженного угрозе ресурса); или перенесен на другое лицо (например, застрахован, в результате чего в случае реализации угрозы безопасности потери будет нести страховая компания, а не владелец ИС).

Как известно, **анализ и оценка рисков** ИБ проводится для получения следующей информации: какие риски информационной безопасности существуют в организации; какова вероятность их реализации; какой ущерб будет нанесен в результате их реализации; какие риски компания может принять (на основе критериев принятия риска); какие средства защиты являются наиболее адекватными для борьбы с той или иной уязвимостью в СИБ; какой объем денежных средств должен быть в резерве на случай возникновения инцидента информационной безопасности и т.д.

При этом есть несколько стандартов, в которых описываются требования к построению систем менеджмента информационной безопасности. Это такие документы, как ГОСТ Р ИСО/МЭК 27001[4] и ГОСТ Р ИСО/МЭК 17799. В обоих из них содержится информация о правилах и порядке проведения анализа и оценки рисков информационной безопасности.

Так, в соответствии с ГОСТ Р ИСО/МЭК 27001 порядок работы с рисками следующий: идентификация рисков – идентифицировать активы, относящиеся к области применения СМИБ, и определить собственников этих активов; идентифицировать угрозы этим активам; идентифицировать уязвимости, которые могут быть использованы этими угрозами; идентифицировать возможные воздействия, которые могут привести к утрате конфиденциальности, целостности и доступности активов.

Для анализа и оценки риска необходимо: оценить ущерб бизнесу, который может быть нанесен в результате нарушения

безопасности с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов; оценить реальную вероятность возникновения такого нарушения безопасности в свете превалирующих угроз и уязвимостей, воздействия на соответствующие активы, а также применяемые меры контроля; оценить уровни рисков; определить, является ли риск приемлемым или требуется обработка риска с использованием определенных критериев.

Очевидно, что данные рекомендации – это примерный и очень общий план действий по управлению рисками информационной безопасности, не позволяющий, если ему следовать, эффективно оценить риски ИБ в крупной компании. Так как государственных стандартов недостаточно, широкое применение приобретают методики, разрабатываемые частными компаниями, такие как Lifecycle Security или методика Microsoft.

Здесь также стоит упомянуть о существовании средства оценки безопасности Microsoft Security Assessment Tool (MSAT), который представляет собой бесплатное программное обеспечение, позволяющее оценить уязвимости в ИТ-средах, предоставить список расставленных по приоритетам проблем и список рекомендаций по минимизации этих угроз.

Рассмотрим **порядок применения программы управления рисками** в системе информационной безопасности по методике Microsoft.

Вначале отметим, что этапы качественной оценки рисков во всех методиках примерно одинаковы: выявление рисков ИБ, определение вероятности возникновения каждого из них, определение стоимости активов, которые пострадают от реализации конкретного риска, а также распределение описанных рисков на группы в зависимости от ранее оговоренных критериев значительности риска, а также возможности его принятия. Так и в данной методике на начальном этапе рискам присваиваются значения в соответствии со шкалой: высокий (красная область), существенный (желтая область), умеренный (синяя область) и незначительный (зеленая область).

При этом для проведения эффективной оценки требуется собрать самые актуальные данные об активах организации, угрозах

безопасности, уязвимостях, текущей среде контроля и предлагаемых элементах контроля. Далее проводится сложный и многоступенчатый процесс анализа и оценки рисков, в результате которого владельцы бизнеса получают информацию не только о существующих рисках, вероятностях их реализации, уровнях влияния на деятельность компании, но и оценку ожидаемого годового ущерба (ALE).

Процесс анализа информационной сети на наличие в ней уязвимостей против возможных угроз и к возможным рискам осуществляется с помощью ответов на более чем 200 вопросов, охватывающих инфраструктуру, приложения, операции и персонал.

Первая серия вопросов предназначена для определения бизнес-модели компании, на основе полученных ответов средство создает профиль бизнес-риска (BRP). По результатам ответа на вторую серию вопросов составляется список защитных мер, внедренных компанией с течением времени.

В совокупности эти меры безопасности образуют уровни защиты, предоставляя большую защищенность от угроз безопасности и конкретных уязвимостей. Сумма уровней, образующих комбинированную систему глубокой защиты, называется индексом глубокой защиты (DiDI).

После этого BRP и DiDI сравниваются между собой для измерения распределения угроз по областям анализа – инфраструктуре, приложениям, операциям и людям. Полученная оценка предназначена для использования в организациях среднего размера, содержащих от 50 до 1500 настольных систем.

В результате ее использования менеджмент компании получает общую информацию о состоянии системы защиты информации предприятия, охватывая большинство областей потенциального риска, но описываемое средство не предусмотрено для предоставления глубокого анализа конкретных технологий или процессов.

Следующая методика – методика CCTA Risk Analysis and Management Method (CRAMM) – одна из первых методик анализа рисков в сфере информационной безопасности. В основе метода CRAMM лежит комплексный подход, сочетающий процедуры количественной и качественной оценки рисков. Исследование

информационной безопасности системы с помощью CRAMM может проводиться двумя способами, преследующими две качественно разные цели: обеспечение базового уровня ИБ и проведение полного анализа рисков. От того, какая задача стоит перед специалистами по оценке рисков, зависит количество проводимых этапов работы.

Перечислим все возможности данной методики, делая акцент на обстоятельствах применения той или иной процедуры анализа. **Первая стадия** является подготовительной и обязательной при постановке любой из двух возможных целей исследования информационной безопасности системы. Во время данного этапа формально определяются границы рассматриваемой информационной системы, ее основные функции, категории пользователей и персонала, принимающего участие в исследовании.

На второй стадии проводится анализ всего, что касается выявления и определения ценности ресурсов рассматриваемой системы: проводится идентификация физических, программных и информационных ресурсов, находящихся внутри границ системы, а затем производится распределение их на заранее выделенные классы. В результате заказчик имеет хорошее представление о состоянии системы и может принять решение о необходимости проведения полного анализа рисков. При условии, что обеспечения базового уровня ИБ клиенту не достаточно, строится модель информационной системы с позиции ИБ, которая позволит выделить наиболее критичные элементы.

На **третьей стадии**, которая проводится только в том случае, если необходимо проведение полного анализа рисков, рассматривается все, что относится к идентификации и оценке уровней угроз для групп ресурсов и их уязвимостей. На данном этапе оценивается влияние определенных групп ресурсов на работоспособность пользовательских сервисов, определяется текущий уровень угроз и уязвимостей, вычисляются уровни рисков и проводится анализ результатов. В итоге заказчик получает идентифицированные и оцененные уровни рисков ИБ для исследуемой системы.

На **четвертой стадии** для каждой группы ресурсов и каждого из 36 типов угроз программное обеспечение CRAMM составляет список вопросов, предполагающих однозначный ответ.

Как и в случае с методикой компании Microsoft, в CRAMM проводится качественная оценка риска путем отнесения уровней угроз к той или иной категории в зависимости от полученных ответов. Всего в данной методике есть пять категорий уровней угроз: очень высокий, высокий, средний, низкий и очень низкий. В свою очередь, уровень уязвимости ресурса оценивается, в зависимости от ответов, как высокий, средний и низкий. На основе данной информации, а также размеров ожидаемых финансовых потерь, рассчитываются уровни рисков по шкале от 1 до 7, объединенные в матрице оценки риска.

При этом следует отметить, что метод CRAMM по праву может быть отнесен к методикам, использующим как качественный, так и количественный подходы к анализу рисков информационной безопасности, так как в процессе проведения оценки учитывается уровень ожидаемых финансовых потерь от реализации риска, а результаты предоставляются в баллах по шкале от 1 до 7. Этот факт значительно повышает рейтинг методики CRAMM в глазах специалистов в данной предметной области.

На **последней стадии** исследования, носящей название «Управление рисками», производится выбор адекватных элементов контроля: программное обеспечение CRAMM генерирует несколько вариантов мер противодействия, адекватных выявленным рискам и их уровням, из которых выбирается оптимальный вариант системы безопасности, удовлетворяющий требованиям заказчика.

Методика Facilitated Risк Analysis Process (FRAP) – это модель построения системы защиты информации, включающая в себя качественный анализ рисков. Приведем предусмотренные в этой методике основные этапы оценки рисков.

На первом этапе, с опорой на данные опросов, техническую документацию, автоматизированный анализ сетей, составляется список находящихся в зоне риска активов.

На следующем этапе проводится идентификация угроз. При составлении списка угроз могут использоваться следующие различающиеся методы.

Конвенциональный (обычный) метод. В этом случае эксперты составляют перечни (checklists) потенциальных угроз, из которых впоследствии выбираются наиболее актуальные для данной системы.

Статистический метод. При этом методе проводится анализ статистики происшествий, связанных с информационной безопасностью данной ИС и подобных ей, и оценивается их средняя частота, после чего производится оценка точек риска.

Метод «мозгового штурма», проводимый сотрудниками компании. Отличие от первого метода состоит в том, что он проводится без привлечения внешних экспертов. Далее, после составления списка потенциальных угроз производится сбор статистики по каждому случаю возникновения риска: частоте той или иной ситуации, а также по уровню претерпеваемого ущерба. Опираясь на эти значения, эксперты оценивают уровень угрозы по обоим параметрам: вероятности возникновения угрозы (High Probability, Medium Probability and Low Probability) и ущерба от нее (High Impact, Medium Impact and Low Impact).

Затем, в соответствии с правилом, задаваемым матрицей рисков, определяется **оценка уровня риска**:

- наивысший уровень, уровень A – направленные на элиминацию угрозы меры (например, внедрение системы защиты информации (СЗИ)) должны быть предприняты немедленно и в обязательном порядке;

- высокий уровень, уровень B – необходимо предпринять меры, направленные на снижение риска;

- средний уровень, уровень C – необходим мониторинг ситуации;

- низкий уровень, уровень D – никаких действий в данный момент предпринимать не требуется.

После того как угрозы были идентифицированы и относительные риски оценены, следует составить план действий, позволяющий устранить риск или уменьшить его до приемлемого уровня.

По окончании оценки рисков результаты должны быть подробно документированы и переведены в стандартизованный формат. Эти данные могут быть использованы при планировании дальнейших процедур в области обеспечения безопасности, бюджета, выделяемого на эти процедуры и т.д.

Программа Risk Advisor – это программный продукт, разработанный компанией MethodWare, в котором реализована методика, позволяющая задать модель информационной системы с позиции информационной безопасности, идентифицировать риски, угрозы, потери в результате инцидентов. При работе с этой программой следует реализовать пять основных этапов работы.

Описание контекста. В первую очередь необходимо создать общую схему внешних и внутренних информационных контактов организации. Эта модель строится в нескольких измерениях и задается следующими параметрами: стратегическим, организационным, бизнес-целями, управлением рисками, критериями. Картина общего контекста с точки зрения стратегии описывает сильные и слабые стороны организации в плане внешних контактов. Здесь производится классификация угроз, связанных с отношениями с партнерами, оцениваются риски, сопряженные с различными вариантами развития внешних связей организации. Описание контекста в организационном измерении включает в себя картину отношений внутри организации, стратегию развития и внутреннюю политику. Схема управления рисками включает в себя концепцию информационной безопасности. Наконец, в контексте бизнес-целей и критериев оценки описываются, как следует из названия, ключевые бизнес-цели и качественные и количественные критерии, с опорой на которые производится управление рисками.

Описание рисков. Для того чтобы облегчить и стандартизировать процесс принятия решений, связанных с управлением рисками, данные по ним необходимо стандартизировать. В разных моделях используются разные шаблоны для формализации имеющейся информации. В описываемой нами методике задается матрица рисков, в которой учитываются не только собственные параметры этих рисков, но и информация об их связях с остальными элементами общей системы. Следует отметить, что риски оцениваются здесь по качественной, а не количественной шкале и делятся всего на две категории: приемлемые и неприемлемые. После этой оценки производится выбор контрмер и анализ стоимости и эффективности выбранных средств защиты.

Описание угроз. Прежде всего составляется общий список угроз. Затем они классифицируются по качественной шкале, описываются взаимосвязи между различными угрозами и связи типа «угроза – риск».

Описание потерь. На этом этапе описываются события, связанные с инцидентами информационной безопасности, после чего оцениваются риски, вызванные этими событиями.

Анализ результатов. После построения модели формируется детальный отчет (состоящий более чем из 100 разделов). Агрегированные описания представляются потребителю в виде графа рисков.

Компания RiskWatch, также как и Microsoft, разработала собственную методику анализа и оценки рисков, которая реализуется в ряде программных средств.

В **методе RiskWatch** в качестве критериев для оценки и управления рисками используются ожидаемые годовые потери (Annual Loss Expectancy, ALE) и оценка возврата инвестиций (Return on Investment, ROI). Методика RiskWatch ориентирована на точную количественную оценку соотношения потерь от угроз безопасности и затрат на создание системы защиты. Процесс анализа рисков состоит из четырех этапов.

На первом этапе, являющемся, по сути, подготовительным, определяется предмет исследования: дается описание типа организации, состава исследуемой системы, базовых требований в области информационной безопасности и т.д. Программное обеспечение RiskWatch предлагает широкий выбор всевозможных категорий защищаемых ресурсов, потерь, угроз, уязвимостей и мер защиты, из которых аналитик выбирает только те, что реально присутствуют в исследуемой системе. Кроме того, есть возможность добавления новых элементов и корректировка уже существующих описаний.

На втором этапе производится более детальное описание системы (какие ресурсы в ней присутствуют, какие типы потерь могут иметь место при реализации риска и какие классы инцидентов можно выделить путем сопоставления категории потерь и категории

ресурсов. Есть два варианта ввода данных: вручную или путем импорта из отчетов, сгенерированных в процессе анализа компьютерной сети на наличие в ней уязвимостей. Для выявления возможных слабых мест системы используется опросник, в котором предлагается ответить более чем на 600 вопросов, связанных с категориями ресурсов. В связи с тем, что компании из разных сфер деятельности имеют свои исключительные особенности, а также учитывая быстро развивающийся рынок информационных технологий, является очень разумным и удобным наличие возможности корректировки вопросов и исключение/добавление новых. Далее определяется частота реализации каждой из присутствующих в системе угроз, уровень уязвимости и ценность ресурсов. На основе данной информации рассчитывается эффективность использования тех или иных элементов контроля информационной безопасности.

На третьем этапе производится количественная оценка риска. Первым делом определяется взаимосвязь между ресурсами, потерями, угрозами и уязвимостями, определенными в процессе проведения первых двух этапов работы. Кроме того моделируются сценарии «что если…», в которых аналогичные ситуации рассматриваются с учетом внедрения средств защиты. Путем сравнения ожидаемых потерь при условии использования элементов контроля и без них можно оценить, насколько эффективным будет внедрение тех или иных защитных мер.

На последнем этапе генерируются отчеты разных видов: краткие итоги, полные и краткие отчеты об элементах, описанных на стадиях 1 и 2, отчет о стоимости защищаемых ресурсов и ожидаемых потерь от реализации угроз, отчет об угрозах и мерах противодействия, отчет о результатах аудита безопасности.

Таким образом, применение этой программы позволяет не только оценить риски, которые на данный момент существуют у предприятия, но и выгоду, которую может принести внедрение физических, технических, программных и прочих средств и механизмов защиты. Подготовленные отчеты и графики дают материал, достаточный для принятия решений об изменении системы обеспечения безопасности предприятия. Кроме того, описываемое

программное обеспечение может являться удобной основой для разработки собственного, максимально подходящего для предприятий конкретного типа (например, кредитных организаций), средства анализа и оценки рисков информационной безопасности.

Отметим также **ГРИФ – российское комплексное средство анализа и управления рисками** информационной системы организации, разработанное компанией Digital Security. Принцип работы данного программного обеспечения основан на двух концептуально разных подходах к оценке рисков информационной безопасности, получивших названия «модель информационных потоков» и «модель угроз и уязвимостей». Рассмотрим каждый из алгоритмов по отдельности.

Модель информационных потоков характеризуется тем, что в основе алгоритма анализа и оценки рисков лежит построение модели информационной системы организации. Расчет значений рисков базируется на информации о средствах защиты ресурсов с ценной информацией, взаимосвязях ресурсов между собой, влиянии прав доступа групп пользователей и организационных мерах противодействия.

На первом этапе необходимо подготовить полное описание архитектуры исследуемой сети, включающее информацию о ценных ресурсах, их взаимосвязях, группах пользователей, средствах защиты информации и др. Исходя из введенных данных, можно построить полную модель информационной системы компании, на основе которой будет проведен анализ защищенности каждого вида информации на ресурсе.

Далее оценка риска производится отдельно по каждой связи «группа пользователей – информация» по трем типам угроз: конфиденциальность, целостность и доступность (при этом для первых двух типов результат рассчитывается в процентах, а для последнего – в часах простоя). Ущерб от реализации разных видов угроз тоже задается отдельно, т.к. оценить комплексные потери не всегда возможно.

Ключевыми критериями, от которых зависит вероятность реализации той или иной угрозы, являются виды (локальный и/или удаленный) и права (чтение, запись, удаление) доступа пользователей

к ресурсам, наличие доступа в интернет, количество человек в группе, использование антивирусного ПО, криптографических средств защиты (особенно значимо для дистанционного доступа) и т.д.

На этом же этапе определяются средства защиты информации и рассчитываются коэффициенты локальной защищенности информации на ресурсе, удаленной защищенности информации на ресурсе и локальной защищенности рабочего места группы пользователей. Минимальный коэффициент отражает реальный уровень защиты ресурса, т.к. указывает на наиболее уязвимое место в информационной системе. Для того чтобы получить итоговую вероятность реализации угрозы, полученный показатель необходимо умножить на базовую вероятность реализации угрозы ИБ, которая рассчитывается на основе метода экспертных оценок.

На последнем этапе значение полученной итоговой вероятности умножается на величину ущерба от реализации угрозы и рассчитывается риск угрозы информационной безопасности для связи «вид информации – группа пользователей». Алгоритм расчета величины риска по угрозе «отказ в обслуживании» имеет незначительные отличия, связанные, в основном, с единицами измерения.

В результате работы использования указанного алгоритма пользователь программы получает следующую информацию: риск реализации по трем базовым угрозам для вида информации, риск реализации по трем базовым угрозам для ресурса, риск реализации суммарно по всем угрозам для ресурса, риск реализации по трем базовым угрозам для информационной системы, риск реализации по всем угрозам для информационной системы, риск реализации по всем угрозам для информационной системы после задания контрмер, эффективность контрмер комплекса контрмер.

Модель анализа угроз и уязвимостей описывает еще один подход к анализу и оценке рисков информационной безопасности. В качестве входной информации выступает перечень ресурсов, содержащих ценную информацию, описание угроз, воздействующих на каждый ресурс, и уязвимостей, через которые возможна реализация вышеупомянутых угроз. Для каждого из видов исходных данных

(кроме уязвимостей) указывается степень критичности. Также вводится вероятность реализации той или иной угрозы.

Этот алгоритм может работать в двух режимах: рассчитывая вероятность реализации одной базовой угрозы или распределяя оценки по трем базовым типам угроз. Перечислим **этапы метода** в общем виде для обоих режимов.

1. Рассчитывается уровень угрозы по конкретной уязвимости на основе критичности и вероятности реализации угрозы через данную уязвимость.

2. Уровень угрозы по всем уязвимостям рассчитывается путем суммирования уровней угроз через конкретные уязвимости.

3. Рассчитывается общий уровень угроз по ресурсу.

4. Рассчитывается риск по ресурсу.

5. Рассчитывается риск по информационной системе.

Алгоритм анализа и оценки рисков ГРИФ – это образец методики, которая учитывает особенности структуры компании заказчика, используя два разных подхода к расчету величин рисков. Каждый из этих двух методов может быть более эффективен в случае с одной фирмой и менее эффективен в ситуации с другой. Таким образом, методика ГРИФ исключает возможность использования неподходящего алгоритма расчета уровня риска, гарантируя достижения оптимального результата.

Очевидно, что среди описанных в данном учебном пособии методик нет идеального варианта, так как ни одна компания-разработчик не ставила своей целью создание алгоритма анализа и оценки рисков ИБ для предприятий какой-либо конкретной сферы.

Наоборот, более логичным является разработка универсального средства для решения проблем информационной безопасности предприятия, которое позволило бы получить максимальную выгоду от его продажи как можно большему числу фирм-клиентов.

Существуют также и **специальные методики**, разрабатываемые применительно для отдельных отраслей и секторов экономики. Так, в банковской сфере существует особая методика анализа и оценки рисков ИБ в организациях банковской системы РФ, разработанная в 2009 году Банком России, однако она носит лишь рекомендательный характер.

Поэтому и до сегодняшнего времени есть и остается потребность в разработке эталонной методики анализа и оценки рисков информационной безопасности в банковской сфере на основе существующих стандартов и методик построения системы защиты информации на предприятии. Кроме того, процесс анализа и оценки рисков информационной безопасности необходимо рассматривать в контексте разработки системы управления информационной безопасностью организации, так как анализ рисков сам по себе не принесет компании желаемого результата, а именно минимизации этих рисков и сокращения ожидаемых потерь от их реализации.

Вопросы безопасности информационных систем. Вопросам безопасности информационных систем (ИС) уделяется большое внимание как на национальном уровне, так и на уровне международного сотрудничества. На национальном уровне страны стремятся, в первую очередь, обеспечить безопасность информации и безопасность средств работы с этой информацией, как аппаратных, так и программных. Важное место при этом уделяется унификации применяемых средств (методов и инструментов) защиты ИС.

Международное сотрудничество между странами также необходимо, поскольку, во-первых, процессы информатизации, по необходимости, имеют глобальный, международный характер – и в производстве материальной основы ИС, и в разработке программных продуктов, управляющих работой ИС. Во-вторых, международное сотрудничество позволяет разрабатывать и внедрять средства и методы защиты безопасности ИС более дешевым и эффективным образом – создавать такие средства и методы, которые носили бы универсальный характер, могли бы использоваться разными странами и для разных типов информационных систем.

Для этих целей разрабатываемые общие для отрасли ИТ стандарты и спецификации. Учитывая изначальное лидерство США в сфере внедрения ИТ в гражданские отрасли, неудивительно, что первые стандарты были разработаны в США и на английском языке. С глобализацией интернета стали появляться международные стандарты безопасности ИС – также на английском языке.

Кроме того, международное сотрудничество разработчиков ИС имеет своим следствием появление фирм, предлагающих универсаль-

ные решения защиты ИС для любых пользователей информационными технологиями. Среди них есть и российские разработчики, например, фирма Касперского, предлагающая средства антивирусной защиты для ИС.

В целом все стандарты, действующие и применяемые в сфере ИТ, подразделяются на две категории: СИК – стандарты оценки и классификации ИС и средств защиты ИС, и стандарты-регламенты (СР). Последние стандарты устанавливают некоторые общие правила работы со средствами защиты ИС.

СИК определяют некоторые общие правила к построению ИС, которые играют роль организационных и архитектурных спецификаций, из которых могут выбирать разработчики ИС.

СР формируют набор требований и условий, которым должны удовлетворять создаваемые ИС определенного назначения и определенной архитектуры.

В число основных СИК входят: «Критерии оценки надежности ИС» – стандарт Министерства обороны США, Федеральный стандарт США «Требования безопасности для криптографических модулей», «Гармонизированные критерии Европейских стран» и международный стандарт «Критерии оценки безопасности информационных технологий». В РФ на основе этих документов разработаны свои, национальные стандарты, представленные в виде Руководящих документов Федеральной службы по техническому и экспертному контролю России.

В качестве СР для наиболее распространенных так называемых распределенных (глобальных) сетей действуют технические спецификации, разрабатываемые Тематической группой по технологиям Интернета – IETF (Internet Engineering Task Force).

В сфере **международных стандартов**, устанавливающих общие правила по управлению информационной безопасностью, наиболее известен **стандарт ISO/IEC** 17799-2000 Code of Practice for Information Security Management (основанный на ранее разработанном аналогичном британском стандарте). Этим стандартом установлены основные критерии оценки механизмов защиты ИБ, а также представлены административно-процедурные нормы и материальные средства защиты ИС.

По своему содержанию данный стандарт разбит на десять **разделов**:

- политика безопасности,
- организация защиты,
- классификация ресурсов и их контроль,
- безопасность персонала,
- физическая безопасность,
- администрирование компьютерных систем и сетей,
- управление доступом,
- разработка и сопровождение ИС,
- планирование бесперебойной работы организации,
- контроль выполнения требований политики безопасности.

При этом основными из этих правил и норм признаются средства контроля безопасности ИС и системы управления рисками, а также анализ их адекватности имеющимся рискам и угрозам.

На основе этого международного стандарта в большинстве стран разработаны и применяются свои, национальные стандарты и нормативные документы, в том числе отраслевого и узкоспециального уровня.

В качестве образцовых технических спецификаций обычно используются документы и нормативы, разработанные IETF, включая правила защиты средств передачи информации – Transport Layer Security (TLS) и разработки приложений – спецификации GSS-API и Kerberos. Важное значение имеют также прикладные спецификации X.500 «Служба директорий: обзор концепций, моделей и сервисов», X.509 «Служба директорий: каркасы сертификатов открытых ключей и атрибутов» и X.800 «Архитектура безопасности для взаимодействия открытых систем».

На программно-техническом уровне ключевым является **международный стандарт ISO** 15408-1999 «Общие критерии оценки безопасности информационных технологий» – Common Criteria for Information Technology Security, утвержденный в 1999 году. В этом

стандарте подробно рассматриваются функциональные требования безопасности ИС – Security Functional Requirements и требования к адекватности реализации функций безопасности – Security Assurance Requirements.

По мере разработки этих международных стандартов и в условиях взрывного распространения ИТ на многие отрасли и сферы деятельности людей появилась концепция интегральной ИБ, в которой объединены средства и меры безопасности баз данных и коммуникаций (каналы передачи данных), безопасности информационных сетей и систем, безопасности применяемых программных продуктов и физической безопасности (помещений, аппаратных средств и людей).

Таким образом, к настоящему времени сформировались **три уровня обеспечения безопасности ИС:**

- индивидуальный – решением частной задачи защиты конкретной информационной системы;

- комплексный – решением совокупности частных задач по единой программе защиты ИС;

- интегральный – решением задачи безопасности конкретной ИС в комплексе, общими средствами защиты самой системы, ее баз данных и ПО, применяемых каналов связи.

При этом стандартный **набор средств защиты ИС** сейчас включает в себя:

- средства надежного и безопасного хранения информации,

- средства авторизации и защиты от несанкционированного доступа;

- средства защиты от внешних угроз при подключении к общедоступных сетям коммуникаций,

- средства защиты от вирусов,

- средства обеспечения целостности и подлинности информации,

- средства активного и непрерывного исследования защищенности информационных ресурсов,

- средства обеспечения централизации управления системой ИБ.

В соответствии с вышесказанным можно сделать вывод, что управление рисками и обеспечение информационной безопасности является важнейшим в развитии цифровой экономики.

ВОПРОСЫ ДЛЯ САМОКОНТРОЛЯ

1. Информационная безопасность как основа конкурентоспособности современного бизнеса.
2. Управление рисками и обеспечение информационной безопасности в условиях цифровизации экономики.
3. Стандарт Банка России СТО БР ИББС-1.3-2016 «Сбор и анализ технических данных при выявлении и расследовании инцидентов информационной безопасности при осуществлении переводов денежных средств».
4. Деятельность служб кибербезопасности государственных структур и частного бизнеса. Центр кибербезопасности Центрального Банка РФ.
5. Методики управления рисками в системе информационной безопасности.
6. ИТ-специалисты как ключевой ресурс в конкурентной стратегии фирмы.
7. Предупреждение и устранение угроз и рисков цифровой экономики, обеспечение безопасности информационной среды – основа конкурентоспособности гражданина, бизнеса и государства.