С.А. Прохоров, А.А. Федосеев, А.В. Иващенко

Автоматизация комплексного управления безопасностью предприятия

Самара 2008

УДК 681.3

Рецензенты:

декан механико-математического факультета
Самарского государственного университета,
заведующий кафедрой безопасности информационных систем
д.ф.-м.н., профессор В.И. Астафьев

генеральный директор ЗАО «Научно-производственная фирма
«СОНДАИНФО» д.т.н. Г.Я. Резников

Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация
комплексного управления безопасностью предприятия /
Самара: СНЦ РАН, 2008 – 55 с., ил.

ISBN 978-5-93424-364-8

Данное пособие предназначено для специалистов в области построения систем обеспечения безопасности предприятия и разработки и внедрения автоматизированных информационных систем, а также студентов специальностей «Автоматизированные системы обработки информации и управления», «Комплексное обеспечение информационной безопасности автоматизированных систем»

Печатается по решению издательского совета
Самарского научного центра Российской академии наук

ISBN 978-5-93424-364-8

Содержание

Введение

Управление современным предприятием непосредственным образом связано с решением двух задач: построения интегрированной информационной среды, которая содержала бы актуальные знания и осуществляла информационную поддержку всех этапов проектирования и производства, и обеспечения безопасности функционирования предприятия в смысле снижения рисков потери, порчи или разглашения информации, подлежащей защите.

Эти задачи являются одними из самых актуальных в настоящее время, благодаря высокому научно-техническому прогрессу в области автоматизации и информатизации производственных процессов. Так, следует отметить, что наряду с развитием новых средств технического обеспечения безопасности, появляются новые методы, алгоритмы и стандарты оценки качества функционирования информационных систем [1 – 5].

При этом традиционно развитие интегрированной информационной среды и средств обеспечения безопасности находятся в противодействии. Сохранения тенденции развития предприятия, активных взаимоотношений с партнерами довольно часто ограничивается с целью обеспечения безопасности. В связи с этим, необходимо определить методику взаимодействия различных подразделений предприятия при решении задач повышения эффективности и качества производства за счет совместного развития интегрированной информационной среды и системы обеспечения безопасности.

В случае, когда вся актуальная информация накапливается в едином информационном пространстве (ЕИП) предприятия, вероятность нарушения безопасности возрастает. С другой стороны, специалисты по обеспечению безопасности получают качественно новый инструмент обработки данных обо всех происходящих событиях.

В данном направлении можно выделить две основные задачи. Во-первых, необходимо внедрять новые методы и технологии мониторинга изменений знаний, накапливаемых в едином информационном пространстве предприятия. Эта система должна быть интегрирована с системами PDM/PLM, ERP, MES, другими автоматизированными системами и подсистемами предприятия, и предоставлять пользователям инструменты управления рисками.

Во-вторых, необходимо предусмотреть средство анализа действий в области обеспечения безопасности, которые позволили бы оп-

ределить баланс между силами, затраченными на устранение рисков и возможностями предприятия по развитию.

Поскольку объект исследования указанных задач постоянно меняется с течением времени, необходимо вместо независимых решений по построению интегрированной информационной среды и системы безопасности решать задачу динамического управления безопасностью и развитием интегрированной информационной среды предприятия как сложной системы.

Оценить допустимые риски в стратегии развития предприятия невозможно без детального и разностороннего изучения всех возможных угроз. На основе проведенного анализа должны быть выработаны мероприятия по снижению вероятности рисков и степени возможного ущерба. Эти мероприятия могут быть объединены в набор стратегий для оперативной поддержки принятия решений.

Определение величины рисков и набора мероприятий может осуществляться на основе экспертных оценок лиц, принимающих решение. Выбор между стратегиями, а также комбинирование стратегий, должно быть автоматизировано в системе поддержки принятия решений на основе событий, отражающихся в ЕИП предприятия.

В этом случае осуществляется переход от системы управления рисками к системе управления безопасностью, которая на основе данных о событиях, накопленных за определенный период, и сведений о результатах выполнения активированных мероприятий делает вывод о целесообразности и эффективности системы безопасности.

Работа такой системы управления с виртуальными данными позволяет строить системы анализа возможных ситуаций, моделировать наиболее вероятные события, в том числе ожидаемые атаки и проверять, насколько быстро работающая система безопасности способна реагировать на эти события и предотвращать вероятный ущерб.

Целью данной работы является определение основного направления работ по повышению эффективности управления безопасностью предприятия как сложной системой путем применения алгоритмов анализа рисков на основе мониторинга изменений единого информационного пространства предприятия.

Для достижения этой цели предлагается относительно новый подход, заключающийся в управлении безопасностью по результатам анализа виртуальных данных, накапливаемых в едином информационном пространстве предприятия.

Практическую значимость представляют информационно-логическая модель автоматизированной системы управления безопасностью предприятия, а также алгоритмическое и программное обеспечение этой системы.

Методики и рекомендации, изложенные в данном пособии, базируются на типовых требованиях и показателях качества функционирования информационных систем [2 – 4].

Описание предлагаемых алгоритмов и информационно-логической модели системы будем производить с использованием нотации UML [6 – 9].

Данное пособие содержит описание некоторых результатов, полученных в ходе выполнения опытно-конструкторской работы по теме «Разработка математической модели комплексной системы безопасности предприятия и программных средств мониторинга ее функционирования» объединенной группой сотрудников Самарского государственного аэрокосмического университета (СГАУ) и ГНПРКЦ «ЦСКБ Прогресс».

Авторы выражают благодарность за поддержку ректору Самарского государственного аэрокосмического университета, члену-корреспонденту РАН, профессору В.А. Сойферу, генеральному директору ГНПРКЦ «ЦСКБ Прогресс» д.т.н., профессору А.Н. Кирилину, первому заместителю генерального директора – генеральному конструктору ГНПРКЦ «ЦСКБ Прогресс» к.т.н. Р.Н. Ахметову

Авторы выражают признательность за помощь в реализации описанных идей старшему преподавателю кафедры информационных систем и технологий СГАУ В.Ф. Денисову и студентам факультета информатики СГАУ Д.А. Уланову, Л.В. Малыгиной, А.С. Свистунову, Д.В. Буренко.

1 Управление безопасностью на основе интеграции знаний

1.1 Обеспечение безопасности современного предприятия

Понятие «безопасность предприятия» подразумевает эффективное использование ресурсов, обеспечивающее стабильное функционирование предприятия в настоящем и устойчивое развитие в будущем. При теоретическом рассмотрении проблемы безопасности обычно используется следующий понятийный аппарат [3, 10]:

- враждебность – воздействие окружающей среды, направленное на предприятие, характеризующееся совокупностью угроз устойчивому функционированию предприятия;
- угроза – это изменения во внешней или внутренней среде субъекта, которые приводят к нежелательным изменениям предмета безопасности;
- риск – вероятность наступления вышеназванных нежелательных изменений;
- ущерб – это нежелательное качественное изменение предмета безопасности, снижение его ценности для субъекта или его полная утрата;
- стратегия безопасности – совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия;
- негативное событие – это любое незапланированное событие, результатом которого выступает материальный ущерб или моральный урон предприятию, и влекущее за собой убытки, дополнительные расходы предприятия.
- предзатраты (превентивные затраты) – затраты на разработку и реализацию мероприятий по предотвращению негативных событий;
- постзатраты – это затраты на ликвидацию последствий реализовавшихся негативных событий;
- общие затраты (стоимость мероприятий) – это затраты на обеспечение безопасности предприятия, представляющие собой сумму предзатрат и постзатрат;

Понятие безопасности предприятия неразрывно связано с такими понятиями как уязвимость и управляемость [10].

Уязвимость предприятия — это показатель, характеризующий степень его подверженности внешним и внутренним опасностям, т.е. степень его незащищенности. Уязвимость – это свойство любого материального объекта природы, техники или социума утрачивать способность к выполнению естественных или заданных функций в результате негативных воздействий опасностей определенного происхождения и интенсивности.

Управляемость предприятия — это комплексная характеристика его способности реагировать на целенаправленное воздействие. Предприятие представляет собой открытую систему, функционирующую в нестабильной окружающей среде.

Современные предприятия предъявляют достаточно высокие требования к средствам обеспечения своей безопасности. В частности, необходимо создание и поддержка функционирования единой системы контроля и обеспечения всех видов безопасности предприятия, включающей средства мониторинга, контроля и управления.

При этом необходимо рассматривать комплексную систему безопасности, которая охватывает все возможные виды методического, технического и организационного обеспечения мероприятий по противодействию угрозам нарушения функционирования предприятия и утечки охраняемой информации.

Система безопасности современного предприятия должна адекватно реагировать на разнообразные события, и развиваться одновременно с предприятием. Последнее означает, что на основе постоянного анализа изменений бизнес-процессов предприятия и внешних условий должна меняться и система безопасности.

Комплексное управление безопасностью предприятия включает в себя организацию мероприятий, направленных не только на охрану информации, но и на защиту всех бизнес-процессов предприятия. Например, безопасность предприятия подразумевает обеспечение сохранности документов (электронных, бумажных и других), обеспечение контроля доступа на предприятие, противодействие кражам и порче изделий, материалов и оборудования и т.п.

В связи с этим, автоматизация управления комплексной безопасностью предприятия заключается не только в обеспечении информационной безопасности, но и в информационной поддержке всех мероприятий, в том числе и никоим образом не связанных с использованием информационных технологий.

На наш взгляд суть автоматизации комплексного управления безопасностью состоит в централизации, то есть создании единой системы поддержки принятия решений.

При этом требуется решить две задачи. Во-первых, необходимо обеспечить централизованное накопление и постоянное обновление актуальных знаний обо всех бизнес-процессах предприятия. Во-вторых, нужно организовать обработку этой информации в автоматическом или автоматизированном режиме и генерирование возможных управляющих воздействий.

Для решения первой задачи предлагается использовать единое информационное пространство предприятия. Отметим несколько аспектов, связанных с управлением безопасностью в этом контексте.

Организация единого информационного пространства в соответствии с современными тенденциями развития информационных технологий состоит в интеграции всех информационных ресурсов предприятия. При этом происходит внедрение автоматизированных систем с различной функциональностью, разработка нового программного обеспечения и активное использование современных информационных технологий на предприятии.

С точки зрения подразделения по обеспечению безопасности, риски возникают

- в связи с активным использованием нового аппаратного и программного обеспечения, безопасность которого в смысле отказоустойчивости и защиты информации часто недостаточно исследована и обоснована,
- в связи с необходимостью организации совместных работ со сторонними организациями, поставляющими это аппаратное и программное обеспечение,
- а также, в связи с централизованным накоплением информации, подлежащей защите, в электронном виде.

Таким образом, возникает задача комплексного управления безопасностью *в условиях* организации единого информационного пространства. Решению ее посвящено достаточно много работ, например [11].

С другой стороны, знания о безопасности предприятия являются неотъемлемой частью единого информационного пространства. В связи с этим, новые технологии хранения данных и их аналитической обработки весьма востребованы и в подразделениях современных предприятий, занимающихся управлением безопасностью.

Однако, с учетом характера этой информации и связанных с ее обработкой процессов, внедряемое для организации этой части единого информационного пространства программное обеспечение должно удовлетворять особым требованиям по обеспечению надежности хранения и защиты информации о системе безопасности предприятия.

Последний, но на наш взгляд, наиболее функционально нагруженный аспект современной автоматизации управления безопасностью – это использование единого информационного пространства в качестве источника актуальной информации для системы поддержки принятия решений.

Современные стандарты по автоматизации предприятия предписывают сохранение актуальной информации обо *всех* бизнес-процессах предприятия. В этих условиях единое информационное пространство является источником достоверной актуальной информации, который должен активно использоваться службой безопасности для информационной поддержки своей деятельности.

Например, в случае сохранения в едином информационном пространстве данных о доступе на предприятие и к охраняемым документам, можно проводить анализ рисков, связанных с утечкой охраняемой информации. В случае поступления информации со складов и проходных предприятия можно анализировать сведения о пропаже изделий и противодействовать кражам. А в случае сохранения данных с датчиков противопожарной сигнализации и сведений о проводимых профилактических работах, можно идентифицировать наиболее пожароопасные участки производства.

Отметим, что позиционируемая комплексность управления безопасностью предприятия базируется на анализе информации обо всех процессах, то есть соответствует современным тенденциям хранения знаний в едином информационном пространстве.

Описанные выше аспекты построения такой системы управления безопасностью приводят к необходимости формулирования новых требований к методам организации единого информационного пространства и используемому аппаратному, программному и информационному обеспечению.

Эти требования включают кроме обеспечения надежности и защиты информации, необходимость сохранения в едином информационном пространстве данных, используемых при анализе рисков и информационной поддержке деятельности подразделения безопасности.

1.2 Использование единого информационного пространства при организации управления безопасностью

Организация мероприятий по обеспечению безопасности современного научно-производственного предприятия осуществляется в условиях сложившегося на этом предприятии единого информационного пространства.

Требования к организации управления предприятием в обязательном порядке включают необходимость комплексной автоматизации жизненного цикла изделия, что является одним из необходимых средств обеспечения эффективности процессов. При этом жизненный цикл изделия включает в себя проектирование, технологическую подготовку производства, обеспечение необходимыми ресурсами, сбыт готовой продукции, и другие стадии.

Современный подход к комплексной автоматизации предприятия [12, 13] заключается в организации единого информационного пространства (ЕИП), которое обеспечивает информационную поддержку всех этапов жизненного цикла изделия. Единое информационное пространство – специальным образом организованное хранилище данных, в котором каждое приложение может на основе уже существующей общедоступной информации создавать новые данные, доступные другим элементам системы.

Единое информационное пространство предприятия включает в себя информацию о продуктах, процессах и ресурсах, которая совместно используется всеми специалистами предприятия в ходе коллективной работы, а значит, может использоваться в качестве исходного материала для системного анализа безопасности предприятия.

Под продуктом в данном случае подразумевается любое изделие, изготавливаемое предприятием, независимо от того, является оно изделием основного производства, то есть продукцией предприятия, или изделием вспомогательного производства, то есть продукцией технологической подготовки производства.

Под процессом подразумевается последовательность действий, связанных с функционированием системы подготовки и обеспечения производства. Как и в случае описания продукта, технологические процессы могут быть представлены описанием их структуры и соответствующей документации.

Под ресурсом подразумеваются различные виды обеспечения, используемые при выполнении бизнес-процессов К таким видам обеспечения можно отнести:

– кадровый ресурс – включает отделы, службы и цеха предприятия, их сотрудников и специалистов;
– производственный ресурс – включает используемое технологическое оборудование, различные виды оснастки и инструмента;
– материальный ресурс – включает используемые материалы, стандартные и покупные изделия;
– информационный ресурс – включает используемые при выполнении бизнес-процессов справочно-информационные материалы;
– обеспечивающий ресурс – включает дополнительные виды обеспечения для поддержки функционирования предприятия, такие как архивы, находящиеся в ведении служб технической документации предприятия.

Для создания комплексных систем поддержки жизненного цикла изделий (разработка – производство – эксплуатация - утилизация) широко используется концепция CALS (Continuous Acquisition and Life cycle Support – непрерывное развитие и поддержка жизненного цикла), направленная в первую очередь на повышение эффективности управления информационными ресурсами предприятия. Эта концепция реализована в специфическом классе информационных технологий, поддерживаемых международными стандартами [12 – 15].

Согласно концептуальным положениям CALS, реальные бизнес-процессы находят отображение в виртуальной информационной среде, в которой определение продукта представлено в виде полного электронного описания изделия, а среда его создания и среда эксплуатации – в виде систем моделирования процессов и их реализации. Все три составляющие (определение продукта, среда его создания и среда эксплуатации) не только взаимосвязаны, но и непрерывно развиваются на всем протяжении жизненного цикла продукта.

Реализация концепции CALS производится путем построения интегрированной информационной среды на основе одного комплекса программно-информационного обеспечения, или, что более распространено в настоящее время, путем интеграции различного программного обеспечения. Прим этом ключевой задачей такой интеграции является объединение функциональности ERP (Enterprise Resource Planning – Управление ресурсами предприятия) и PLM (Product Life-cycle Management – Управление жизненным циклом продукта) систем.

При этом создается единая информационная среда, реализуемая средствами этих систем и обеспечивающая совместную, согласован-

ную работу конструкторов, технологов и других специалистов, которая содержит полное и соответствующее действительности описание деятельности предприятия.

В данной работе подразумевается, что единое информационное пространство содержит знания не только об основных процессах, непосредственно связанных с жизненным циклом изделия, но обо всех процессах предприятия, в том числе управленческих и вспомогательных.

Обычно при построении системы безопасности предприятия действия по обеспечению хранения и обмена данными воспринимаются как источник риска возможной утечки информации. Связано это с высоким прогрессом современной вычислительной техники, опережающим развитие средств обеспечения безопасности. Этот факт также обуславливает необходимость внедрения в единое информационное пространство средств анализа информационных потоков и определения возможных рисков и угроз.

Таким образом, единое информационное пространство позволяет обеспечить кооперативное взаимодействие различных служб предприятия при решении задач повышения эффективности и качества производства за счет совместного развития интегрированной информационной среды. В состав этих служб входит и служба безопасности.

Взаимодействие субъектов обеспечения функционирования ЕИП предприятия в системе управления безопасностью приведено на рис. 1. Здесь выделены компоненты единого информационного пространства, обеспечивающие конструкторско-технологическую подготовку производства и управление процессами и ресурсами. Данные компоненты составляют общепринятую структуру ЕИП предприятия, которая широко применяется в машиностроении.

Сложность такой структуры заключается в необходимости поддерживать различные по своей природе этапы жизненного цикла изделия, от проектных работ, связанных с коллективной обработкой большого количества информации и инновационной деятельностью, до управления материально-техническим обеспечением производственных процессов, связанного с решением задачи оптимального использования ресурсов при множественных критериях и ограничениях.

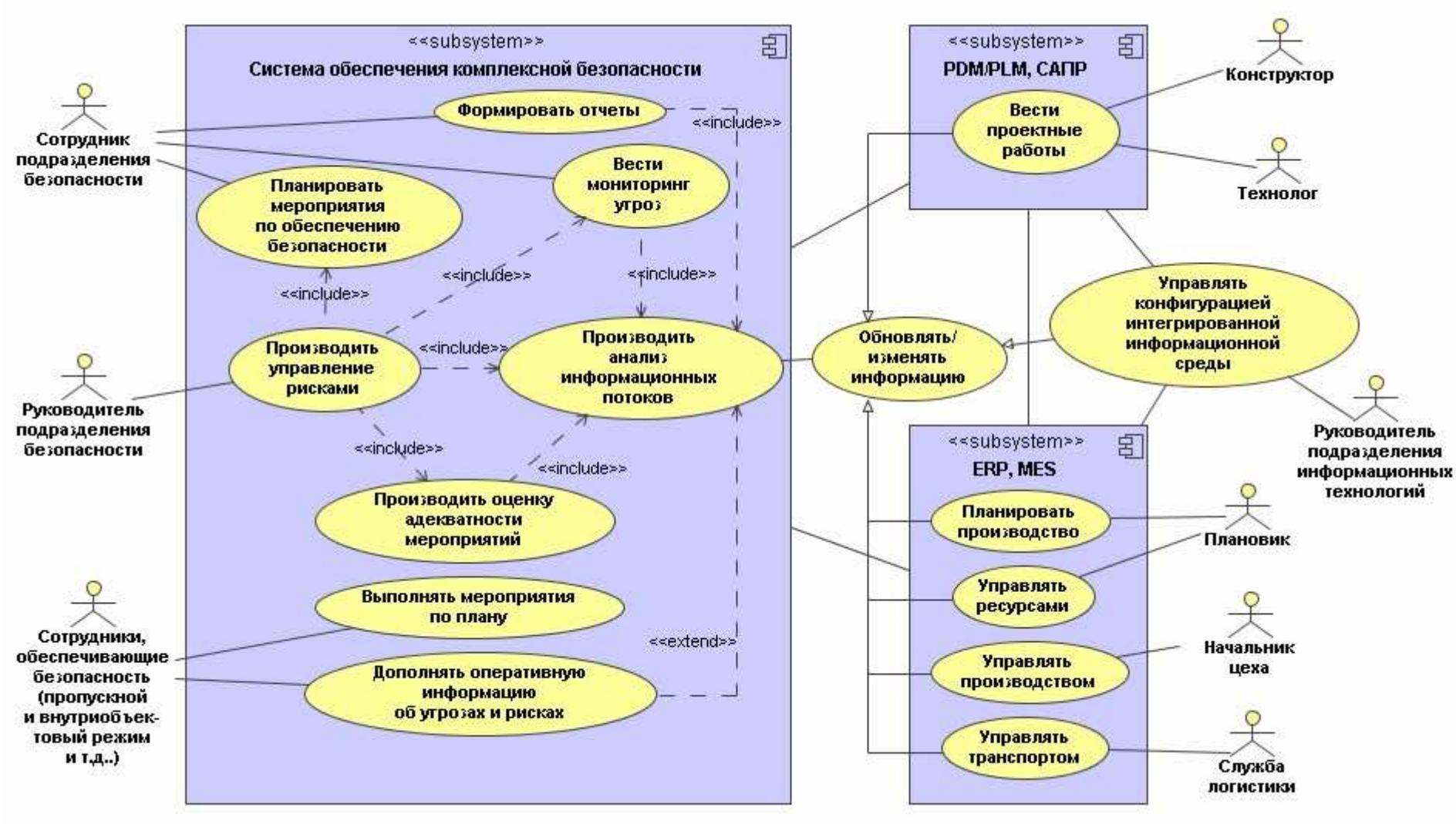

Рис. 1. Управление безопасностью предприятия

Поскольку у этих процессов разный характер, различаются и задачи по обеспечению безопасности при их организации. Действительно, если при организации документооборота основной акцент следует делать на снижении вероятности утечки защищаемой информации, производственный процесс в большей степени требует обеспечения контроля качества изделий.

Тем не менее, все этапы жизненного цикла изделия схожи в том смысле, что могут быть представлены в имитационной модели в виде последовательных преобразований некоторых информационных объектов. При этом объединяющим и сохраняющим знания об этих информационных объектах является единое информационное пространство.

В связи с этим, на описываемой диаграмме можно выделить цепочку взаимосвязанных вариантов использования: обобщенная функциональность по обновлению и изменению информации, которая используется всеми участниками основного бизнес-процесса и управления руководителем отдела информационных технологий посредством конфигурирования интегрированной информационной среды предприятия, позволяет отслеживать информационные потоки предприятия и управлять рисками по нарушению безопасности.

Структура ЕИП предприятия, соответствующая описанным прецедентам, приведена на рис. 2. Отметим, что современное ЕИП является динамично меняющейся сложной системой [16]. Причем изменения могут касаться не только логической структуры этого взаимодействующих сущностей, но и конфигурации программного обеспечения их существования.

Наиболее узким местом в данном случае является интеграция подсистем с различающимся поведением, которые могут работать на разных платформах. При этом весьма сложным является обеспечение адаптивного характера функционирования системы управления безопасностью.

Решить эту проблему можно, унифицировав форму хранения знаний, которые использует система управления безопасностью. Все объекты жизненного цикла изделия можно представить в виде совокупности информационных объектов, природа которых не определяет общих механизмов организации режима безопасности.

Согласно поставленной выше задаче для информационной поддержки системы управления безопасностью, в ЕИП нужно обеспечить хранения сведений о следующих основных сущностях:

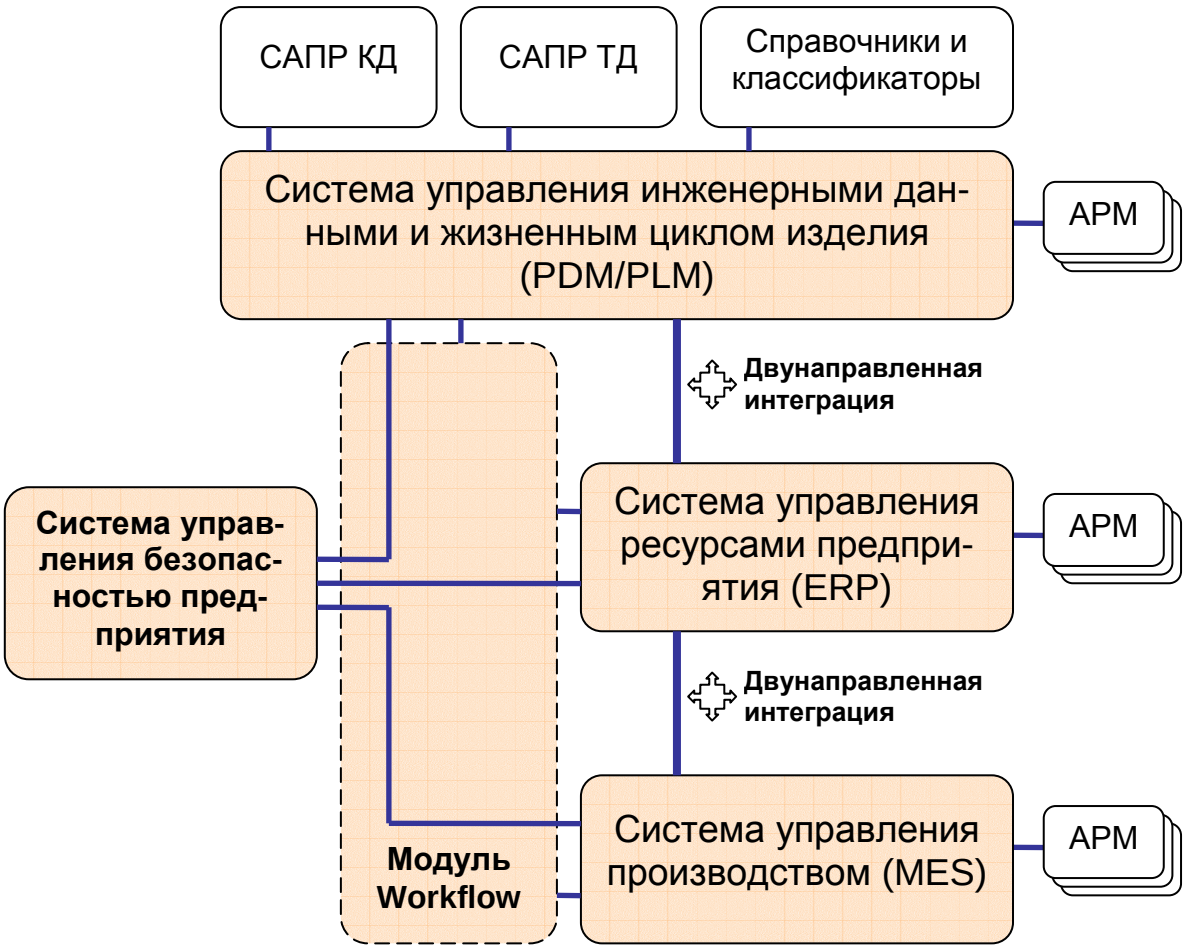

Рис. 2. Структура единого информационного пространства

– Информационные объекты: абстрактное описание любых продуктов или процессов жизненного цикла изделия, для которых законодательно, в ходе экспертной оценки или в результате статистического анализа определены специфические требования по безопасности. В идеальном случае информационные объекты представляют собой полное отображение всех хранимых знаний в PLM и ERP системах.
– Риски: количественно описывают угрозы. Риск предлагается представить в виде пары значений: вероятности возникновения ущерба и величины ущерба в условных единицах.
– Мероприятия фактически отражают действия, осуществляемые предприятием для снижения или устранения выявленных рисков. Мероприятие характеризуется стоимостью и эффективностью в смысле снижения вероятности риска или величины ожидаемого ущерба.

Описанные выше концепции образуют понятийный аппарат в виде четырех объектов: «угроза», «риск», «мероприятие», «преграда», достаточный для построения системы управления безопасно-

стью. Угроза представляет собой возможное причинение ущерба предприятию, риск количественно (или качественно) описывает угрозу и служит для оценки безопасности предприятия.

Изменять безопасность можно путем активации мероприятий, а отслеживать изменения – путем анализа значения рисков. Активация мероприятий имеет результат в виде устанавливаемых преград возможным угрозам. Такой подход в своей основе имеет предположение об инициативном характере возникновения угроз, то есть о том, что угрозы возникают в результате деятельности человека.

Эта деятельность может быть сознательная или случайная, она может быть направлена на изменение процессов предприятия, или сама по себе являться частью или результатом таких процессов. Весьма важно определить, что источник угроз безопасности предприятия неотделим от самой деятельности предприятия – часто это не внешняя сила, генерирующая события вне системы проектирования и производства, а некоторое возмущающее воздействие, источник хаотического состояния, возникающий внутри предприятия как сложной системы.

Отметим, что под управлением безопасностью фактически понимается управление процессами проектирования и производства, то есть изменение логики выполнения процессов, создание новых процессов и корректировка старых в результате проводимых мероприятий.

Однако для обоснования управленческих решений и оценки их эффективности в силу сложности бизнес-процессов предприятия используются оценки рисков.

Алгоритмы работы с указанными понятиями определены в разделе 2, здесь же опишем основные механизмы хранения информации, необходимой для работы этих алгоритмов в едином информационном пространстве. Общая схема взаимосвязи указанных сущностей показана на диаграмме сущностных классов в нотации UML (см. рис. 3).

Следует отметить следующие особенности этой схемы. Так, для обеспечения сохранности информации и требуемого уровня ответственности необходимо поддержка версионности.

Для информационных объектов определены риски и мероприятия по их устранению, при этом каждое мероприятия при применении к заданному риску должно снижать связанный с его наступлением ущерб или вероятность его возникновения.

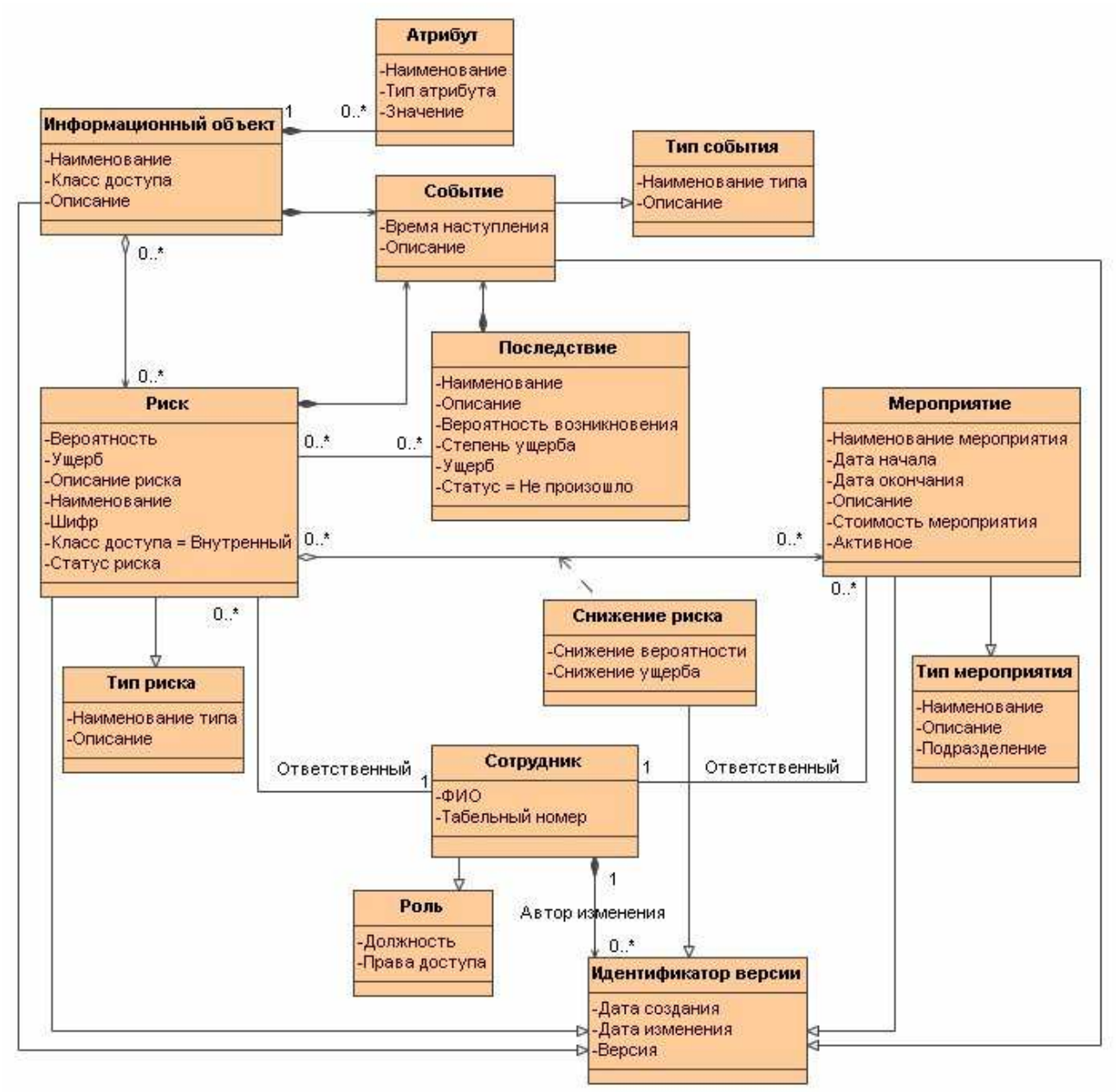

Рис. 3. Диаграмма сущностных классов системы управления безопасностью

Отметим, что классификация информационных объектов является отдельной задачей, частный случай которой – отнесение документов к разным классам конфиденциальности. Эта задача может быть решена путем введения справочника ключевых слов, описывающих тему, относящуюся к заданному режиму конфиденциальности и в случае высокого процента нахождения ключевых слов заданной группы, системы может выделять информационные объекты, потенциально относящиеся к данной группе конфиденциальности.

Список возможных мероприятий задается вручную. Коэффициенты снижения вероятности ли ущерба рисков задаются экспертным путем. Назначение мероприятий может быть автоматизировано в

случае определение механизма их запуска (например, в зависимости от показателей риска при достижении ими критических значений, могут запускать антикризисные мероприятия).

Необходимо также вести учет последствий рисков, причем последствия должны быть указаны в момент определения риска для более точной оценки его параметров.

В целом, риск имеет достаточно простую схему состояний (см. рис. 4). Отметим, что риск может быть закрыт в случае его устранения, либо срабатывания. Обобщенная архитектура системы управления безопасностью предприятия приведена на рис. 5, где ESB (Enterprise Service Bus) представляет собой инструмент информационной интеграции подразделений предприятия по передаче данных.

При построении системы безопасности предприятия необходимо обеспечить управление рисками, а именно: определить риски, выработать мероприятия по снижению рисков и создать такую систему безопасности, при которой риски будут находиться в приемлемом (допустимом) состоянии.

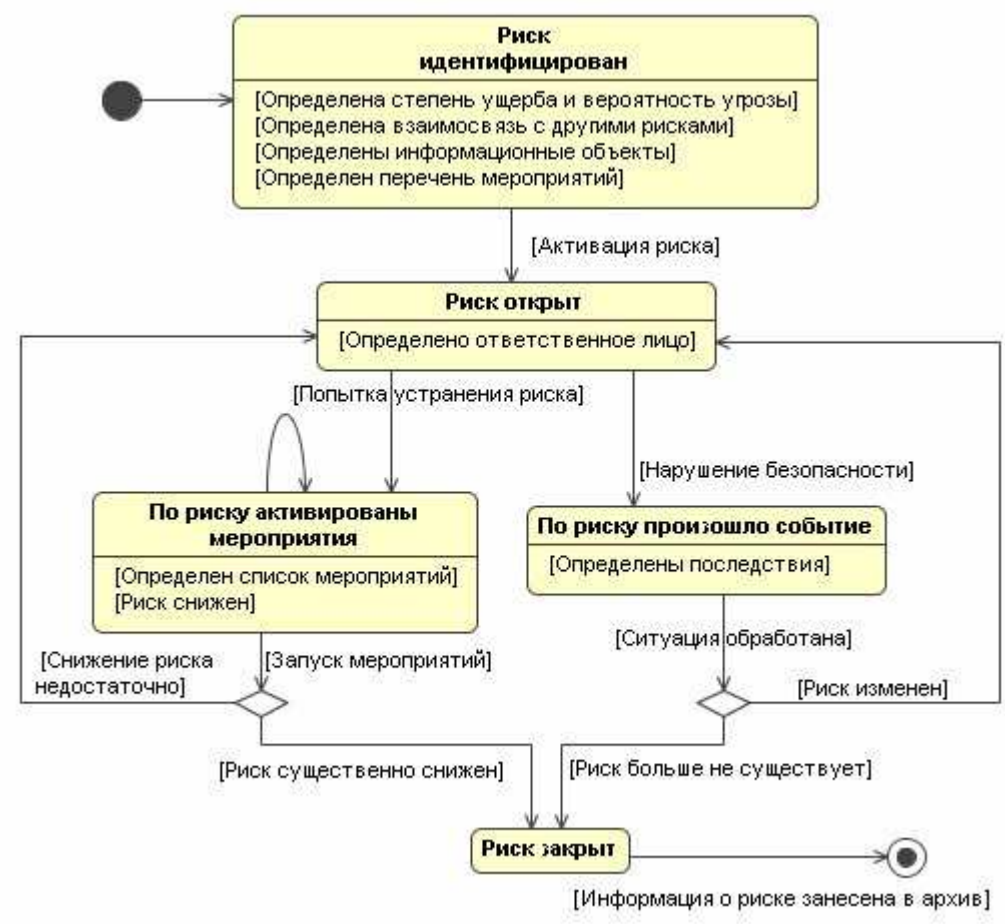

Рис. 4. Состояния риска

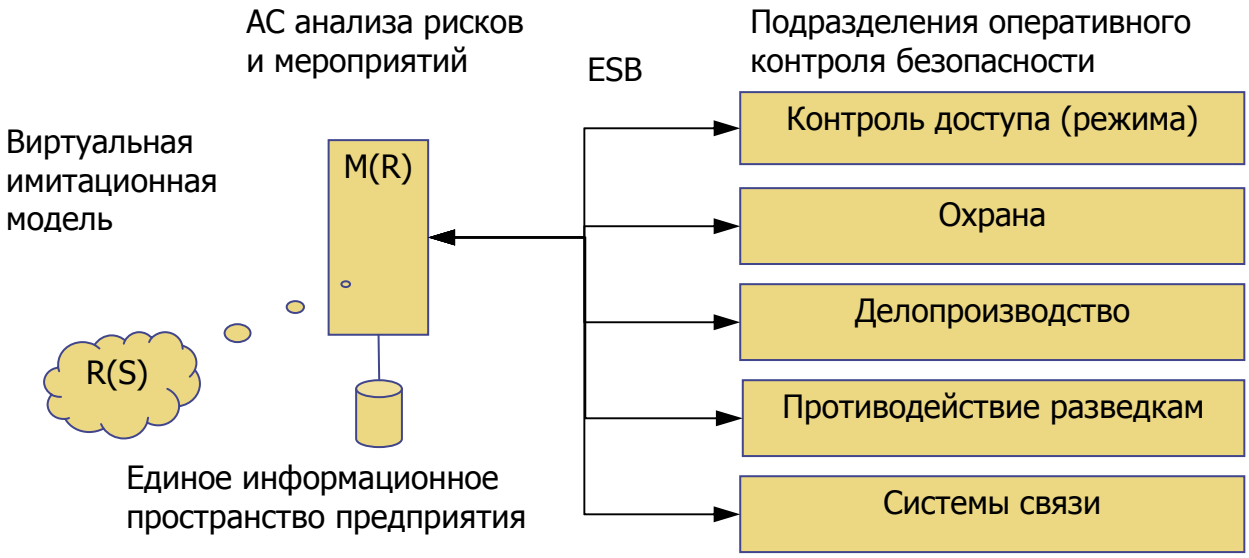

Рис. 5. Обобщенная архитектура системы управления безопасностью предприятия

Управление безопасностью в данном контексте будет заключаться в диагностировании отклонения одного или нескольких рисков от допустимого состояния и выработки реакций на это отклонение, то есть запуск резервных мероприятий, направленных на возвращение риска в допустимые пределы.

Отметим, что действие мероприятий не обязательно должно быть симметричным. Внешнее воздействие может иметь непрерывный или периодический характер. В этом случае мероприятие должно обеспечить компенсацию продолжения действия по увеличению риска.

Определить величину такого противодействия достаточно сложно. В связи с этим более целесообразным при увеличении одного из показателей риска (вероятности или величины ущерба) производить компенсирующее воздействие на второй показатель соответственно.

Например, в случае увеличения вероятности риска более чем на допустимую величину, может быть целесообразно перераспределение информации таким образом, чтобы уменьшился ущерб. Такое противодействие может быть более эффективно, чем выполнения мероприятий по противодействию увеличению вероятности.

Решить эту задачу достаточно сложно, поскольку требуется производить анализ всей ситуации по безопасности предприятия в целом. Результаты комбинированного анализа рисков в данном случае не позволят количественно оценить общую ситуацию по обеспечению безопасности предприятия.

В связи с этим в дополнение к описанному выше управлению рисками можно предложить модель, основанную на анализе интегрированных показателей безопасности предприятия.

Можно выделить три основных направления развития предприятия. Безопасность предприятия может быть выражена в условных единицах возможного ущерба, отнесенного к вероятности возникновения выявленных рисков. Безопасность можно считать высокой, когда риски и ущерб находятся в допустимых пределах и низкой в случае существования риска или набора рисков с высокой вероятностью наступления. При оценке безопасности таким образом можно использовать модель управления рисками.

Поскольку обеспечение высокой безопасности производится путем ввода в действие некоторого набора мероприятий, безопасность также может условно характеризоваться суммарной стоимостью всех мероприятий, выполняемых для устранения рисков.

В случае, когда стоимость мероприятий не имеет четкого денежного выражения, возможно определение некоторой виртуальной стоимости, позволяющей в рамках предприятия сравнивать мероприятия по временным затратам и количеству востребованных для его проведения ресурсов.

Отметим, что мероприятия могут иметь отложенный эффект, когда затраты на их проведение производятся ранее (или позднее), чем воздействие этих мероприятий на риски. Однако в рамках рассматриваемой проблемы такое расхождение по времени влияет лишь на своевременность диагностирования момента применения нужного управления, то есть вносят вклад в методическую погрешность.

Показатели безопасности и ее стоимости не полностью описывают направления развития предприятия. При построении равновесия между двумя этими показателями всегда ключевым является безопасность, а стоимость мероприятий является лишь ограничением.

В связи с этим следует выделить еще один показатель, характеризующий развитие предприятия – адаптивность. Этот показатель описывает возможности развития предприятия; он также находится в конфликтном противодействии безопасности, так как подразумевает применение самых новых технологий, открытости и модифицируемости производственных процессов. Вообще, эта характеристика присуща всем сложным системам [17].

Действительно, высокий показатель адаптивности свидетельствует о гибкости производственных процессов, частоте переходных

периодов. С одной стороны, он позволяет добиться новых результатов, пересмотреть цели и задачи предприятия, провести реинжиниринг бизнес-процессов. С другой стороны, большое количество случайных изменений, присущих адаптивным предприятиям, и связанных с ошибками в управлении, недостаточными знаниями о новых внешних условиях, невозможности четко координировать всю деятельности и держать ее под полным контролем и т.п., могут легко привести к хаосу и разрушению и, следовательно, противоречат требованиям по безопасности предприятия.

Аналогичным образом можно трактовать адаптивность и с точки зрения определения доступа к информации. Привлечение большого количества пользователей информации позволяют повысить эффект инновационной деятельности. С другой стороны, лавинообразно увеличивается вероятность утечки информации, а главное, теряется контроль над ее использованием, так как сама информация имеет свойство необратимо и неконтролируемо тиражироваться.

Использование указанных трех параметров (безопасность, стоимость и адаптивность) для определенной выше задачи позволяет производить анализ текущей деятельности предприятия. Мониторинг изменения этих параметров, определение скорости этих изменений, позволяет сделать вывод о необходимости усиления или ослабления мероприятий не в качестве ответной реакции на возможные угрозы, а с точки зрения стратегических целей предприятия.

Например, если требуется обеспечить контролируемые изменения бизнес-процессов предприятия, возможно повышение показателя адаптивности, что приведет к понижению безопасности в требуемых рамках и позволит изменить бюджет в пользу реинжиниринга бизнес-процессов предприятия. Однако по истечению выделенного времени возможно включение механизмов восстановления безопасности, возможно с учетом сделанных изменений.

Главный эффект от такого анализа состоит не столько в формализации процесса управления безопасностью, сколько в обеспечении подконтрольности случайных воздействий, неизбежных при реинжиниринге бизнес-процессов. Анализ целесообразности мероприятий и комплексный характер их применения позволит обеспечить требуемый уровень безопасности даже в режиме повышенной нагрузки на предприятие в целом и систему безопасности в частности в случае освоения новых видов производств, внедрения новых технологий, опытной деятельности и т.п.

2 Алгоритмы управления безопасностью

В данном разделе описаны основные алгоритмы комплексного управления безопасностью предприятия, использующие для поддержки принятия решений единое информационное пространство предприятия. Вначале приведены основные теоретические сведения, необходимые для построения системы управления безопасностью, далее описан собственно алгоритм управления безопасностью на основе анализа рисков.

2.1 Классификация угроз

В настоящее время на большинстве предприятий информация, представляющая собой государственную или коммерческую тайну, находится на бумажных или машинных носителях и может передаваться по телефону, телефаксу, телексу, обрабатываться, храниться и передаваться средствами вычислительной техники, записываться и воспроизводиться с использованием современного оборудования. Наконец информация присутствует в воздушной среде в виде акустических сигналов при переговорах [10].

Нанесение ущерба предприятию может быть произведено физическими воздействиями стихийных природных явлений, не зависящих от человека. В этом случае можно использовать достаточно распространенный инструмент теории игр и статистического анализа.

Однако более широк и опасен круг искусственных угроз, вызванных человеческой деятельностью, среди которых, исходя из мотивов, можно выделить [10]:

- неумышленные (непреднамеренные) угрозы, вызываемые ошибками в проектировании и при производстве, в действиях обслуживающего персонала, программного обеспечения, случайными сбоями в работе средств вычислительной техники и линий связи, энергоснабжения, воздействием на аппаратуру физических полей и т.д.;
- умышленные (преднамеренные) угрозы, обусловленные несанкционированными действиями сотрудников предприятия и несанкционированным доступом к информации посторонних лиц.

Результатом реализации угроз нарушения безопасности может быть: утрата (разрушение, уничтожение), утечка (извлечение, копирование, подслушивание), искажение (модификация, подделка) или блокирование.

Наиболее типичной естественной угрозой системам обработки данных, не всегда связанной с деятельностью человека, является пожар. Поэтому при проектировании и эксплуатации систем обработки данных в обязательном плане решаются вопросы противопожарной безопасности. Особое внимание при этом следует уделить защите от пожара носителей компьютерных данных, файл-серверов, отдельных вычислительных машин, центров связи, архивов, и другого оборудования и помещений. Для этих целей могут быть использованы специальные несгораемые сейфы, контейнеры и др.

Другая угроза для систем обработки данных в компьютерных системах – удары молнии. Эта проблема возникает не часто, но ущерб может быть нанесен очень большой. Причем ущерб не столько материальный, связанный с ремонтом или заменой вышедшей из строя техники и восстановлением потерянной информации, циркулирующей в компьютерных сетях, но прежде всего, если не применены необходимые технические меры защиты от мощных электромагнитных излучений грозовых разрядов, выходят из строя отдельные рабочие станции или серверы сети, и на значительное время парализуется работа объекта [10].

Для зданий, где размещаются технические средства обработки информации, расположенных в долинах рек или на побережье, весьма вероятной угрозой является затопления. В этих случаях аппаратные средства не должны устанавливаться на нижних этажах зданий и должны приниматься другие меры предосторожности. Нанесение ущерба ресурсам систем обработки данных может также быть вызвано землетрясениями, ураганами, взрывами газа и т.д. Ущерб может быть нанесен при технических авариях, например, при внезапном отключении электропитания и т.д.

Угрозы, связанные с деятельностью человека можно разделить на:

- угрозы системе обработки информации в результате несанкционированного использования штатных технических и программных средств, а также их хищения, порчи, разрушения;
- угрозы использования специальных средств, не входящих в состав системы обработки данных (побочные излучения, наводки по цепям питания, использование аппаратуры звукоусиления, прием сигналов из линий связи, акустические каналы);
- угрозы использования специальных методов и технических средств (фотографирование, электронные закладки, разрушающие

или искажающие информацию, а также передающие обрабатываемую или речевую информацию);
- облучение технических средств зондирующими сигналами, в результате чего может происходить искажение или разрушение информации, а при значительной мощности облучений и вывод из строя аппаратуры.

К числу наиболее вероятных каналов утечки охраняемой информации относят следующие:
- совместную деятельность с другими предприятиями;
- проведение переговоров;
- экскурсии и посещения предприятия;
- рекламу, публикации в печати, интервью для прессы;
- консультации специалистов со стороны, получающих доступ к документации и производственной деятельности;
- фиктивные запросы о возможности работы, заключения с ней сделок, осуществления совместной деятельности;
- рассылку отдельным сотрудникам различных анкет и вопросников под видом научных или маркетинговых исследований;
- частные беседы с сотрудниками предприятия, навязывание им незапланированных дискуссий по тем или иным проблемам.

Анализ системы защиты государственной, служебной и коммерческой тайны, моделирование вероятных угроз позволяет намечать дополнительные меры безопасности. При этом степень их целесообразности определяется достаточно просто: затраты на обеспечение надлежащей секретности должны быть существенно меньше, чем возможный экономический ущерб.

Ключевыми фигурами систем защиты охраняемых сведений являются сотрудники предприятия, причем не только те, которые работают с закрытой информацией. Рядовой сотрудник, не имеющий доступа к этим сведениям, тоже может оказать помощь конкурентам в проведении электронного шпионажа, обеспечить условия для хищения носителей информации, для выведывания, снятия копий [10].

Таким образом, персонал предприятия является, с одной стороны, важнейшим производственным ресурсом, а с другой, отдельные сотрудники в силу различных обстоятельств могут стать источником крупных потерь. Именно поэтому организационные и административные меры защиты закрытой информации необходимо сочетать с социально-психологическими мерами.

Среди социально-психологических мер защиты выделяют два основных направления: это, во-первых, правильный подбор и расстановка кадров и, во-вторых, использование материальных и моральных стимулов.

Управление удовлетворением и мотивацией сотрудников позволяет обеспечить режим работы, основанный на сотрудничестве и взаимодействии. Это существенно влияет на безопасность предприятия.

Во-первых, создавая условия для удовлетворения сотрудником его потребностей в самореализации способностей и потенций, в общественном признании его значимости, можно в рамках предприятия установить благоприятный социально-психологический климат, максимально снизить текучесть кадров. В такой обстановке маловероятно появление работника, пытающегося самоутвердиться путем передачи конкурентам секретов [10].

Во-вторых, такой подход позволяет правильно организовать режим работы с данными единого информационного пространства, обеспечить соблюдение требований по безопасности на всех этапах жизненного цикла изделия и инициировать действия по взаимному контролю использования информации.

В связи с этим, следует использовать любую возможность для пропаганды программ обеспечения безопасности предприятия; вознаграждать сотрудников предприятия за успехи в этой работе; стимулировать участие сотрудников предприятия в реализации программ обеспечения секретности.

2.2 Каналы утечки информации

Возможные каналы утечки информации можно разбить на четыре группы.

Первая группа – каналы, связанные с доступом к элементам системы обработки данных, но не требующие изменения компонентов системы. К этой группе относятся каналы образующиеся за счет дистанционного скрытого видеонаблюдения или фотографирования; применения подслушивающих устройств; перехвата электромагнитных излучений и наводок и т.д.

Вторая группа – каналы, связанные с доступом к элементам системы и изменением структуры ее компонентов. Ко второй группе относятся:

– наблюдение за информацией с целью ее запоминания в процессе обработки;
– хищение носителей информации;
– сбор производственных отходов, содержащих обрабатываемую информацию;
– преднамеренное считывание данных из файлов других пользователей;
– чтение остаточной информации, т.е. данных, остающихся на магнитных носителях после выполнения заданий;
– копирование носителей информации;
– преднамеренное использование для доступа к информации терминалов зарегистрированных пользователей;
– маскировка под зарегистрированного пользователя путем похищения паролей и других реквизитов разграничения доступа к информации, используемой в системах обработки;
– использование для доступа к информации возможностей обхода механизма разграничения доступа, возникающих вследствие несовершенства общесистемных компонентов программного обеспечения (операционных систем, систем управления базами данных и др.) и неоднозначностями языков программирования применяемых в автоматизированных системах обработки данных.

Третья группа, к которой относятся:
– незаконное подключение специальной регистрирующей аппаратуры к устройствам системы или линиям связи (перехват модемной и факсимильной связи);
– злоумышленное изменение программ таким образом, чтобы эти программы наряду с основными функциями обработки информации осуществляли также несанкционированный сбор и регистрацию защищаемой информации;
– злоумышленный вывод из строя механизмов защиты.

Четвертая группа, к которой относится несанкционированное получение информации путем подкупа или шантажа должностных лиц соответствующих служб и получение информации путем подкупа и шантажа сотрудников, знакомых, обслуживающего персонала или родственников, знающих о роде деятельности.

2.3 Оценка и управление рисками

Анализ рисков является наиболее важной частью комплексной оценки безопасности предприятия. Риск описывает вероятный ущерб,

который зависит от защищенности системы, и характеризуется парой значений: вероятность ущерба и величина ущерба в условных единицах. На выходе процедура анализа риска можно получить либо количественную оценку рисков, либо качественную (уровни риска; обычно: высокий, средний, низкий).

Существует несколько подходов к анализу рисков: обычно условно выделяется анализ рисков базового и полного уровня. Для анализа рисков базового уровня достаточно проверить риск невыполнения требований общепринятого стандарта безопасности (например, ISO 17799) с получением на выходе качественной оценки уровня рисков (высокий, средний, низкий).

Основное отличие полного анализа рисков от базового состоит в необходимости построения полной модели анализируемой системы. Модель должна включать: виды ценной информации, объекты ее хранения; группы пользователей и виды доступа к информации; средства защиты (включая политику безопасности), виды угроз. После моделирования необходимо перейти к анализу защищенности построенной полной модели информационной системы.

Управление рисками заключается в снижении вероятности или последствий воздействия событий, которые могут явиться причиной изменений качества, затрат, сроков или технических характеристик производственных процессов предприятия. В ходе управления рисками производится установление, оценка, анализ и контроль рисков, возникающих в течение полного жизненного цикла системы, а также выработка ответных мероприятий по обеспечению безопасности.

При управлении проектом или системой необходимо определить и классифицировать риски, количественно оценить вероятности и последствия возникновения рисков, установить статус и стратегию по обработке каждого из рисков, и обеспечить принятие соответствующих мер в случае в случае, если риск вышел за допустимые пределы.

При осуществлении процесса управления рисками предприятие должна осуществлять следующие действия в соответствии с проводимой ею политикой:

– установить системный подход к определению рисков, их оценке и управлению (определение событий, которые отрицательно влияют на систему, проект или организацию; классификация рисков; выбор методов оценки с учетом качества, затрат, сроков или технических характеристик системы);

– определять множество угроз возникновения рисков (исходные события, связанные с каждым риском, взаимосвязи между источниками рисков);
– определять вероятностные выражения рисков и возможные последствия рисков, используя установленные критерии;
– устанавливать приоритеты рисков в зависимости от вероятностных значений и возможных последствий;
– определять стратегии по управлению рисками;
– определять допустимые значения для каждого из установленных рисков;
– устанавливать меры безопасности в случае, если допустимые границы рисков нарушены;
– информировать о мерах безопасности, их логике и в статусе в соответствии с политикой предприятия;
– вести непрерывный учет рисков в течение всех бизнес-процессов.

Управление рисками может осуществляться на основе анализа периодически составляемых отчетов, содержащих список рисков с указанием следующих параметров:
– Класс доступа (внутренний/внешний) – указывается, является ли информация о данном риске закрытой,
– Шифр риска (внутренний номер для ссылок),
– Наименование риска и его описание,
– Категория риска, классифицирующая его по характеру бизнес-процесса, или тип риска,
– Дата обнаружения,
– Лицо, обнаружившее риск (автор),
– Лицо, ответственное за риск,
– Описание возможных последствий,
– Степень последствия (высокая, средняя, низкая),
– Вероятность,
– Величина ущерба (в условных единицах),
– Список возможных мероприятий по устранению риска,
– Список активных (действующих) мероприятий по устранению риска,
– Дата последнего изменения,
– Статус риска (открытый, закрытый).

Для данной таблицы рисков необходимо поддерживать контроль версий с сохранением всех изменений и указанием даты, времени, ав-

тора и содержания изменения. Следует особенно отметить, что для таких документов прав доступа, разрешающих изменение без образования новой версии и сохранения содержания изменения, не существует. Также в отчет о рисках необходимо добавить информацию об авторе отчета, контролирующем лице, дате и времени создания отчета и информации о классе его конфиденциальности.

Выбор мероприятия по устранению риска может быть осуществлен как вручную лицом, принимающим решение, на основе информации о событии, характеризующем возникновение риска, так и автоматически с использованием современных автоматизированных систем поддержки принятия решений.

Согласно современным стандартам [2 – 4], процессы установления, оценки и контроля уровня целостности системы включают определение, анализ и контроль рисков, в том числе расчет рисков и оценка ущерба и обоснование приемлемых (допустимых) рисков.

Отметим, что в последовательности указанных процессов устанавливается обратная связь, которая позволяет на основе анализа возникающих на этапе контроля рисков угроз сформировать необходимость корректирующих воздействий на этапе определения рисков. Соответствующие прецеденты управления рисками приведены на рис. 6.

В целом, управление рисками играет важную роль, так как позволяет производить упреждающие действия, связанные с недопущением нарушения безопасности. В целом, такой характер бизнес-процесса по управлению безопасностью не позволяет применять распространенную в настоящее время методику управления по событиям, заключающуюся в создании децентрализованных центров обработки событий, которые в реальном времени генерируют управляющие воздействия.

Выходом из данной ситуации является применение методов имитационного моделирования и применение функциональности «Что будет, если», которая позволит лицу, производящему анализ рисков моделировать различные ситуации и оценивать возможный ущерб. Особенно актуальна такая функциональность при определении допустимых рисков, связанных с обеспечением требуемого уровня развития предприятия за счет открытого обмена информацией либо использования новых информационных технологий.

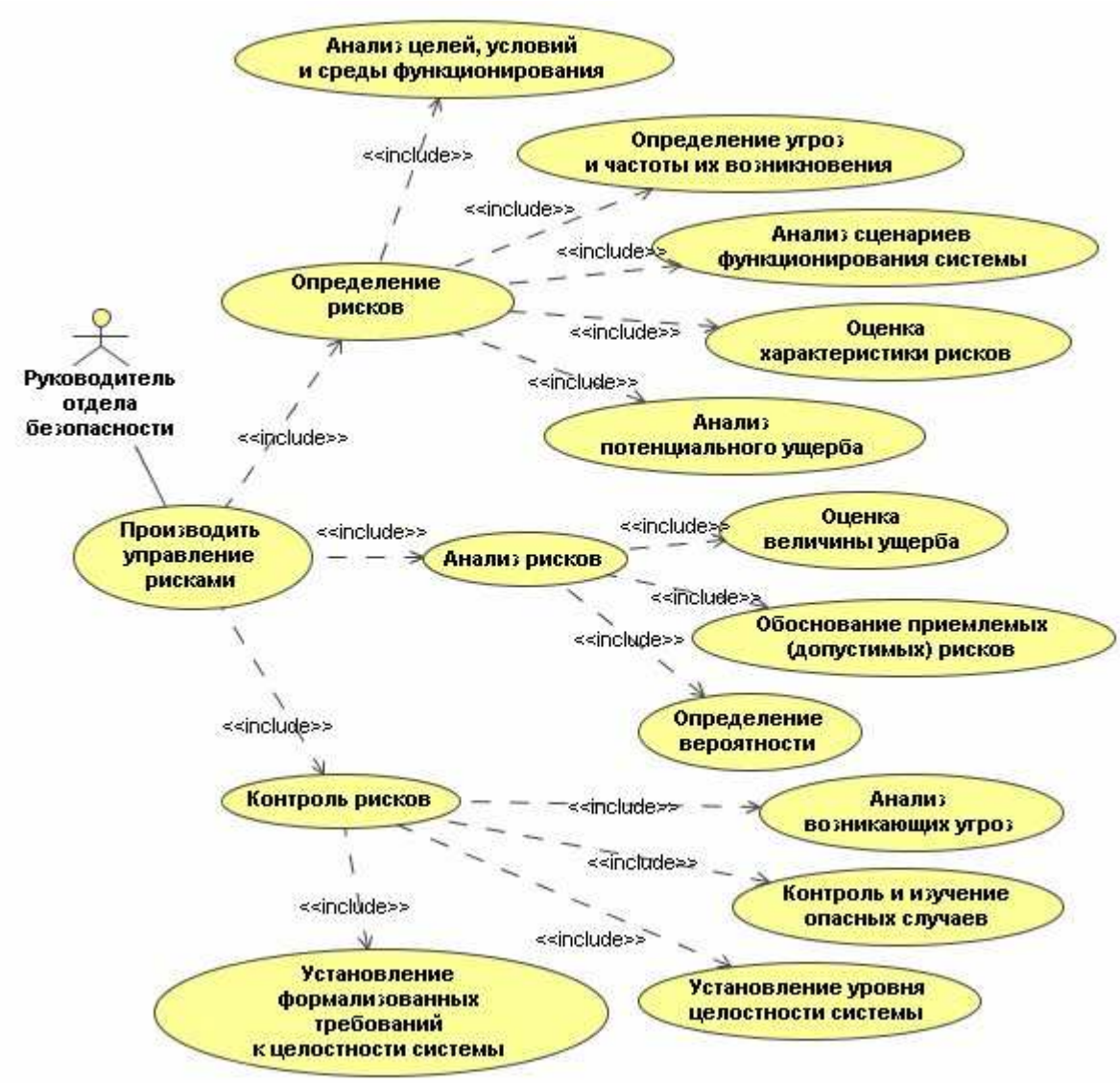

Рис. 6. Диаграмма прецедентов управления рисками

2.5 Оценка сохранения конфиденциальности информации

Модель оценки сохранения конфиденциальности информации регламентирована в работах [2, 3, 4, 18]. Требуемая конфиденциальность информации обеспечивается на основе реализации мероприятий, гарантирующих защищенность информационных ресурсов системы от несанкционированного доступа до истечения периода объективной конфиденциальности данной информации.

Моделируемые случаи соотношения между временем смены значений параметров преград системы защиты и их расшифровки (вскрытия) и периодом объективной конфиденциальности информации для одной преграды приведены на рис. 7 [2, 18].

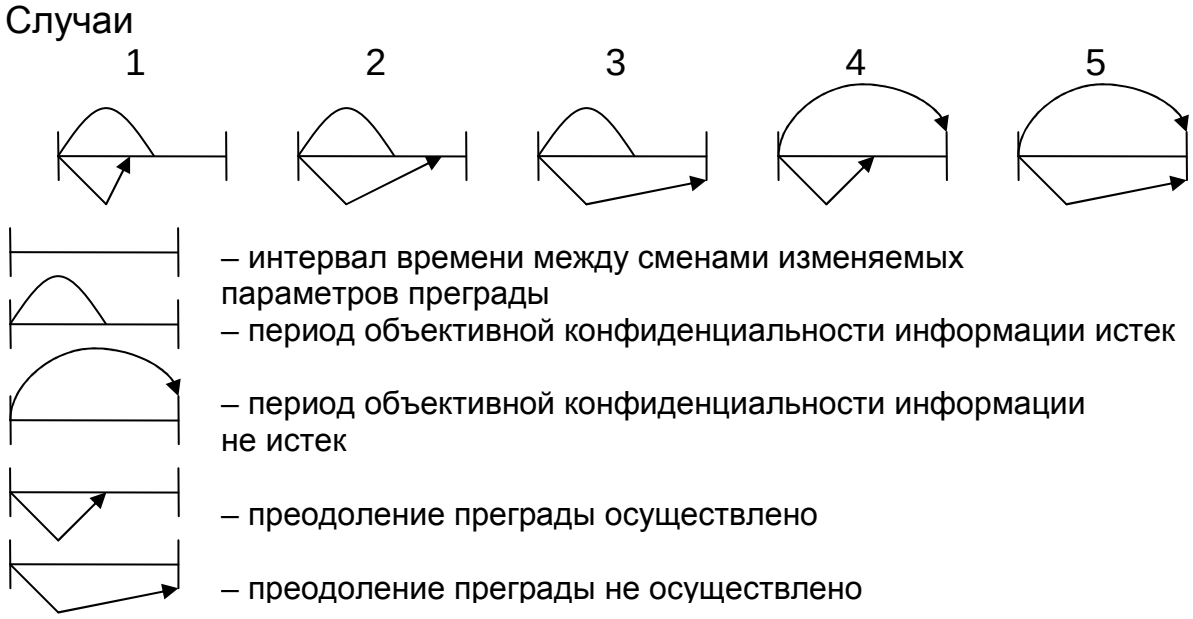

Рис. 7. Иллюстрация формальных процессов нарушения конфиденциальности информации (на примере одной преграды)

Конфиденциальность информации сохранена в случаях 2, 3, 5, нарушена в случаях 1, 4. Вероятность сохранения конфиденциальности информации [2, 18] вычисляют по формуле:

$$P_{конф} = 1 - \prod_{m=1}^{k} P_{преод\ \ конф\ \ m}, \qquad (1)$$

где k – количество преград, которое необходимо преодолеть нарушителю, чтобы получить доступ к информации;

$P_{преод\ конф\ m}$ – вероятность преодоления нарушителем m-ой преграды до истечения периода объективной конфиденциальности информации Тконф.

Для экспоненциальной аппроксимации распределений исходных характеристик [2, 18] при их независимости $P_{преод\ конф\ m}$ равна:

$$P_{преод\ \ конф\ \ m} = \frac{T_{конф} f_m}{T_{конф} f_m + u_m f_m + u_m T_{конф}}, \qquad (2)$$

где f_m – среднее время между соседними изменениями параметров защиты m-ой преграды;

u_m – среднее время преодоления (вскрытия значений параметров защиты) m-ой преграды;

$T_{конф}$. – средняя длительность периода объективной конфиденциальности информации.

Необходимые для моделирования исходные количество преград k и пределы значений u_m определяют в результате дополнительного моделирования, натурных экспериментов, учитывающих специфику

системы защиты и возможные сценарии действий нарушителей, или сравнения с аналогами, диапазон возможных значений $T_{конф}$ задают в техническом задании или в постановках функциональных задач.

Будем считать, что преграда для доступа, установленная в результате отработки ряда запланированных мероприятий может воспрепятствовать как нарушителю (событие $A_н$), так и добропорядочному сотруднику (событие), для которого эта информация предназначается. Событие преодоления нарушителем m-ой преграды обозначим $A_{преод\ конф\ m}$.

Таким образом, вероятность того, что пользователь, получающий доступ к информации является нарушителем P_H, а вероятности сохранения охраняемой информации в этом случае можно вычислить по формуле:

$$P_{конф} = 1 - \prod_{m=1}^{k} P(A_{преод\ \ конф\ \ m} / A_н), \qquad (3)$$

2.6 Управление безопасностью

Для управления безопасностью по комбинации трех параметров расширим описанную выше модель следующим образом.

Определим множество информационных объектов

$$O = \{O_k\}, \qquad (4)$$

где $k=1..K$, K – количество всех информационных объектов.

Для каждого информационного объекта можно задать совокупность атрибутов A_{O_k} и связей R_{O_k}, то есть все информационное пространство предприятия представляет собой семантическую сеть.

Совокупность информационных объектов также является информационным объектом. В связи с чем, набор рисков имеет смысл задавать для информационного объекта следующим образом:

$$R_{O_k} = \{r_i = (p_i, d_i, t_в)\}, \qquad (5)$$

где $i=1..N_R$, N_R – количество всех предусмотренных рисков.

p_i – вероятность наступления i-го риска,

d_i – ущерб в результате наступления i-го риска (измеряется в условных единицах),

$t_в$ – время выявления риска.

Каждый риск может быть определен для некоторого набора сценариев потенциальных угроз G_{R_i}, представляющих собой факторы,

обуславливающие появление риска. Сценарии угроз описываются в виде изменения семантической сети во времени и могут быть представлены в виде цепочки событий

Для снижения риска может быть введена группа мероприятий

$$M_j = \left\{\left(R_{O_k,j}, \delta_j^M, \Delta p_j, \Delta d_j, c_j\right)\right\}, \quad (6)$$

где $j=1..N_M$, N_M – количество всех предусмотренных мероприятий,

δ_j^M – флаг активации мероприятия, равен 1, если мероприятие активировано и 0 в противном случае,

Δp_j – изменение вероятности риска при активации мероприятия,

Δd_j – абсолютное изменение величины ущерба при активации мероприятия,

c_j – стоимость мероприятия.

Определим мероприятия, активированные в момент времени t в виде $M_{j,t}$. При такой постановке задачи управление безопасностью заключается в определении в каждый момент времени некоторого количества активированных мероприятий, которые приводят к снижению риска.

Поскольку полное устранение риска невозможно, цель активации мероприятий можно считать достигнутой, если значение риска не превышает значения допустимого риска

$$R_{доп} = \left\{\left(p_{доп_i}, d_{доп_i}\right)\right\}, \quad (7)$$

где

$p_{доп_i}$ – вероятность i-го риска,

$d_{доп_i}$ – оценка ущерба i-го риска.

Остаточный риск

$$R_{ост} = \left\{\left(p_{ост_i}, d_{ост_i}\right)\right\}, \quad (8)$$

описывает текущее состояние безопасности предприятия в условиях отработки активированных мероприятий. Целью функционирования системы управления рисками является снижение остаточных рисков до тех пор, пока они не будут меньше или равными допустимым.

Для комплексной оценки безопасности предприятия можно выделить ряд интегральных параметров, характеризующих в целом остаточный риск. Отметим, что, несмотря на то, что эти параметры обладают меньшей информационной нагрузкой, нежели значения до-

пустимого риска, они могут использоваться для обобщенной оценки безопасности предприятия.

Пессимистичную оценку риска позволяет сделать вероятность общего ущерба:

$$p_{ост}^{O} = \prod_{i=1}^{N_R} p_{ост_i} \delta_{ост_i}^{(p)} \tag{9}$$

и собственно величина общего ущерба:

$$d_{ост}^{O} = \sum_{i=1}^{N_R} d_{ост_i} \delta_{ост_i}^{(d)}, \tag{10}$$

где

$$p_{ост_i} = p_i - \sum_{j=1}^{N_M} \Delta p_j \delta_j^M, \; d_{ост_i} = d_i - \sum_{j=1}^{N_M} \Delta d_j \delta_j^M \tag{11}$$

$$\delta_j^M = \begin{cases} 1, \textit{если } p_{ост_i} > p_{доп_i}, d_{ост_i} > d_{доп_i} \\ 0, \textit{иначе} \end{cases} \tag{12}$$

Использование этих параметров обусловлено соображением минимизации ущерба и вероятности риска для решения задачи обеспечения безопасности предприятия, так как устранение одного риска равносильно уменьшению другого с точки зрения общей оценки ущерба и при условии, что оценка ущерба производится унифицировано для всех рисков.

Стоимость мероприятий по снижению рисков определяется следующим образом:

$$C_M = \sum_{j=1}^{N_M} c_j \delta_j^M \tag{13}$$

Стоимость активированных мероприятий, направленных на снижение неактуальных рисков характеризует возможность снижения затрат на обеспечение безопасности:

$$C_M^{изб} = \sum_{j=1}^{N_M} c_j \delta_j^M \delta_j^{изб} \tag{14}$$

$$\delta_j^{изб} = \begin{cases} 1, \textit{если } \forall R_{O_k} \Delta p_{O_k j} \cdot \prod_{R_{O_k}} p_i = 0 \vee \Delta d_{O_k j} = 0 \vee \sum_{R_{O_k}} d_i = 0 \\ 0, \textit{иначе} \end{cases} \tag{15}$$

Будем называть лиц, которые получают доступ к информационным объектам акторами. Это могут быть сотрудники предприятия

или внешние лица, которые для выполнения различных служебных заданий должны получать доступ к данным системы.

Актор с некоторой вероятностью p_{uz} может быть злоумышленником, то есть его доступ к системе с вероятностью 1 приведет к срабатыванию одного или нескольких рисков. Мероприятия в данном случае должны приводить к недопущению доступа таких акторов в систему.

С другой стороны, возможен некоторый набор мероприятий, активация которых приведет к запрету допуска акторов, не являющихся злоумышленниками. При этом можно оценить ущерб от недопуска их к информационным объектам, заключающийся во временных задержках и ограничении к развитию информационного объекта.

На основании данных о тенденциях изменения введенных параметров: вероятности и величины ущерба рисков можно сделать следующие предположения о характере их изменения. В основе этого предположения лежит тезис о постоянном затухающем изменении риска во времени, связанном с потерей актуальности информации и потерей интереса.

На рисунке 7 приведены зависимости вероятности одного риска от времени с момента идентификации риска. Действительно, динамика изменения риска имеет следующий характер: вероятность может уменьшаться со временем при условии потери актуальности (кривые 3, 4), возрастать под воздействием внешних условий (1), либо оставаться постоянной в течение длительного времени (2).

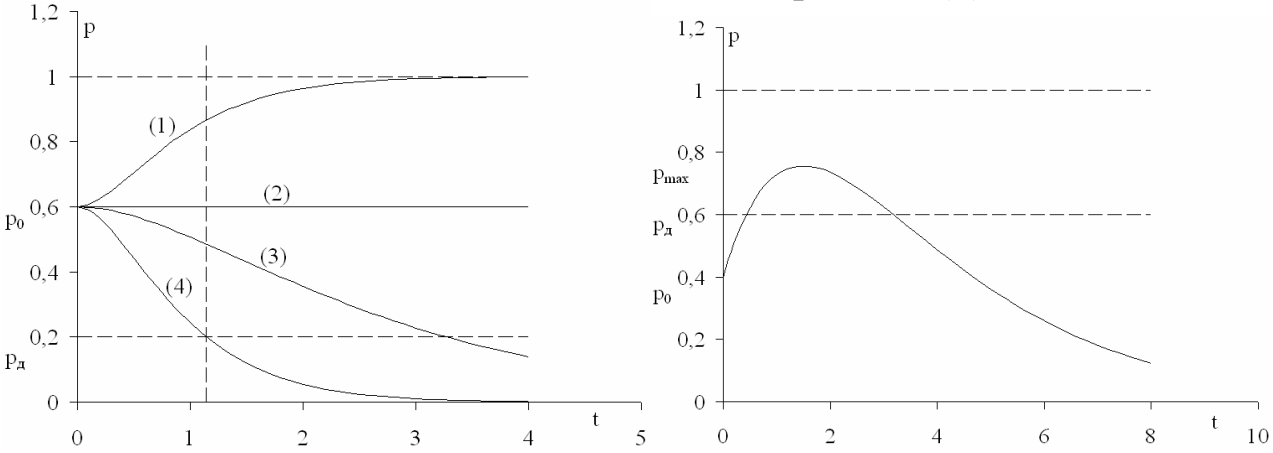

Рис. 7. Динамика изменения вероятности риска:
варианты изменения (справа)
и изменение вероятности при условии действия мероприятия (слева)

Будем считать, что изменение вероятности риска происходит плавно. В практических задачах риски могут меняться скачкообразно, однако, в промежутках между скачкообразными изменениями могут

рассматриваться с учетом сделанного ограничения. Достижение риска значения 1 будем считать событием срабатывания.

Анализ существующих данных [1, 4, 18] позволяет сделать вывод о возможности аппроксимации зависимости риска от времени стандартными параметрическими моделями – функциями заданного вида [19]. При этом параметры модели характеризуют скорость приближения значения вероятности к предельным значениям.

Действие мероприятий по снижению рисков должно быть направлено на обеспечение требуемого снижения выбранных показателей. Вероятность риска в начальный момент времени (при идентификации) может быть ниже допустимого предела, а с течением времени увеличиваться.

В этом случае может быть выбран комплекс мероприятий, приводящий к снижению вероятности риска. Аналогичные зависимости могут быть построены и для оценки величины ожидаемого ущерба.

Отслеживание динамики изменения вероятности и величины ущерба позволяют идентифицировать необходимость применения мероприятий в ходе функционирования предприятия.

На погрешность управления влияет неточность оценки вероятности и величины ущерба рисков, а также изменения вероятности и ущерба рисков для мероприятий; определения актуальности мероприятий и наличия запаздываний эффекта мероприятий с момента их активации.

Алгоритм управления безопасностью в этом контексте выглядит следующим образом:

1. Фаза конфигурирования – содержит действия по настройке системы управления и построению автомата, описывающего обработку риска.
   - 1.1. Идентификация рисков, определение текущей вероятности наступления риска и величины возможного ущерба: производится на основе обработки данных единого информационного пространства:
     - 1.1.1. Определение информационных объектов, связанных с риском;
     - 1.1.2. Определение режима доступа лиц к этим информационным объектам и т.п.;
     - 1.1.3. Оценка ущерба;
     - 1.1.4. Определение взаимосвязи рисков и влияния их наступления друг на друга

1.2. Выработка мероприятий по устранению рисков.
    1.2.1. Создание и обеспечение ведения справочника мероприятий и рисков с описанием экспертной оценки эффективности мероприятий в смысле величины и времени снижения вероятности и/или величины ущерба.
    1.2.2. Описание конкретных мероприятий для выявленного риска с уточнением вариантов управленческих решений. Для каждого риска рекомендуется определить не менее 5 вариантов применения мероприятия.
1.3. Определение текущего статуса риска
    1.3.1. Если риск активен, то есть имеет значение вероятности или ущерба выше допустимого предела, необходимо активировать мероприятие по его снижению
    1.3.2. Если риск не превышает допустимый предел, активация мероприятия не осуществляется
2. Фаза оперативного мониторинга включает действия, направленные на постоянное отслеживание изменения статуса выявленных рисков и активации мероприятий при необходимости
2.1. Оценка динамики изменения вероятности риска и величины ожидаемого ущерба
    2.1.1. Аппроксимативный анализ зависимости показателей риска от времени по каждому риску (для аппроксимации могут использоваться как параметрические модели – функции заданного вида, что облегчит процедуру идентификации, так и ортогональные функции, определенные на полубесконечном интервале, что позволит лучше исследовать характер изменения выбранных параметров).
    2.1.2. Определение событий превышения показателями рисков допустимых значений.
    2.1.3. Определение тенденции повышения или понижение величины риска.
    2.1.4. Оценка текущего состояния забывающего автомата.
2.2. Определение мероприятий с учетом агрессивности среды
    2.2.1. В случае идентификации положительной динамики изменения риска, дополнение (или замена) мероприятий, заключающееся в изменении конфигурации преград.
    2.2.2. В случае если предыдущее мероприятие неэффективно, и дополнительных изменений не было, дополнение но-

вым мероприятием, или замена мероприятия на более эффективное.

2.2.3. В случае если предыдущее мероприятие неэффективно, при этом было активировано новое мероприятие, однако по истечении времени оно опять преодолевается, идентификация враждебной стороны.

2.3. Активация мероприятий по результатам выбора, состоящего в анализе стоимости и эффективности.

2.4. Анализ избыточных мероприятий – в случае, когда риск находится ниже допустимого предела, и он является единственным, на которое направлено мероприятие, необходимо рекомендовать лицу, принимающему решение, отказаться от этого мероприятия и перераспределить ресурсы.

В указанном алгоритме наибольшую сложность имеют два действия: оценка величины риска и выбор мероприятия.

Повторно отметим, что для каждого риска на подготовительном этапе (в фазе конфигурирования) определяется список возможных мероприятий с разной эффективностью. Это творческий процесс, выполняемый аналитиком и состоящий в экспертной оценке эффективности каждого мероприятия.

Автоматизация этого процесса состоит в ведении базы данных мероприятий и накоплении статистики их использования. Эта база данных по сути является основным инструментом специалиста по безопасности, который используется для учета выполняемых работ.

Организационно необходимо обеспечить работу службы безопасности с этой системой таким образом, чтобы информация обо всех мероприятиях и выставляемых преградах сохранялась в базе данных. Сделать это можно следующим образом: автоматизировать формирование отчетности по результатам работы и обеспечить регулярный характер проверки создаваемой отчетности. Косвенным преимуществом в этом случае будет обеспечение более жесткого контроля деятельности службы безопасности со стороны руководства предприятия и других контролирующих органов.

Отдельно стоит отметить событие диагностирования ожидаемой эффективности мероприятия, что свидетельствует о потенциальной возможности существования противника и активного противодействия мероприятиям.

Можно выделить две причины снижения ожидаемой эффективности мероприятия: погрешность оценки величины риска или харак-

теристик мероприятия, а также существование противодействующей стороны. В этом случае следует переосмыслить эффективность мероприятий и скорректировать управляющее воздействие, а также активировать деятельность по определению источника воздействия.

Определение величины риска состоит в оценке первоначальных значений вероятности и ожидаемого ущерба и периодической повторной оценке этих параметров в течение времени.

Оценка вероятности риска может производиться на основе анализа статистики событий, информация о которых накапливается в едином информационном пространстве предприятия и корректироваться экспертами. Периодическое изменение значения вероятности может производиться на основе проведения регулярного повторного анализа.

Оценка ожидаемого ущерба складывается из условной стоимости физического или информационного объекта, а также потерь предприятия в случае срабатывания риска, в том числе стоимость мероприятий по устранению последствий.

При оценке риска следует исходить из наиболее пессимистичного предположении о том, что для любого риска есть активная противодействующая сторона, деятельность которой направлена на увеличение риска.

При оценке рисков и выборе мероприятий может использоваться теория игр [20]. При условии, что известна эффективность мероприятия по снижению определенного риска (по результатам статистической обработки исторических данных, на основании экспертных оценок или данных, полученных в ходе имитационного моделирования) задача управления безопасностью состоит в определении характера текущего изменения риска и определения набора необходимых мероприятий.

Будем считать, что противодействие рискам производится во «враждебной» среде [21]. Действительно, оценка рисков должна производиться не в условиях взаимодействия с природой, когда воздействие на систему безопасности носит случайный характер, а в процессе взаимодействия с противником в игре с неизвестными платежами. При этом необходимо учитывать возможность появления неконтролируемых искажающих воздействий.

В классической постановке теории игр задача игрового взаимодействия решается в предположении, что противникам известны все возможные исходы игры. Однако задачу управления безопасностью

следует отнести к классу задач, связанных с неравноправием партнеров: когда противник располагает неизвестными возможностями.

Действия предприятия заключаются в активации мероприятий и направлены на снижение риска. Действия противника заключаются в создании новых угроз и направлены на повышение риска. Отметим, что действия противника в едином информационном пространстве можно отследить. Это определенное изменение данных, связанное с понижением эффективности мероприятия.

Оценка риска является закрытой деятельностью предприятия, и принятие решений производится при условии, что противник знает о проводимых мероприятиях, но не знает о том, в связи с каким риском производится активация мероприятий.

Поскольку при управлении безопасностью необходимо обеспечивать предупредительные действия, производится анализ рисков, а не событий. Игра во враждебной ситуации выражается в действии игроков на существующую систему преград. Предприятие совершенствует ее, применяя комплекс мероприятий, а противник старается преодолеть преграды. Если выбор стратегии (набора мероприятий) при особых условиях производится случайно, то есть реализуется смешанная стратегия, противодействие противника затруднено.

Решения, принимаемые на основе статистической оценки свойств среды, могут быть неэффективными во враждебной среде, то если при наличии специальной последовательности действия, выбираемых противником. В работе [21] показано, что для решения таких задач необходимо использовать тактику «забывающего» автомата, которая наиболее устойчива к действиям противника.

Допустим, необходимо выбрать мероприятие по противодействию риску при условии, что по стоимости можно организовать выполнение только одного мероприятия, а противник может подготовить преодоление также только одного мероприятия. Опишем автомат для простого случая, выбора между двумя мероприятиями m_1, m_2.

Множество состояний такого автомата обозначим в виде

$$S = \{(m_j, r_1, r_2, n_1, n_2)\}, \qquad (17)$$

где r_i – пара значений (вероятность и ущерб) оценки i-го риска,

m_j – выбранное мероприятие, являющееся действием автомата,

r_1, r_2 – риски, оценивающие эффективность действия,

n_1, n_2 – значения счетчиков выполнения действий.

Смена состояний автомата производится следующим образом. Пусть в момент времени t имеем

$$S(t) = \left\{\left(m_j(t), r_1(t), r_2(t), n_1(t), n_2(t)\right)\right\}, \tag{18}$$

Определим $x(t) = \{1, 0\}$ – вход автомата (подкрепление или штраф).

Если $m_j(t) = m_j$, то

$$\begin{gathered} r_j(t+1) = \frac{n_j(t)}{n_j(t)+1} r_1(t) + \frac{1}{n_j(t)+1} x(t), \\ r_l(t+1) = r_l(t), \quad \forall l \neq j \\ n_j(t+1) = n_j(t) + 1 \\ n_l(t+1) = n_l(t) \end{gathered} \tag{19}$$

Это забывающий автомат с изменяющимися коэффициентами сохранения. Выбор мероприятия производится следующим образом:

– Если $r_i(t+1) - r_l(t+1) \geq \Delta$, то $m(t+1) = m_j$,

– Если $r_i(t+1) - r_l(t+1) < \Delta$, то $m(t+1) = m_\theta$,

где $\Delta \in (0, 1)$ – критическая разность,

θ – случайная величина, равномерно распределенная на множестве индексов действий, $prob\{\theta = j\} = 1/2$

Отметим, что оценка риска производится по двум значениям: вероятности и величине ущерба с учетом их динамики изменения. При этом, в случае сравнения двух рисков, когда один из них лучше другого по вероятности, но хуже по величине ущерба, предпочтение следует отдавать оценке вероятности (естественно предусмотреть возможность конфигурирования этого параметра при реализации в автоматизированной системе управления).

При $\Delta = 0$ на каждом шаге предпочтение отдается действию, имеющему лучшую оценку, что соответствует наиболее известной схеме статистического поведения [21].

Стратегия противника состоит в следующем:

– При $|r_1(t) - r_2(t)| < \Delta$ выполняется действие по преодолению мероприятия g_1;

– При $|r_1(t) - r_2(t)| \geq \Delta$ противник выполняет действие g_2;

Автомат будет получать подкрепление только за мероприятие m_1. Учитывая, что на каждое подкрепление среднее число выполнения мероприятия равно $1/\Delta$, средний доход автомата составит

$$\omega = \Delta/(1+\Delta) \qquad (20)$$

При уменьшении Δ в равнодушной среде возможность автомата выбирать лучшее из действий улучшается, а во враждебной среде снижается возможность автомата противостоять враждебным действиям.

3 Автоматизированная система управления безопасностью

В данном разделе опишем один из вариантов возможной реализации описанных выше алгоритмов в автоматизированной системе комплексного управления безопасностью предприятия, основанной на использовании единого информационного пространства предприятия.

Структура базы данных системы приведена на рис. 8. Она расширяет единое информационное пространство предприятия введением понятий риска, ущерба, мероприятия и определяет соответствие с информационными объектами, путем введения ссылок на них.

Базовый функционал системы (см. рис. 9, 10) включает представление семантической сети объектов, рисков и мероприятий. Для справочника объектов есть возможность просмотра и редактирования рисков и мероприятий.

Вести оперативный учет мероприятий с отслеживанием их статуса можно с помощью справочника мероприятий (см. рис. 10). Для каждого мероприятия указываются компенсируемые им риски и объекты, которые с ними связаны.

Одно и тоже мероприятие может действовать сразу на несколько рисков, уменьшая вероятности и ущерб на различные величины. Для каждого риска показывается его исходная вероятность и ущерб и конечные – с учетом мероприятий. К некоторому риску можно добавить новое или уже существующее мероприятие, редактировать мероприятие и удалить мероприятие для данного риска или для всех рисков.

Рис. 8. Модель базы данных системы

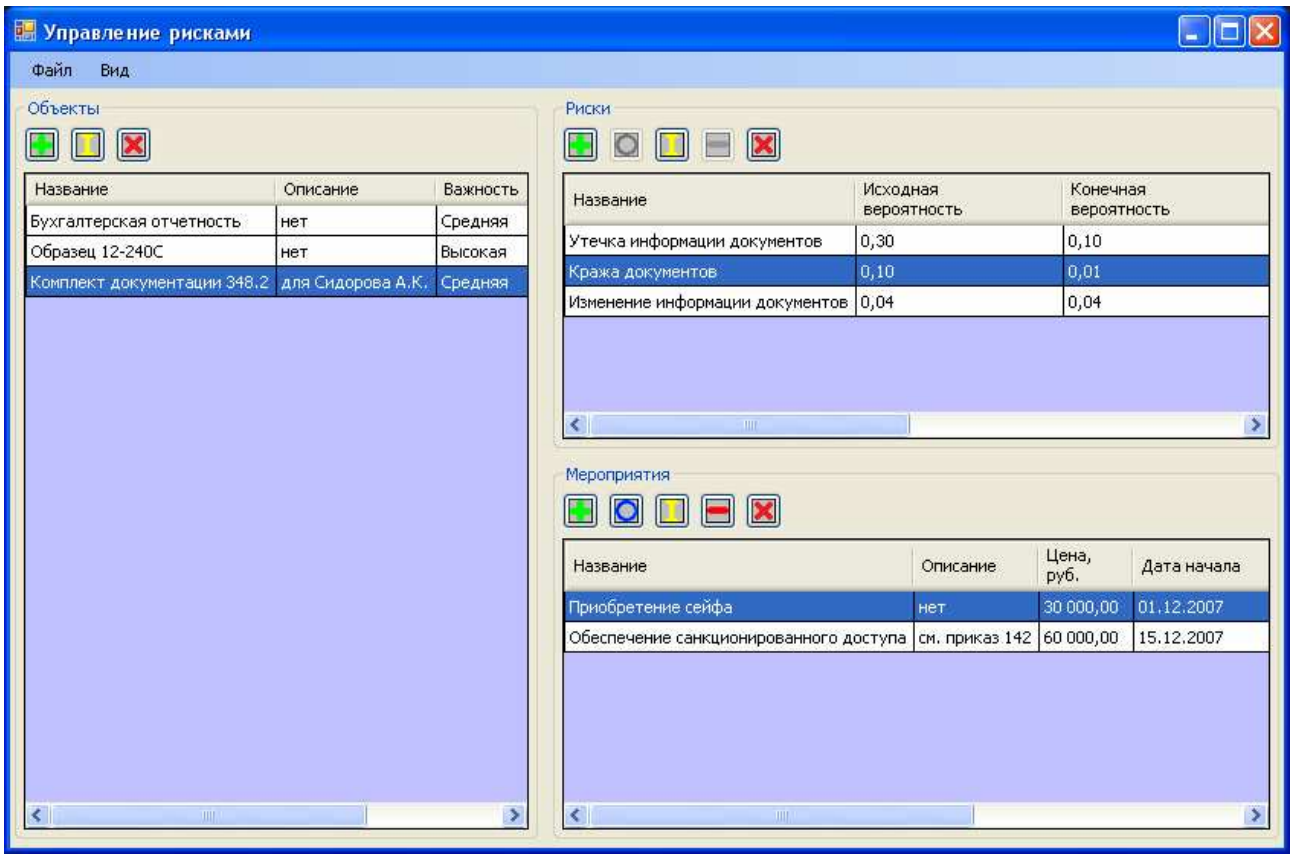

Рис. 9. Ведение справочника объектов и рисков

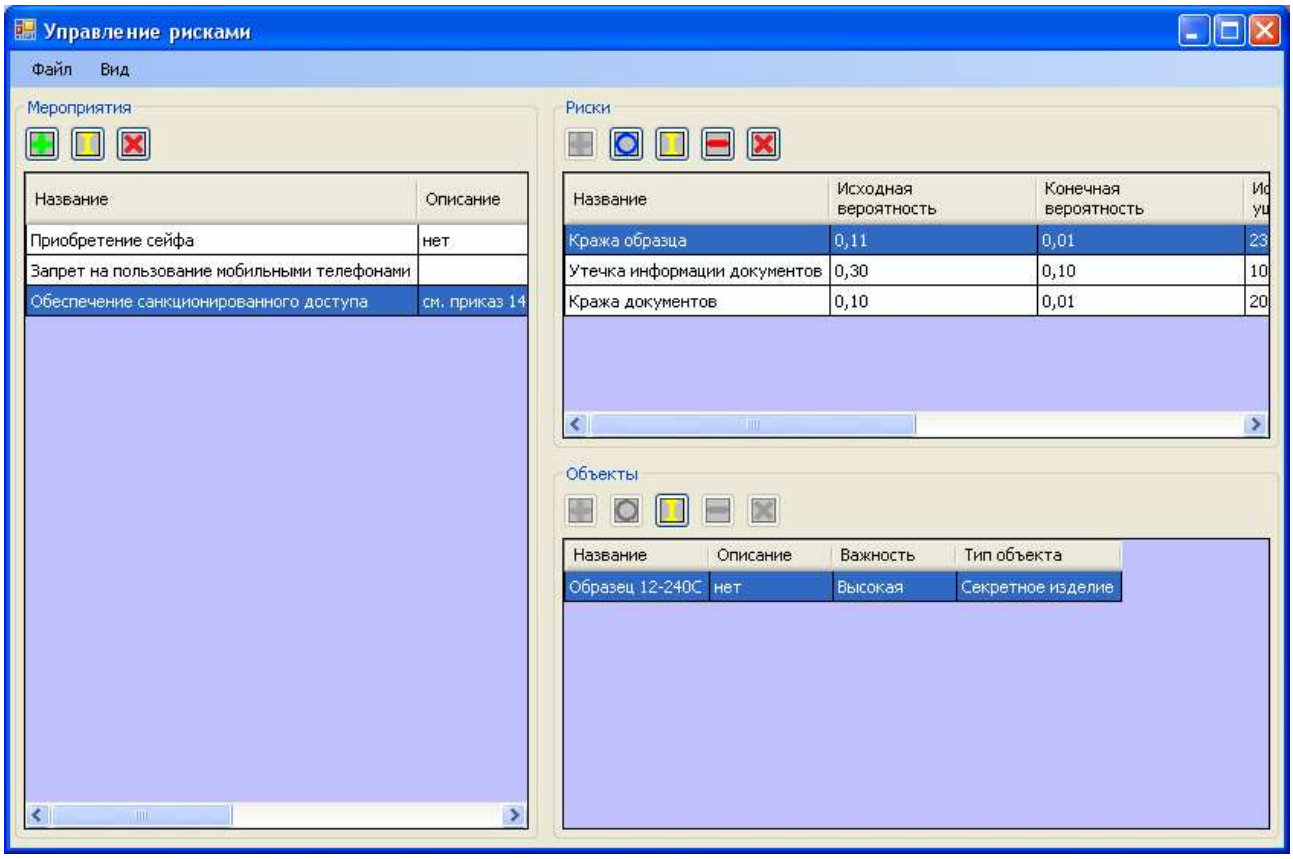

Рис. 10. Ведение справочника мероприятий и рисков

Основное назначение системы – предоставить сотрудникам подразделения, ответственного за безопасность предприятия инструмент организации мероприятий, связанных с обеспечением безопасности отдельных информационных объектов, а руководителю подразделения безопасности – инструмент мониторинга и анализа рисков и оценки эффективности мероприятий.

Интеграция с системами единого информационного пространства может быть произведена с использованием файлов передачи и API PLM и ERP систем. Второй вариант является наиболее предпочтительным, в связи с тем, что интеграцию достаточно сделать однонаправленную (обеспечить только доступ из системы управления безопасностью к объектам PLM системы).

Современные PLM системы (например, ЛОЦМАН:PLM, производитель ГК АСКОН [22]) позволяют достаточно легко решать эту задачу с учетом требований по обеспечению актуальности информации.

Для анализа системы безопасности и поддержки принятия решений для каждого риска предусмотрен специальный отчет, позволяющий упорядочить мероприятия по приоритету с учетом враждебности среды и рекомендовать лицу, принимающему решения, наиболее эффективное противодействие возникающим угрозам.

Заключение

Основные выводы включают в первую очередь следующее:

1. При организации системы управления безопасностью современного предприятия необходимо обеспечить тесное взаимодействие сотрудников подразделений информационных технологий и обеспечения безопасности.

2. Единое информационное пространство предприятия должно быть сформировано с учетом необходимости использования его элементов для управления безопасностью.

3. Информационная поддержка принятия решений по обеспечению комплексной безопасности предприятия должна осуществляться на основе использования актуальных знаний, накапливаемых в едином информационном пространстве.

4. Для поддержки принятия решения в состав единого информационного пространства предприятия необходимо включить подсистемы мониторинга и управления безопасностью.

5. Функциональность системы поддержки принятия решений должна включать возможность ведения базы данных мероприятий и предоставлять инструментарий оперативной работы сотрудникам подразделений, обеспечивающих безопасность предприятия

6. Управление безопасностью необходимо организовать на основе анализа динамики изменения рисков, представленных парой параметров (вероятности возникновения и оценки ущерба). Управление безопасностью – непрерывный процесс, связанный с постоянным анализом рисков и активацией или отменой мероприятий на основе соображений о безопасности и экономии затрат на ее обеспечение.

7. При оценке рисков и выборе мероприятий необходимо учитывать враждебность среды, в связи с чем, в алгоритмах управления целесообразно использовать методы теории игр, в частности, тактику «забывающего» автомата.

8. При реализации предлагаемых алгоритмов следует особое внимание уделить механизмам интеграции подсистемы обеспечения безопасности с PLM и ERP системами предприятия, а также проработке пользовательского интерфейса системы.

Продолжение исследований необходимо, прежде всего, для уточнения экспертных оценок рисков и эффективности мероприятий и проработке методики внедрения предлагаемых алгоритмов в машиностроении.

Приложение. Системы анализа рисков

В данном приложении содержатся сведения о наиболее распространенных системах анализа рисков [23]. Интеграция этих систем в единое информационное пространство предприятия может обеспечить необходимые инструменты для организации системы управления безопасностью.

Отметим, что все указанные в данном приложении системы позволяют проводить единовременный анализ рисков, то есть требуют организации некоторой процедуры повторного анализа для снижения погрешностей анализа и выявления эффективности выбранных мероприятий.

Также все системы в качестве способа оценки рисков используют опросы в виде интервью с уполномоченными представителями организации (CRAMM), опросника, база которого содержит более 600 вопросов, связанных с категориями ресурсов, (Risck Watch) и опроса руководителя службы информационных технологий (ГРИФ).

Итак, приведем некоторые сведения об этих системах.

CRAMM

Метод CRAMM (the UK Goverment Risk Analysis and Managment Method) был разработан Службой Безопасности Великобритании по заданию Британского правительства и взят на вооружение в качестве государственного стандарта. Фирма Insight Consulting Limited занимается разработкой и сопровождением одноименного программного продукта, реализующего метод CRAMM (www.cramm.com).

В настоящее время CRAMM – это довольно мощный и универсальный инструмент, позволяющий, помимо анализа рисков, решать также и ряд других аудиторских задач, включая:

- проведение обследования информационной системы и выпуск сопроводительной документации на всех этапах его проведения;
- проведение аудита в соответствии с требованиями BS 7799:1995 - Code of Practice for Information Security Management BS7799;
- разработка политики безопасности и плана обеспечения непрерывности бизнеса.

В основе метода CRAMM лежит комплексный подход к оценке рисков, сочетающий количественные и качественные методы анализа. Метод является универсальным и подходит для различных предприятий, как правительственного, так и коммерческого сектора. Вер-

сии программного обеспечения CRAMM, ориентированные на разные типы организаций, отличаются друг от друга своими базами знаний.

Одним из результатов, которые можно получить с помощью CRAMM, является экономическое обоснование расходов организации на обеспечение безопасности и поддержку выбранной стратегии управления рисками.

К недостаткам метода CRAMM относят [23] необходимость специальной подготовки и высокой квалификации аудитора, высокую трудоемкость аудита, фиксированное содержание отчетов и большой объем бумажной документации, и сложности при внедрении, особенно в новых организациях.

RiskWatch

Программное обеспечение RiskWatch (разработчик RiskWatch, Inc.), является мощным средством анализа и управления рисками. В семейство RiskWatch входят программные продукты для проведения различных видов аудита безопасности. Оно включает в себя следующие средства аудита и анализа рисков:

- RiskWatch for Physical Security -для физических методов защиты;
- RiskWatch for Information Systems - для анализа информационных рисков;
- HIPAA-WATCH for Healthcare Industry - для оценки соответствия требованиям стандарта HIPAA;
- RiskWatch RW17799 for ISO17799 - для оценки требованиям стандарта ISO17799.

В методе RiskWatch в качестве критериев для оценки и управления рисками используются предсказание годовых потерь (Annual Loss Expectancy - ALE) и оценка возврата от инвестиций (Return on Investment - ROI). RiskWatch помогает провести анализ рисков и обосновать выбор мер и средств защиты.

Метод в основном ориентирован на анализ рисков на программно-техническом уровне защиты, а получаемые оценки рисков не позволяют осуществлять комплексный подход к обеспечению безопасности.

ГРИФ

ГРИФ – это отечественная разработка (компания Digital Security), позволяющая провести глубокий анализ особенностей практической реализации информационной системы и дать макси-

мально точную оценку существующих в информационной системе рисков. Она имеет простой пользовательский интерфейс и ориентирована на применение руководителями и системными администраторами.

Основная задача системы ГРИФ – оценить уровень рисков в информационной системе, эффективность существующей практики по обеспечению безопасности предприятия и обосновать необходимость инвестиций. В результате работы в системе формируется полная модель информационной системы с точки зрения информационной безопасности, что позволяет перейти к комплексной оценке рисков.

Этапы анализа рисков описанными методами приведены в таблицу П1.

Таблица П1 Этапы анализа рисков

Этап	CRAMM	Risk Watch	ГРИФ
1	Определение достаточности применения для защиты системы средств базового уровня, реализующих традиционные функции безопасности	Определение предмета исследования (параметров организации): типа организации, состава исследуемой системы, базовых требований в области безопасности.	Определения полного списка информационных ресурсов
2	Анализ угроз безопасности и уязвимостей	Ввод данных, описывающих конкретные характеристики системы: ресурсы, потери и классы инцидентов. Задается частота возникновения каждой из выделенных угроз, степень уязвимости и ценность ресурсов.	Определение видов информации, представляющей ценность для компании, с указанием ущерба по всем видам угроз.
3	Выбор адекватных контрмер на основании результатов обоснования	Оценка рисков. Определение связей между ресурсами, потерями, угрозами и уяз-	Определение пользователей информации и сопоставление групп поль-

Этап	CRAMM	Risk Watch	ГРИФ
	с учетом расходов, их приемлемость и конечную выгоду	вимостями и расчет математических ожидания потерь за год. Анализ эффективности систем защиты с помощью сценариев "что если...", которые позволяют описать аналогичные ситуации при условии внедрения средств защиты.	зователей и информационных объектов. Определение видов и прав доступа
4		Генерация отчетов	Определение средств защиты информации и затрат на их приобретение и техническую поддержку
5			Анализ политики безопасности и оценка реального уровня защищенности системы и рисков. Оценка адекватности использования имеющихся средств защиты и политики безопасности

Список сокращений

ЕИП – Единое информационное пространство

CALS – Continuous Acquisition and Life cycle Support, Непрерывное развитие и поддержка жизненного цикла (продукта, изделия)

PDM – Product Data Management, Управление инженерными данными

PLM – Product Lifecycle Management, Управление жизненным циклом (продукта, изделия)

ERP – Enterprise Resource Planning, Управление ресурсами предприятия

MES – Manufacturing Execution Systems, Системы управления производством

ESB – Enterprise Service Bus, Корпоративная сервисная шина

UML – Unified Modeling Language, Унифицированный язык моделирования

Литература

1. Резников Г.Я., Бабин С.А., Костогрызов А.И., Родионов В.Н. Количественная оценка защищенности автоматизированных систем от несанкционированного доступа // Информационные технологии в проектировании и производстве, № 1, 2004 с. 11-22
2. Костогрызов А.И. и др. Методическое руководство по оценке качества функционирования информационных систем (в контексте стандарта ГОСТ РВ 51987 «ИТ. КСАС. Требования и показатели качества функционирования информационных систем. Общие положения»). М. – 2004., 352с.
3. Костогрызов А.И., Пьявченко А.Н., Харауз Дж., Бикчентаев Т.Т., Токарева М.А., Львов В.М. Термины и определения международных стандартов в области системной и программной инженерии – М: Мир, 2003. – 168 с.
4. Костогрызов А.И., Нистратов Г.А. Стандартизация, математическое моделирование, рациональное управление и сертификация в области системной и программной инженерии. М. Изд. «Вооружение, политика, конверсия», 2004, 395с.
5. Галатенко В.А. Стандарты информационной безопасности / Под редакцией академика РАН В.Б. Бетелина, М.: ИНТУИТ.РУ «Интернет-университет информационных тенологий», 2004 – 328 с.
6. Буч Г, Рамбо Дж., Джекобсон А. UML. Проектирование программных комплексов, информационных систем. – М.: ДМК Пресс, СПб.: Питер, 2003, – 432 с.
7. Буч Г., Рамбо Дж., Джекобсон А. Язык UML. Руководство пользователя: Пер. с англ. – М.: ДМК Пресс; СПб.: Питер, 2004. – 432 с.
8. Леоненков А.В. Самоучитель UML. – 2-е изд., перераб. и доп. – СПб.: БХВ-Петербург, 2004. - 432с.
9. Рамбо Дж., Якобсон А., Буч Г. UML: специальный справочник. – СПб.: Питер, 2002. – 656 с.: ил.
10. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. – К.: ДиаСофт, 2005 – 614 с.
11. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и Ко», 2004. – 336 с.

12. Колчин А.Ф., Овсянников М.В., Стрекалов А.Ф., Сумароков С.В. Управление жизненным циклом продукции. – М.: Ахарсис, 2002. – 304 с.

13. Норенков И.П., Кузьмик П.К. Информационная поддержка наукоемких изделий. CALS-технологии. - М.: Изд-во МГТУ им. Н.Э. Баумана, 2002 г. - 320 с., ил.

14. Зильбербург Л.И., Молочник В.И., Яблочников Е.И. Реинжиниринг и автоматизация технологической подготовки производства в машиностроении. – СПб: Компьютербург, 2003. – 152 с.: ил.

15. Интеграция данных об изделии на основе ИПИ/CALS – технологий. Часть первая. М.:ГОУ «ГМЦ CALS-технологий», 2002

16. Иващенко А.В., Кременецкая М.Е. Автореинжиниринг единого информационного пространства предприятия – Самара: СНЦ РАН, 2006 – 116 с., ил.

17. Виттих В.А., Скобелев П.О. Мультиагентные модели взаимодействия для построения сетей потребностей и возможностей в открытых системах // Автоматика и телемеханика. – 2003. - №1. – с. 177-185.

18. Резников Г.Я. Рациональный мониторинг процессов менеджмента качества на предприятиях – М.: Мир, 2005 – 284 с.

19. Прикладной анализ случайных процессов. Под ред. Прохорова С.А./ СНЦ РАН, 2007. 582 с.

20. Карлин С. Математические методы в теории игр, программировании и экономике. Пер. с англ. М.: Мир, 1964

21. Журавлев Г.Е. Принятие решений во «враждебной» среде // Проблемы принятия решения М.: Наука, 1976 – с. 262 – 282

22. Дорн Т., Аитов В. Новая версия ЛОЦМАН:PLM Управляйте инженерными данными в совершенстве, Сапр и графика № 12, 2006 – с. 18 – 21

23. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний // iXBT.com. Май-2008

Сергей Антонович Прохоров
Андрей Алексеевич Федосеев
Антон Владимирович Иващенко

Автоматизация комплексного управления безопасностью предприятия

Издательство Самарского научного центра РАН
Лицензия на издательскую деятельность
ЛР № 040910 от 10.08.98 г.

Подписано в печать
Формат 60x84 1/8 Бумага офсетная. Печать офсетная.
Гарнитура Times New Roman. Усл. печ. л. 3,3
Тираж 300 экз. Заказ №

Отпечатано в типографии АНО «Издательство СНЦ РАН»
443001, г. Самара, Студенческий переулок, 3а
тел.: 42-37-07