



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: 2009149132/08, 28.12.2009

(24) Дата начала отсчета срока действия патента:
28.12.2009

Приоритет(ы):

(22) Дата подачи заявки: 28.12.2009

(45) Опубликовано: 20.05.2011 Бюл. № 14

(56) Список документов, цитированных в отчете о
поиске: RU 2246134 C2, 10.02.2005. WO 2005/122047
A2, 22.12.2005. RU 2181216 C1, 10.04.2002. US
5966700 A, 12.10.1999.

Адрес для переписки:

350003, г.Краснодар, а/я 5337, Р.Э. Палий

(72) Автор(ы):

Лучников Павел Константинович (RU)

(73) Патентообладатель(и):

Лучников Павел Константинович (RU)

(54) СИСТЕМА МИНИМИЗАЦИИ РИСКОВ

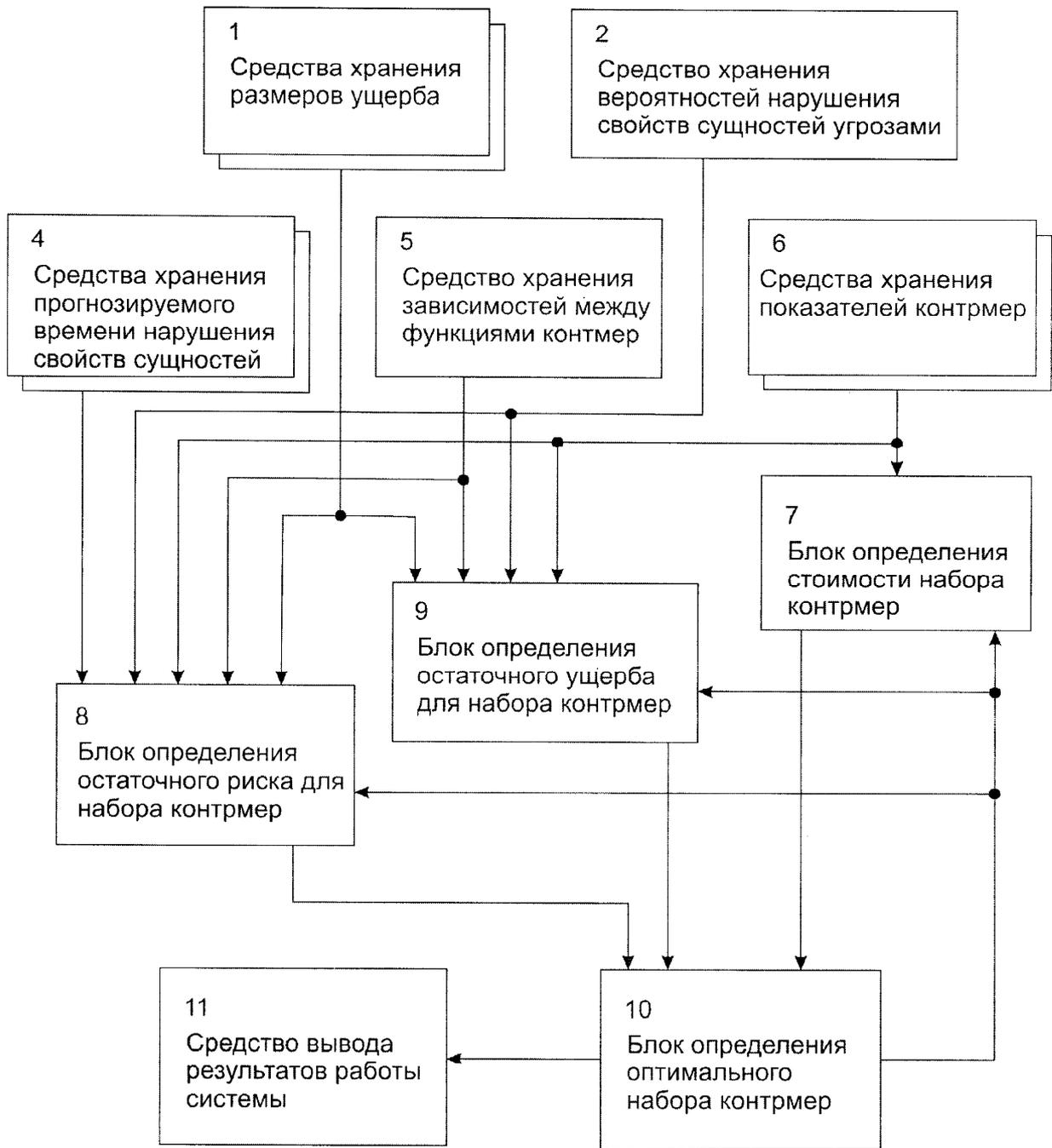
(57) Реферат:

Изобретение относится к способам и устройствам обработки цифровых данных и методам цифровых вычислений, предназначенным для принятия максимально эффективных решений, а также для контроля эффективности уже принятых решений. Техническим результатом являются автоматизация поиска наиболее оптимального минимизирующего риск решения и повышение точности вычисления параметров. Система минимизации рисков содержит: средства хранения размеров ущерба, блок определения остаточного риска, средство хранения вероятностей нарушения свойств сущностей угрозами, средств хранения прогнозируемого

времени нарушения свойств сущностей в случае реализации угроз, средство хранения зависимостей между функциями контрмер, средств хранения показателей контрмер, блок определения стоимости S_{zor}^T набора контрмер z , блок определения остаточного риска S_{zoy}^T для набора контрмер z , средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер, блок определения остаточного ущерба S_{zoy}^T для набора контрмер z , средство вывода результатов контрмер. 5 з.п. ф-лы, 3 ил., 8 табл.

RU 2 419 155 C1

RU 2 419 155 C1



Фиг. 1



FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(51) Int. Cl.
G06Q 90/00 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2009149132/08, 28.12.2009**

(24) Effective date for property rights:
28.12.2009

Priority:

(22) Date of filing: **28.12.2009**

(45) Date of publication: **20.05.2011 Bull. 14**

Mail address:

350003, g.Krasnodar, a/ja 5337, R.Eh. Palij

(72) Inventor(s):

Luchnikov Pavel Konstantinovich (RU)

(73) Proprietor(s):

Luchnikov Pavel Konstantinovich (RU)

(54) SYSTEM TO MINIMISE RISKS

(57) Abstract:

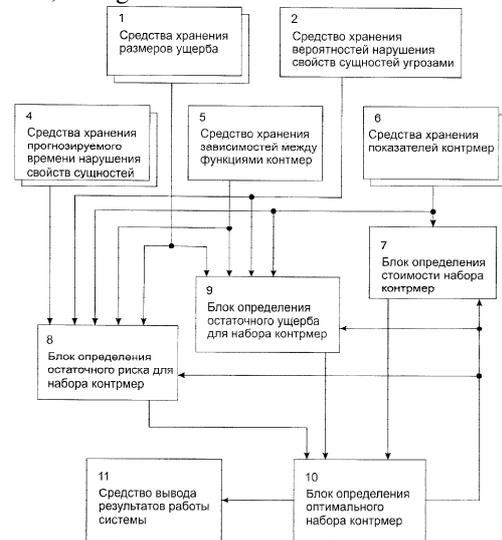
FIELD: information technologies.

SUBSTANCE: system to minimise risks comprises the following components: facilities to store size of damage, a unit to determine a residual risk, a facility to store probabilities of substance properties damage by threats, facilities to store forecasted time of substance properties violation in case threats are realised, a facility to store dependencies between functions of countermeasures, facilities to store indices of countermeasures, a unit to detect cost S_{zor}^T of a set of countermeasures z , a unit to detect a residual risk S_{zor}^T for a set of countermeasures z , facilities to store dependencies between functions of countermeasures, facilities to store indices of countermeasures, a unit to detect residual damage S_{zoy}^T for a set of countermeasures z , a facility to display results of countermeasures.

EFFECT: automation of searching for an optimal

risk-minimising solution and improved accuracy of parametres calculation.

6 cl, 3 dwg



Фиг. 1

RU 2 419 155 C1

RU 2 419 155 C1

Изобретение относится к способам и устройствам обработки цифровых данных и методам цифровых вычислений, предназначенным для принятия максимально эффективных решений, а также для контроля эффективности уже принятых решений.

Практически все виды деятельности требуют принятия решений, от эффективности которых зависит эффективность данных видов деятельности в целом. Эффективность представляет собой соотношение эффекта или достигнутого результата и затрат на его получение.

Примером таких видов деятельности и решений, является, например:

- коммерческая деятельность (купля-продажа товаров и услуг), которая, например, требует принятия решений о выборе товаров, их закупке, логистике, охране, хранении, поиске и проверке клиентов;

- производственная деятельность (производство продукции, услуг), которая, например, требует принятия решений об открытии новых (закрытии существующих) производственных мощностей, организации охраны и защиты, выпуске продукции, инвестировании в новые виды услуг;

- финансовая деятельность (венчурное инвестирование, покупка акций, селинговые операции, кредитные операции и др.), которая, например, требует принятия решений об инвестировании в конкретное предприятие, покупке акций, выдаче кредита;

- консалтинговая деятельность, требующая принятия решений об организации работы, продвижении ее на рынке;

- страховая деятельность.

Эффективность указанных решений зависит от соотношения величины возможных потерь к величине возможных выгод, связанных с реализацией данных решений.

Любой вид деятельности характеризуется набором материальных или нематериальных сущностей, которые используются для его осуществления. Такими сущностями могут быть, например, помещения, машины, оборудование, вычислительная техника, информация, люди и другие ресурсы.

Каждая сущность обладает одним или несколькими свойствами, от состояния которых зависит возможность эффективного использования сущности для осуществления рассматриваемого вида деятельности. Примеры свойств - целостность сущности, доступность (наличие в нужном месте в нужное время),

конфиденциальность сущности-информации.

Появление потерь связано с существованием объективных факторов (угроз, рисков), которые негативно отражаются на данных видах деятельности, например пожары, кражи, задержки, аварии, сбои в работе систем, увольнения.

Определение возможных потерь относится к области оценки рисков.

Существует два подхода к оценке рисков:

- качественный анализ;

- количественный анализ.

Качественный анализ связан с качественной оценкой вероятности возникновения угроз и величины возможных потерь от реализации угроз.

Количественный анализ - это определение размера потерь и вероятности угроз в некоторых количественных единицах.

При количественном анализе риск может определяться величиной возможных потерь в стоимостном (денежном) выражении.

Если удастся тем или иным способом спрогнозировать, оценить возможные потери по какой-либо деятельности, то значит, получена количественная оценка риска.

Говоря о том, что риск измеряется величиной возможных (вероятных) потерь,

следует учитывать случайный характер таких потерь. Вероятность наступления события может быть определена объективным методом и субъективным.

Объективным методом пользуются для определения вероятности наступления события на основе исчисления частоты, с которой происходит данное событие.

Субъективный метод базируется на использовании субъективных критериев, которые основываются на различных предположениях. К таким предположениям может относиться мнение оценщика, его личный опыт, экспертная оценка, заключение аудитора.

Таким образом, в основе оценки рисков лежит нахождение зависимости между определенными размерами потерь и вероятностью их возникновения.

Наиболее часто используемый подход к количественной оценке рисков заключается в расчете математического ожидания потерь по формуле:

$$m = p \times v, \quad (1)$$

где p - вероятность возникновения угрозы в течение года,

v - стоимость ущерба в случае, если угроза произойдет.

После выполнения оценки рисков выбирается оптимальная стратегия управления рисками. К базовым стратегиям относятся:

- снижение уровня риска (например, использование системы автоматического пожаротушения снижает вероятность возникновения пожара);

- уход от риска (например, возможность отказа от использования сервиса удаленного доступа позволяет уйти от угроз, реализуемых мобильными пользователями);

- перенос риска (например, при страховании некоторых рисков возможные потери переносятся на страховую компанию);

- принятие риска (когда, например, риск не может быть уменьшен, возможно, наилучшей стратегией будет его принять).

Каждую из стратегий можно реализовать одной или несколькими контрмерами. Например, стратегия «снижения уровня риска» в отношении такой угрозы, как пожар, может быть реализована:

- установкой системы автоматического пожаротушения;

- установкой системы охранно-пожарной сигнализации;

- использованием специальных жаропрочных конструкций.

Использование тех или иных контрмер ведет к снижению вероятности возникновения угрозы в отношении рассматриваемой деятельности и, соответственно, снижает ожидаемые величины потерь. Так, стратегия «переноса риска» переносит риск возникновения угрозы на другую организацию, снижая таким образом вероятность его возникновения в отношении рассматриваемой деятельности.

Совокупность контрмер, которые используются для защиты от рисков для некоторого вида деятельности (например, некоторого предприятия или организации в целом), составляют систему защиты от рисков.

Система минимизации рисков позволяет получить информацию о такой системе защиты, которая максимально снижает риски рассматриваемого вида деятельности по одному или нескольким параметрам.

Традиционно используемый подход к оценке эффективности контрмер, реализующих стратегию «снижения уровня риска», заключается в расчете математического ожидания потерь при условии использования контрмеры (так называемый остаточный риск) по формуле:

$$m_k = p_k \times v, \quad (2)$$

где p_k - вероятность возникновения угрозы в течение года при условии использования контрмеры,

v - стоимость ущерба в случае, если угроза произойдет.

Приведенные математические принципы заложены в основу процесса оптимизации рисков в таких, например, продуктах, как:

- «RiskWatch» (<http://www.riskwatch.com/>);
- «АванГард»;
- «ГРИФ» (<http://www.dsec.ru>).

Качественные оценки рисков используются в таких, например, продуктах, как:

- «CRAMM» (<http://www.cramm.com>);
- «COBRA» (<http://www.security-nsk-analysis.com/riskcon.htm>);
- «КОНДОР» (<http://www.dsec.ru>).

К недостаткам упомянутых продуктов количественной оценки рисков относится отсутствие комплексного учета следующих факторов:

- при учете остаточного риска, как правило, не учитывается остаточный ущерб - ущерб, который может возникнуть, даже если контрмера успешно срабатывает на угрозу. Например, в случае потери информации сервера баз данных и даже при наличии системы резервирования информации требуется время на восстановление данной информации. Данное время недоступности информации может привести к ущербу, связанному с простоем. При этом срабатывание различных контрмер в общем случае приводит к различным уровням остаточного ущерба;

- при расчете остаточного ущерба не учитывается, что ущерб в результате реализации угрозы - величина в общем случае нелинейная, изменяющаяся с течением времени;

- не учитываются взаимосвязи между различными контрмерами, когда результаты функционирования одной контрмеры могут использоваться другими контрмерами;

- в упомянутых продуктах учитываются только контрмеры, реализующие стратегию управления рисками «снижение уровня риска», что потенциально может не позволить выбрать оптимальный набор контрмер;

- способы, модели, заложенные в основу данных продуктов, ограничены и предназначены для оптимизации рисков информационным процессам обработки информации, не позволяя комплексно оценить и другие виды деятельности;

- постоянное расчетное время риска в 1 год не позволяет корректно оценить эффективность комплекса контрмер - для многих контрмер существенной характеристикой являются ежегодные эксплуатационные расходы, т.е. при увеличении расчетного времени соотношение между стоимостью различных вариантов контрмер может существенно измениться.

Кроме того, к существенному недостатку существующих продуктов количественной оптимизации рисков как отечественных, так и зарубежных относится отсутствие механизма автоматического выбора наиболее оптимального комплекса контрмер, т.е. оператор должен сам выбрать набор контрмер, для которого продукт (средство) посчитает уровень остаточного риска. При этом при наличии даже 10 контрмер число возможных комбинаций контрмер в 2^{10} фактически не позволяет проверить все эти комбинации вручную, что очевидно ведет к невозможности выбора самого оптимального варианта защиты.

К недостаткам методов с качественной оценкой рисков относится:

- субъективность - качественные оценки зависят от мнения экспертов,

консультантов, которое может быть неправильным, учитывая сложность оценки всех возможных комбинаций взаимно влияющих угроз и контрмер;

- не формальность критериев оценки, что потенциально может привести к двусмысленности, ошибочным оценкам риска;

- непрозрачность выгод - качественные методы не позволяют дать конкретную оценку: насколько выгодно применения комплекса контрмер и выгодно ли вообще.

Известна система оценки и управления рисками «ГРИФ» ООО «Диджитал Секьюрити» [1]. Система относится к области анализа и управления рисками информационной системы компаний. Система «ГРИФ» позволяет:

- анализировать уровень защищенности ценных ресурсов информационной системы,
- оценить возможный ущерб, который понесет компания в результате реализации угроз информационной безопасности;

- управлять рисками при помощи выбора контрмер, оптимальных по соотношению цена/качество.

Данная система содержит наиболее продвинутый математический аппарат оценки и управления рисками из аналогичных по классу изобретений. По совокупности существенных признаков система оценки и управления рисками «ГРИФ» принята в качестве прототипа.

К недостаткам системы «ГРИФ» относятся следующие:

- область действия прототипа ограничена оценкой рисков в области защиты информации, которые являются только частью общей проблемы управления рисками, охватывающей также финансовые, страховые, коммерческие, кредитные, производственные риски;

- при анализе рисков информационной безопасности система «ГРИФ» учитывает угрозы только по трем свойствам информации (конфиденциальности, целостности и доступности). В то же время даже в информационных системах известно большее количество видов угроз, например угрозы, при реализации которых ресурсы используются не по назначению и которые несут ущерб деятельности (например, сотрудники используют сервис доступа в Интернет не по назначению);

- оценка стоимостных показателей контрмер в системе «ГРИФ» производится посредством указания значения «Стоимости внедрения контрмеры». В то же время известно, что каждая контрмера требует затрат не только на внедрение, но и на поддержку, обслуживание, причем такие постоянные затраты могут значительно превышать стоимость внедрения. Помимо стоимости внедрения и стоимости обслуживания существуют различные контрмеры, которые требуют дополнительных затрат в случае использования их для защиты от угроз. Например, в случае обрыва кабеля, возможно, потребуются затраты на вызов ремонтной организации;

- ущерб по свойствам конфиденциальности, целостности, доступности в системе «ГРИФ» вводится как фиксированное значение возможных затрат в случае реализации угрозы в год (для доступности, затраты в час). В то же время ущерб после реализации угрозы в общем случае функция нелинейная. Например, через месяц после реализации угрозы доступности компания понесет существенные убытки, связанные с неустойкой, а до этого момента величина ущерба может быть незначительной;

- заданное в комплексе постоянное расчетное время риска в 1 год не позволяет корректно оценить эффективность комплекса контрмер - для многих контрмер существенной характеристикой являются ежегодные эксплуатационные расходы, т.е. при увеличении расчетного времени соотношение между стоимостью различных вариантов контрмер может существенно измениться;

- в системе «ГРИФ» используется ограниченное, заданное количество контрмер. Однако, известно, что, например, два антивирусных средства разных производителей могут обладать совершенно разным уровнем эффективности. Невозможность учета разных уровней эффективности одинаковых по классу средств не позволяет сделать вывод о том, что является предпочтительным (особенно учитывая возможную разницу в их стоимости). Кроме того, в системе отсутствует множество альтернативных контрмер, например, такой способ снижения ущерба, как страхование риска;

- в расчетах учитывается остаточный риск, однако в расчетах необходимо также учитывать «остаточный ущерб» - ущерб, который может возникнуть, даже если контрмера успешно срабатывает на угрозу. Например, если контрмера перехватывает большую часть атак, то остаточный риск будет низким, однако если при этом на перехват каждой атаки потребуется значительное время, в течение которого на ресурсы будет действовать угроза, например, 1 час, то для критичного ресурса данная контрмера не будет приемлемой;

- в системе отсутствует возможность учета связей между контрмерами. В то же время это является важной характеристикой существующих контрмер, когда, например, обнаружение атаки производится комплексом средств защиты, возможно, разных производителей, а нейтрализация угрозы производится комплексом средств защиты других производителей. В то же время применение этих средств по отдельности не позволяет снизить ущерб от угрозы;

- в системе отсутствует механизм автоматического выбора наиболее оптимального комплекса контрмер, т.е. оператор должен сам выбрать набор контрмер, для которого система посчитает уровень риска. При этом при наличии даже 10 контрмер число возможных комбинаций контрмер в 2^{10} фактически не позволяет проверить все эти комбинации вручную, что, очевидно, ведет к невозможности выбора самого оптимального варианта защиты;

- в системе используются абстрактные понятия «коэффициент защищенности», «эффективность» контрмеры, выраженные в некоторых числовых значениях, при этом не ясна зависимость между данными значениями и реальной эффективностью контрмер.

Техническим результатом заявляемого изобретения являются:

- автоматический поиск наиболее оптимального решения, минимизирующего риск;
- многопараметричность системы минимизации рисков;
- повышение точности вычисления параметров;
- расширение области применения системы минимизации рисков;
- унификация используемых системой минимизации рисков способов минимизации рисков и зависимостей между ними.

Сущность заявленного изобретения заключается в том, что система минимизации рисков содержит:

- А средств хранения размеров ущерба;
- блок определения остаточного риска;

при этом каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности. При этом система дополнительно содержит:

- средство хранения вероятностей нарушения свойств сущностей угрозами, выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы

приведет к нарушению свойства сущности;

- А средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

- средство хранения зависимостей между функциями контрмер. Средство представлено в форме ориентированного графа. Каждой дуге графа соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризующее степень защиты от одной или нескольких угроз. При этом узлы графа разделяются на начальные, промежуточные и целевые.

Начальные узлы не содержат входящих в них дуг. Совокупность начальных узлов соответствует состоянию такой системы защиты от рисков, при которой контрмеры отсутствуют. Целевые узлы не содержат выходящих из них дуг. Каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких начальных узлов к целевому узлу. Промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты от рисков, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы;

- С средств хранения показателей контрмер, выполненных с возможностью хранения в составе параметров для каждой контрмеры: стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении каждой угрозы, на нейтрализацию которой эта функция направлена;

- блок определения стоимости S_{ztc}^T набора контрмер z , выполненный с возможностью определения стоимости набора контрмер как суммы стоимостей каждой контрмеры, входящей в набор. При этом информационные входы блока определения стоимости набора контрмер связаны с информационными выходами средств хранения показателей контрмер;

- блок определения остаточного риска S_{zot}^T для набора контрмер z выполнен с возможностью определения остаточного риска как суммы по всем свойствам сущностей произведения размера ущерба от нарушения свойства сущности за время, равное прогнозируемому времени нарушения свойства сущности, на сумму по всем угрозам произведения вероятности того, что реализация угрозы приведет к нарушению свойства сущности, на вероятность того, что набор контрмер не сможет снизить ущерб при реализации угрозы. При этом информационные входы блока определения остаточного риска связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средств хранения прогнозируемого времени нарушения свойств сущностей, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

- блок определения остаточного ущерба S_{zou}^T для набора контрмер z , выполненный с возможностью определения остаточного ущерба как суммы по всем сущностям, всем свойствам сущностей и всем угрозам произведения следующих величин:

а) вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

б) вычисленное для всех путей нейтрализации угрозы по графу зависимостей функций контрмер математическое ожидание произведения вероятности того, что для

нейтрализации угрозы сработает конкретный путь, на сумму размера ущерба, вычисленного для времени, равного сумме времен срабатывания всех функций контрмер, входящих в этот путь, и суммарной стоимости реализации всех функций контрмер, входящих в этот путь.

5 При этом информационные входы блока определения остаточного ущерба связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средства хранения

10 зависимостей между функциями контрмер, средств хранения показателей контрмер; - блок определения оптимального набора контрмер, выполненный с возможностью определения такого набора контрмер z , для которого величина $s_z = s_{z_{tco}}^T + s_{z_{or}}^T + s_{z_{oy}}^T$

минимальна. При этом информационные входы блока определения оптимального набора контрмер связаны с информационными выходами 15 блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба, а управляющий выход блока определения оптимального набора контрмер связан с управляющими входами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба;

20 - средство вывода результатов, вход которого связан с информационным выходом блока определения оптимального набора контрмер.

Каждое средство хранения размера ущерба может быть выполнено в виде набора регистров, реализующего одномерный массив размеров ущерба, индексом которого является время от нарушения свойства сущности.

25 Каждое средство хранения размеров ущерба допустимо выполнять в виде блока хранения, имеющего вход времени и информационный выход размера ущерба.

Средство хранения вероятностей нарушения свойств сущностей угрозами целесообразно выполнять в виде набора регистров для хранения двумерной таблицы 30 размером $B \times A$, при этом первый индекс в таблице соответствует номеру угрозы, а второй - номеру свойства сущности.

Средство хранения зависимостей между функциями контрмер возможно выполнять в виде массива наборов регистров, в котором каждый набор регистров относится к одной дуге графа и содержит четыре регистра для хранения соответственно:

- 35
- номера узла, из которого выходит дуга;
 - номера узла, в который входит дуга;
 - номера контрмеры;
 - номера функции контрмеры, которая соответствует дуге.

40 Систему минимизации рисков предпочтительно выполнять в виде процессора и памяти, при этом память должна содержать данные и команды программного обеспечения, исполняемые процессором, для:

- 45
- получения для каждого свойства сущности размера ущерба в заданный момент времени от начала нарушения этого свойства сущности;
 - получения для каждого свойства сущности в отношении каждой угрозы вероятности того, что реализация угрозы приведет к нарушению свойства сущности;
 - получения для каждого свойства сущности прогнозируемого времени его нарушения в случае реализации угроз в отношении этого свойства;
 - получения перечней функций контрмер таких, что каждый перечень соответствует 50 пути в графе зависимости функций контрмер между двумя заданными узлами;
 - получения для каждой контрмеры ее стоимости;
 - получения для каждой функции каждой контрмеры стоимости ее реализации для нейтрализации угроз;

- получения для каждой функции каждой контрмеры времени, необходимого на реализацию этой функции;

- получения для каждой функции каждой контрмеры вероятностей того, что функция не будет выполнена в отношении каждой из угроз;

5 - генерирования наборов контрмер;

- вычисления на основе упомянутых выше полученных значений для каждого набора контрмер стоимости набора контрмер;

10 - вычисления на основе упомянутых выше полученных значений для каждого набора контрмер остаточного риска;

- вычисления на основе упомянутых выше полученных значений для каждого набора контрмер остаточного ущерба;

- определения такого набора контрмер, для которого сумма стоимости, остаточного риска и остаточного ущерба минимальна.

15 Заявляемая система оптимизации рисков поясняется следующими графическими материалами. На фиг.1 показана схема системы минимизации рисков, на фиг.2, 3 - схемы примеров графа зависимостей между функциями контрмер.

Заявляемая система минимизации рисков содержит:

20 - А средств хранения размеров ущерба 1;

- средство хранения вероятностей нарушения свойств сущностей угрозами 2;

- А средств хранения прогнозируемого времени нарушения свойств сущностей 4 в случае реализации угроз;

25 - средство хранения зависимостей между функциями контрмер 5;

- С средств хранения показателей контрмер 6;

- блок определения стоимости набора контрмер 7;

- блок определения остаточного риска для набора контрмер 8;

- блок определения остаточного ущерба для набора контрмер 9;

30 - блок определения оптимального набора контрмер 10;

- средство вывода результатов работы системы 11.

Каждое из средств хранения 1, 2, 4, 5, 6 снабжено по крайней мере одним информационным выходом.

35 Назначение конструктивных элементов системы оптимизации рисков и примеры их выполнения будут указаны далее, при описании работы системы.

Информационные выходы средств хранения показателей контрмер 6 соединены с информационными входами блока определения стоимости набора контрмер 7.

40 Информационные выходы средств хранения 1, 2, 4, 5, 6 соединены с информационными входами блока определения остаточного риска 8.

Информационные выходы средств хранения 1, 2, 5, 6 соединены с информационными входами блока определения остаточного ущерба 9.

45 Информационные выходы блока определения стоимости набора контрмер 7, блока определения остаточного риска для набора контрмер 8, блока определения остаточного ущерба для набора контрмер 9 соединены с соответствующими информационными входами блока определения оптимального набора контрмер 10.

50 Управляющий выход блока определения оптимального набора контрмер 10 соединен с управляющими входами блока определения стоимости набора контрмер 7, блока определения остаточного риска для набора контрмер 8 и блока определения остаточного ущерба для набора контрмер 9.

Информационный выход блока определения оптимального набора контрмер 10 соединен со входом средства вывода результатов работы системы 11.

Заявляемая система минимизации рисков работает следующим образом.

Предварительно производят ввод информации в средства хранения системы. Для этого выполняют следующее.

1. Выявляют максимальное количество сущностей, от которых зависит эффективность функционирования рассматриваемого вида деятельности. Далее O обозначает общее число сущностей.

2. Определяют свойства сущностей. Для каждой сущности o ($o=1, \dots, O$) определяют все возможные свойства, нарушение которых потенциально может нанести ущерб эффективности функционирования рассматриваемого вида деятельности. Далее U^o обозначает число свойств у сущности o .

3. Определяют ожидаемый размер ущерба S_{ulos}^o , который будет нанесен деятельности при нарушении каждого из свойств каждой сущности в отдельности в условиях отсутствия контрмер.

Здесь o - номер сущности, u - номер свойства сущности, $u=1, \dots, U^o$.

Размер ущерба в общем случае есть функция времени $S_{ulos}^o = S_{ulos}^o(t)$,

где t - время с момента нарушения свойства u сущности o .

Размер ущерба определяется в денежных или условных единицах. Определение ущерба может производиться любым путем, который дает приемлемый для целей оптимизации результат (аналитическим, статистическим и т.п.).

Каждое из значений размеров ущерба заносят в отдельное средство хранения размера ущерба 1 . При этом количество A средств хранения 1 определяется из следующего выражения:

$$A = \sum_{o=1}^O U^o$$

Каждое средство хранения размера ущерба 1 может быть выполнено в виде набора регистров, реализующего одномерный массив размеров ущерба, индексом которого является время от нарушения свойства сущности.

Каждое средство хранения размера ущерба 1 может быть выполнено в виде блока хранения, имеющего вход времени и информационный выход размера ущерба. При подаче на вход времени сигнала, соответствующего времени t от нарушения свойства сущности, на информационном выходе размера ущерба формируется сигнал, соответствующий значению размера ущерба, если от нарушения свойства сущности прошло время t .

4. Определяют угрозы, которые могут нарушить свойства сущностей и, соответственно, нанести ущерб эффективности функционирования рассматриваемого вида деятельности. Далее B обозначает общее число выявленных угроз. Далее в тексте индексу обозначает номер угрозы, $y=1, \dots, B$.

Одновременно для каждой угрозы y в отношении каждого свойства и каждой сущности o определяют вероятность $V_{u,y}^{o,T}$ того, что реализация угрозы y приведет к нарушению свойства и сущности o за период времени T .

Здесь и далее в тексте T - промежуток времени существования вида деятельности, для которого выполняется минимизация рисков.

Вероятность $V_{u,y}^{o,T}$ далее в тексте упоминается как вероятность нарушения свойства сущности угрозой. Эта вероятность $V_{u,y}^{o,T}$ может определяться любым доступным способом, в том числе могут использоваться следующие методы:

- аналитический, посредством расчета значений;
- статистический, посредством применения статистики возникновения угроз в аналогичных видах деятельности;
- экспертный, посредством сбора и обработки мнений экспертов в предметной области.

Полученные значения вероятностей $V_{u,y}^{0,T}$ заносят в средство хранения вероятностей нарушения свойств сущностей угрозами 2. Указанное средство хранения 2 может быть выполнено в виде набора регистров для хранения двумерной таблицы размером $B \times A$. Первый индекс в таблице соответствует номеру угрозы, а второй - номеру свойства сущности в системе. В каждом регистре хранится одно значение вероятности $V_{u,y}^{0,T}$.

5. Для каждого свойства u сущности o определяют прогнозируемое время t_{uk}^0 в промежутке времени T , в течение которого угрозы в случае своей реализации будут нарушать это свойство сущности при отсутствии контрмер.

Указанное время t_{uk}^0 , как и вероятность нарушения свойств сущностей угрозами $V_{u,y}^{0,T}$, может определяться любым доступным способом, в том числе могут

использоваться следующие методы:

- аналитический, посредством расчета значений;
- статистический, посредством применения статистики возникновения угроз в аналогичных видах деятельности;
- экспертный, посредством сбора и обработки мнений экспертов в предметной области.

Найденные значения времен t_{uk}^0 записывают в средства хранения прогнозируемого времени нарушения свойств сущностей 4. Каждое из указанных средств хранения 4 целесообразно выполнять в виде регистра данных.

6. Определяют возможные контрмеры. На этом этапе выявляют максимально возможное количество контрмер (правовых, финансовых, страховых, организационных, технических, организационно-технических и других мер и средств), которые могут позволить реализовать хотя бы одну из стратегий управления рисками в отношении выявленных на этапе 4 угроз и применимых в отношении выявленных на этапе 1 сущностей.

Далее C обозначает общее число выявленных контрмер.

7. Для каждой контрмеры k определяют функции f , которые эта контрмера выполняет для нейтрализации угроз. Здесь f - номер функции, $f=1, \dots, F^k$; F^k - количество функций у контрмеры k .

8. Определяют зависимости между функциями контрмер и записывают их в соответствующем средстве хранения 5. Зависимость между функциями контрмер представлена в виде ориентированного графа. Каждой дуге графа соответствует одна функция какой-либо контрмеры.

Каждому узлу графа соответствует состояние вида деятельности, характеризуемое той или иной степенью защиты от одной или нескольких угроз и являющееся результатом выполнения контрмерой ее функций. Узлы графа разделяются на начальные, промежуточные и целевые.

Начальные узлы не содержат входящих в них дуг. Совокупность начальных узлов соответствует состоянию такой системы защиты вида деятельности от рисков, при которой контрмеры отсутствуют.

Целевые узлы не содержат выходящих из них дуг. Каждый целевой узел

соответствует состоянию системы защиты вида деятельности от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких начальных узлов к целевому узлу.

Промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты вида деятельности, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы.

Каждой дуге графа зависимостей между функциями контрмер, исходящей из узла i и входящей в узел j , соответствует функция f контрмеры k . Такая функция обозначается далее $f_{ij}^{k,m}$, где m - порядковый номер дуги, соединяющей узлы i и j и направленной из узла i в узел j , $m=1, \dots, M_{ij}$. M_{ij} соответствует числу дуг, выходящих из узла i и входящих в узел j .

Средство хранения зависимостей между функциями контрмер каждой тройке номеров $\{i, j, m\}$ ставит в соответствие пару номеров $\{k, j\}$.

Средство хранения зависимостей между функциями контрмер может быть выполнено в виде массива наборов регистров, в котором каждый набор регистров относится к одной дуге графа и содержит четыре регистра для хранения:

- номера узла, из которого выходит дуга;
- номера узла, в который входит дуга;
- номера контрмеры;
- номера функции контрмеры, которая соответствует дуге.

9. Определяют показатели контрмер. Для каждой контрмеры k ($k=1, \dots, C$) определяют следующие показатели:

- стоимость контрмеры s_k^T ;
- вероятность $v_{y,f}^k$ того, что контрмера k не выполнит свою функцию f в отношении

угрозы y в случае ее реализации;

- время t_f^k , необходимое на реализацию функции f контрмеры k , в течение которого угрозы наносят ущерб деятельности, нарушая свойства сущностей;
- стоимость s_f^k реализации функции f контрмеры k в случае ее использования для

нейтрализации угрозы.

Значения параметров записывают в средство показателей контрмер б.

9.1. Стоимость контрмеры s_k^T определяют как сумму следующих затрат:

- постоянных затрат на эксплуатацию контрмеры;
- разовых затрат, например, на внедрение, применение, установку, закупку контрмеры;

- других возможных видов постоянных или разовых затрат, связанных с использованием контрмеры.

9.2. Вероятность $v_{y,f}^k$ и время t_f^k могут определяться любым доступным способом, в

том числе могут использоваться следующие методы:

- аналитический, посредством расчета значений вероятности;
- статистический, посредством применения статистики предотвращения угроз;
- практический, посредством проведения испытаний эффективности конкретных контрмер;

- экспертный, посредством сбора и обработки мнений экспертов в предметной области относительно величины вероятностей угроз.

Вероятность $v_{y,f}^k$ того, что контрмера k не выполнит свою функцию f в отношении угрозы y , определяется в отдельности для каждой функции f контрмеры в отношении

каждой угрозы u , на нейтрализацию которой направлена эта функция f .

Время t_f^k , необходимое на реализацию функции f контрмеры k , определяется для каждой функции f контрмеры k .

5 9.3. Стоимость реализации s_f^k функций контрмер может определяться практически, аналитически либо иным другим способом, дающим приемлемый результат.

Практическое определение стоимости реализации функции контрмеры может, например, заключаться в определении стоимости вызова ремонтной организации.

10 Введенная информация из средств хранения 1, 2, 4, 5, 6 поступает на вход следующих блоков:

- блока определения стоимости набора контрмер 7;
- блока определения остаточного риска для набора контрмер 8;
- блока определения остаточного ущерба для набора контрмер 9.

15 На управляющий вход каждого из указанных блоков 7, 8, 9 поступает информация, задающая набор контрмер z , одинаковый для всех трех блоков 7-9. Указанная информация поступает из управляющего выхода блока определения оптимального набора контрмер 10. В зависимости от состояния управляющего входа каждый из

20 блоков 7-9 выдает на свой выход значение параметра, характеризующего набор контрмер z :

- блок определения стоимости набора контрмер 7 выдает стоимость $s_{z\text{то}}^T$ варианта системы защиты, представленного набором контрмер z ;

25 - блок определения остаточного риска 8 выдает остаточный риск $s_{z\text{ор}}^T$ варианта системы защиты;

- блок определения остаточного ущерба 9 выдает остаточный ущерб $s_{z\text{ой}}^T$ варианта системы защиты.

30 При этом стоимость набора контрмер $s_{z\text{то}}^T = \sum_{x=1}^{C_z} s_{k_x^z}^T$ определяется как сумма

стоимости каждой контрмеры, входящей в набор z .

Здесь C_z - количество контрмер в наборе z ;

35 z - номер набора контрмер, $z=1, \dots, Q$;

Q - количество возможных наборов контрмер, $Q=2^C$;

k_x^z - номер контрмеры, стоящей в наборе z в позиции x .

Остаточный риск варианта системы защиты определяется из следующего

40 выражения:

$$s_{z\text{ор}}^T = \sum_{o=1}^O \sum_{u=1}^{U^o} (s_{\text{ulos}}^o(t_{uk}^o)) \times \sum_{y=1}^B (v_{u,y}^{o,T} \times v_{ys}^Z)$$

Здесь сумма произведений вероятностей рассчитывается как сумма совместных событий.

45 Здесь v_{ys}^z - вероятность того, что набор контрмер z (вариант системы защиты) не

сможет снизить ущерб от угрозы u в случае ее реализации. v_{ys}^z есть произведение

вероятностей недостижения каждого из целевых узлов графа. Расчет v_{ys}^z производится

50 следующим образом.

Для каждого из узлов графа j , начиная с начальных узлов, вычисляются значения вероятностей недостижения этих узлов, то есть вероятностей того, что для любого существующего пути от начального узла к узлу j найдется хотя бы одна функция

контрмеры, которая не будет выполнена. При этом рассматриваются только те дуги графа, которым соответствуют функции рассматриваемого набора контрмер z. При этом очевидно, что вероятности недостижения начальных узлов равны нулю, а вероятности недостижения целевых узлов, в которые не входит ни одна функция контрмеры, равны единице.

$$V_{y,j}^z = \prod_{\forall i \in f_{i,j}^k} \left(V_{y,i}^z + \prod_{m=1}^{M_{i,j}} V_{y,f_{i,j}^{k,m}}^k - V_{y,i}^z \times \prod_{m=1}^{M_{i,j}} V_{y,f_{i,j}^{k,m}}^k \right).$$

Здесь $V_{y,i}^z$, $V_{y,j}^z$ - вероятности недостижения соответственно узлов i и j в наборе контрмер z;

$\forall i \in f_{i,j}^k$ означает все узлы i, для которых существуют функции f контрмеры k, входящей в набор z, такие, что соответствующие этим функциям дуги графа направлены из узла i в узел j;

$V_{y,f_{i,j}^{k,m}}^k$ - вероятность того, что контрмера k не выполнит свою функцию $f_{i,j}^{k,m}$ в отношении угрозы y.

Затем определяют $V_{yS}^z = \prod_{\forall \text{целевых } j} V_{y,j}^z$ как произведение вероятностей $V_{y,j}^z$ для всех узлов, являющихся целевыми узлами.

Остаточный ущерб варианта системы защиты определяется из следующего выражения:

$$S_{zoy}^T = \sum_{o=1}^O \sum_{u=1}^{U^o} \sum_{y=1}^B \left(\frac{\sum_{n=1}^{N^{z,y}} (S_{u \text{ los}}^o \left(\sum_{\forall i,j,m \in K_y^n} t_{f_{i,j}^{k,m}}^k \right) + \sum_{\forall i,j,m \in K_y^n} S_{f_{i,j}^{k,m}}^k \right) \times V_{yc}^n}{N^{z,y}} V_{u,y}^{o,T} \right)$$

Здесь K_y^n - один из n путей нейтрализации угрозы y, характеризуемый маршрутом в графе зависимости между функциями контрмер из начального узла, характеризующего отсутствие контрмер в отношении угрозы y, в один из целевых узлов, характеризующий нейтрализацию угрозы y. $n=1, \dots, N^{z,y}$. $N^{z,y}$ - количество путей нейтрализации угрозы y в наборе контрмер z;

$\sum_{\forall i,j,m \in K_y^n} t_{f_{i,j}^{k,m}}^k$ - сумма времен, необходимых на реализацию функций f, соответствующих дугам, входящим в маршрут K_y^n нейтрализации угрозы y;

$\sum_{\forall i,j,m \in K_y^n} S_{f_{i,j}^{k,m}}^k$ - сумма стоимостей реализации функций f, соответствующих дугам, входящим в маршрут K_y^n нейтрализации угрозы y;

V_{yc}^o - вероятность того, что для нейтрализации ущерба от угрозы sработает маршрут K_y^n , рассчитываемая по формуле $V_{yc}^n = 1 - \sum_{\forall i,j,m \in K_y^n} V_{y,f_{i,j}^{k,m}}^k$ где сумма вероятностей

рассчитывается как сумма совместных событий.

Значения с выходов блока определения стоимости набора контрмер, блока определения остаточного риска и блока определения остаточного ущерба попадают на входы блока определения оптимального набора контрмер.

Для определения оптимального набора контрмер соответствующий блок выполняет перебор вариантов организации системы защиты (генерацию наборов контрмер), определяя для каждого варианта значение $S_z = S_{z_{tco}}^T + S_{zor}^T + S_{zoy}^T$. При этом

5 частным случаем набора контрмер является, например, полное отсутствие контрмер. Вариант системы защиты, которому соответствует минимальное значение S_z , будет оптимальным с точки зрения минимизации рисков. Сведения об оптимальном варианте системы защиты с выхода блока определения оптимального набора контрмер поступают на средство вывода информации об оптимальном наборе контрмер. Туда же могут поступать сведения о промежуточных этапах работы системы оптимизации рисков и, в частности, текущие значения набора контрмер, его стоимости, остаточного риска и остаточного ущерба.

15 Генерация вариантов организации системы защиты от рисков может производиться произвольным способом, например:

- путем полного перебора всех возможных вариантов. Данный способ дает возможность поиска наиболее оптимального варианта системы защиты от рисков, однако при большом количестве контрмер требует значительного машинного времени;

20 - путем использования любого возможного метода оптимизации перебора. Данный способ также дает возможность поиска наиболее оптимального варианта системы защиты от рисков, но, возможно, с некоторой погрешностью;

25 - путем произвольного задания вариантов, что дает возможность проверки эффективности конкретных вариантов организации системы защиты от рисков.

Пример выполнения системы. Система может быть реализована в виде компьютерной системы, снабженной процессором и памятью, причем память содержит данные и команды программного обеспечения, исполняемые процессором, для:

30 - получения для каждого свойства сущности размера ущерба в заданный момент времени от начала нарушения этого свойства сущности;

- получения для каждого свойства сущности в отношении каждой угрозы вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

35 - получения для каждого свойства сущности прогнозируемого времени его нарушения в случае реализации угроз и отсутствия контрмер;

- получения перечней функций контрмер таких, что каждый перечень соответствует пути в графе зависимости функций контрмер между двумя заданными узлами;

- получения для каждой контрмеры ее стоимости;

40 - получения для каждой функции каждой контрмеры стоимости ее реализации для нейтрализации угроз;

- получения для каждой функции каждой контрмеры времени, необходимого на реализацию этой функции;

45 - получения для каждой функции каждой контрмеры вероятностей того, что функция не будет выполнена в отношении каждой из угроз;

- генерирования наборов контрмер;

- вычисления на основе упомянутых выше полученных значений для каждого набора контрмер стоимости набора контрмер;

50 - вычисления на основе упомянутых выше полученных значений для каждого набора контрмер остаточного риска;

- вычисления на основе упомянутых выше полученных значений для каждого набора контрмер остаточного ущерба;

- определения такого набора контрмер, для которого сумма стоимости, остаточного риска и остаточного ущерба минимальна.

Работа системы минимизации рисков поясняется следующим иллюстративным примером.

5

1. Выявлены следующие сущности:

Номер сущности (o)	Наименование сущности
1	Компьютер с ценной информацией
2	Бумажный документ с данными по премиям

10

Число сущностей $O=2$

Требуется минимизировать риск при функционировании вида деятельности на протяжении одного года ($T=1$ год).

15

2. Для выявленных сущностей свойствами, нарушение которых потенциально может нанести ущерб эффективности функционирования рассматриваемого вида деятельности, являются:

o	Сущность	Номер свойства (u)	Наименование свойства
1	Компьютер с ценной информацией	1	Конфиденциальность информации
		2	Целостность информации
2	Бумажный документ с данными по премиям	1	Конфиденциальность информации

20

Число свойств сущности №1 $U^1=2$

25

Число свойств сущности №2 $U^2=1$

3. Ожидаемый размер ущерба $s_{ulos}^o = s_{ulos}^o(t)$, который будет нанесен деятельности при нарушении каждого из свойств каждой сущности в отдельности в условиях отсутствия контрмер, определен практически в нескольких временных точках с момента нарушения свойства сущности:

30

o	Сущность	u	Свойство	Ожидаемый размер ущерба, тыс.руб.				
				T=0 час	1 час	5 дней	1 мес	1 год
1	Компьютер с ценной информацией	1	Конфиденциальность информации	0	0	10	100	1000
		2	Целостность информации	0	200	200	500	500
2	Бумажный документ с данными по премиям	1	Конфиденциальность информации	500	500	500	500	500

35

При необходимости нахождения значения ожидаемого размера ущерба в произвольной точке времени производится аппроксимация известными способами. Значения ожидаемого размера ущерба записывают в средства хранения размеров ущерба 1.

40

4. Свойства сущностей могут нарушить следующие угрозы:

45

Номер угрозы (y)	Наименование угрозы
1	Кража компьютера
2	Пожар
3	Кража документа

50

Число угроз $V=3$.

Вероятности $v_{u,y}^{o,T}$ того, что реализация угрозы y приведет к нарушению свойства и сущности o за период времени T , определены на основе статистических данных и

показаны в следующей таблице размером В×А:

	Угроза: у	1	2	3
Свойство: {o, u}				
5 {1, 1}		0,1	0	0
{1, 2}		0	0,2	0
{2, 1}		0	0	0,1

5. Для всех свойств сущностей экспертным методом установлено, что прогнозируемое время t_{uk}^0 , в течение которого угрозы в случае своей реализации будут нарушать эти свойства сущностей при отсутствии контрмер, равно одному году.

6. Определены следующие контрмеры:

15 Номер контрмеры (k)	Наименование контрмеры
1	Установка замка на дверь
2	Установка автоматического пожаротушения (АПТ)
3	Покупка сейфа

Число контрмер $C=3$

7. Контрмера №1 «установка замка на дверь» выполняет одну функцию - предотвращение угрозы ($f=1$) в отношении угроз №1 «кража компьютера» и №3 «кража документа».

Контрмера №2 «установка АПТ» выполняет две функции в отношении угрозы №2 «пожар»:

- обнаружение угрозы ($f=1$);
- нейтрализация угрозы ($f=2$).

Контрмера №3 «покупка сейфа» выполняет одну функцию - предотвращение угрозы ($f=1$) в отношении угрозы №3 «кража документа».

8. Ориентированный граф зависимости между функциями контрмер для этого примера представлен на фиг.3. Этот граф представлен в средстве хранения 5 следующими соответствиями $\{i,j,m\} \rightarrow \{k,f\}$:

- $\{1, 2, 1\} \rightarrow \{1, 1\}$;
- $\{3, 4, 1\} \rightarrow \{1, 1\}$;
- 35 - $\{3, 4, 2\} \rightarrow \{3, 1\}$;
- $\{5, 6, 1\} \rightarrow \{2, 1\}$;
- $\{6, 7, 1\} \rightarrow \{2, 2\}$.

9. Показатели контрмер, определенные экспериментальным и расчетным способами, отражены в следующей таблице:

k	S_k^T , тыс. руб.	y	f	$V_{y,f}^k$	t_f^k , часов	S_f^k , руб.
1	2	1	1	0,1	0	0
		3	1	0,1	0	0
45 2	300	2	1	0,2	0,2	0
			2	0,1	0,3	0
3	10	3	1	0,01	0	0

Перебор контрмер блоком определения оптимального набора контрмер 10 и результаты расчета блоками 7, 8, 9 значений трех параметров приведены в следующей таблице:

Z	Контрмеры, входящие в набор			$S_{z_{tco}}^T$, тыс. руб.	$S_{z_{or}}^T$, тыс. руб.	$S_{z_{ou}}^T$, тыс. руб.	S_z , тыс. руб.
	1	2	3				
1	-	-	-	0	250	0	250
2	-	-	+	10	200,5	0	210,5
3	-	+	-	300	178	21,6	499,6
4	-	+	+	310	128,5	21,6	460,1
5	+	-	-	2	115	0	117
6	+	-	+	12	110,05	0	122,05
7	+	+	-	302	43	21,6	366,6
8	+	+	+	312	38,05	21,6	371,65

Наименьшей итоговой стоимостью обладает набор под номером 5 ($z=5$). В состав этого набора входит только одна контрмера - «Установка замка на дверь».

Информация об этом наборе поступает из блока определения оптимального набора контрмер 10 в средство вывода результатов работы системы 11.

В заявляемом изобретении заявляемый технический результат «автоматический поиск наиболее оптимального решения, минимизирующего риск» достигается за счет того, что система минимизации рисков содержит:

- А средств хранения размеров ущерба;
- блок определения остаточного риска;

при этом каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности, при этом система дополнительно содержит:

- средство хранения вероятностей нарушения свойств сущностей угрозами, выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

- А средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

- средство хранения зависимостей между функциями контрмер, представленных в форме ориентированного графа, в котором каждой дуге графа соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризующее степень защиты от одной или нескольких угроз, при этом узлы графа разделяются на начальные, промежуточные и целевые, начальные узлы не содержат входящих в них дуг, совокупность начальных узлов соответствует состоянию такой системы защиты от рисков, при которой контрмеры отсутствуют, целевые узлы не содержат выходящих из них дуг, при этом каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких начальных узлов к целевому узлу, промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты от рисков, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы;

- С средств хранения показателей контрмер, выполненных с возможностью хранения в составе параметров для каждой контрмеры: стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении каждой угрозы, на нейтрализацию которой эта функция направлена;

- блок определения стоимости $S_{z_{tco}}^T$ набора контрмер z , выполненный с

возможностью определения стоимости набора контрмер как суммы стоимостей каждой контрмеры, входящей в набор, при этом информационные входы блока определения стоимости набора контрмер связаны с информационными выходами средств хранения показателей контрмер;

- блок определения остаточного риска $S_{z_{or}}^T$ для набора контрмер z выполнен с

возможностью определения остаточного риска как суммы по всем свойствам сущностей произведения размера ущерба от нарушения свойства сущности за время, равное прогнозируемому времени нарушения свойства сущности, на сумму по всем угрозам произведения вероятности того, что реализация угрозы приведет к нарушению свойства сущности, на вероятность того, что набор контрмер не сможет снизить ущерб при реализации угрозы, при этом информационные входы блока определения остаточного риска связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средств хранения прогнозируемого времени нарушения свойств сущностей, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

- блок определения остаточного ущерба $S_{z_{oy}}^T$ для набора контрмер z , выполненный

с возможностью определения остаточного ущерба как суммы по всем сущностям, всем свойствам сущностей и всем угрозам произведения следующих величин:

а) вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

б) вычисленное для всех путей нейтрализации угрозы по графу зависимостей функций контрмер математическое ожидание произведения вероятности того, что для нейтрализации угрозы сработает конкретный путь, на сумму размера ущерба, вычисленного для времени, равного сумме времен срабатывания всех функций контрмер, входящих в этот путь, и суммарной стоимости реализации всех функций контрмер, входящих в этот путь,

при этом информационные входы блока определения остаточного ущерба связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

- блок определения оптимального набора контрмер, выполненный с возможностью определения такого набора контрмер z , для которого величина $S_z = S_{z_{tco}}^T + S_{z_{or}}^T + S_{z_{oy}}^T$

минимальна, при этом информационные входы блока определения оптимального набора контрмер связаны с информационными выходами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба, а управляющий выход блока определения оптимального набора контрмер связан с управляющими входами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба;

- средство вывода результатов, вход которого связан с информационным выходом блока определения оптимального набора контрмер. Благодаря такому техническому решению заявляемой системы минимизации рисков имеется возможность автоматической генерации наборов контрмер, оценки их параметров и выбора наиболее оптимального набора по трем заданным параметрам: стоимости, остаточному риску и остаточному ущербу.

В заявляемом изобретении заявляемый технический результат

«многопараметричность системы минимизации рисков» достигается за счет того, что система содержит:

- А средств хранения размеров ущерба;
- блок определения остаточного риска;

5 при этом каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности, при этом система дополнительно содержит:

10 - средство хранения вероятностей нарушения свойств сущностей угрозами, выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

15 - А средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

20 - средство хранения зависимостей между функциями контрмер, представленных в форме ориентированного графа, в котором каждой дуге графа соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризующее степень защиты от одной или нескольких угроз, при этом узлы графа разделяются на начальные, промежуточные и целевые, начальные узлы не содержат входящих в них дуг, совокупность начальных узлов соответствует состоянию такой системы защиты от рисков, при которой контрмеры отсутствуют, целевые узлы не содержат выходящих из них дуг, при этом каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько 25 угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких начальных узлов к целевому узлу, промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты от рисков, являющиеся результатом выполнения 30 контрмерами функций, дуги которых входят в эти узлы;

35 - С средств хранения показателей контрмер, выполненных с возможностью хранения в составе параметров для каждой контрмеры: стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении каждой угрозы, на 40 нейтрализацию которой эта функция направлена;

45 - блок определения стоимости S_{ztc}^T набора контрмер z , выполненный с возможностью определения стоимости набора контрмер как суммы стоимостей 40 каждой контрмеры, входящей в набор, при этом информационные входы блока определения стоимости набора контрмер связаны с информационными выходами средств хранения показателей контрмер;

50 - блок определения остаточного риска S_{zot}^T для набора контрмер z выполнен с возможностью определения остаточного риска как суммы по всем свойствам сущностей произведения размера ущерба от нарушения свойства сущности за время, равное прогнозируемому времени нарушения свойства сущности, на сумму по всем угрозам произведения вероятности того, что реализация угрозы приведет к 50 нарушению свойства сущности, на вероятность того, что набор контрмер не сможет снизить ущерб при реализации угрозы, при этом информационные входы блока определения остаточного риска связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств

сущностей угрозами, средств хранения прогнозируемого времени нарушения свойств сущностей, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

5 - блок определения остаточного ущерба s_{zoy}^T для набора контрмер z , выполненный с возможностью определения остаточного ущерба как суммы по всем сущностям, всем свойствам сущностей и всем угрозам произведения следующих величин:

а) вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

10 б) вычисленное для всех путей нейтрализации угрозы по графу зависимостей функций контрмер математическое ожидание произведения вероятности того, что для нейтрализации угрозы сработает конкретный путь, на сумму размера ущерба, вычисленного для времени, равного сумме времен срабатывания всех функций контрмер, входящих в этот путь, и суммарной стоимости реализации всех функций контрмер, входящих в этот путь,

при этом информационные входы блока определения остаточного ущерба связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

20 - блок определения оптимального набора контрмер, выполненный с возможностью определения такого набора контрмер z , для которого величина $s_z = s_{zto}^T + s_{zor}^T + s_{zoy}^T$

25 минимальна, при этом информационные входы блока определения оптимального набора контрмер связаны с информационными выходами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба, а управляющий выход блока определения оптимального набора контрмер связан с управляющими входами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба. Многопараметричность обусловлена обеспечением возможности одновременной оценки эффективности набора контрмер (системы защиты) по трем параметрам: стоимости, остаточного риска и остаточного ущерба.

35 В заявляемом изобретении заявляемый технический результат «повышение точности вычисления параметров» достигается за счет того, что:

- каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности;

40 - система содержит средство хранения вероятностей нарушения свойств сущностей угрозами, выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

45 - система содержит А средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

50 - система содержит средство хранения зависимостей между функциями контрмер, представленных в форме ориентированного графа, в котором каждой дуге графа соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризующее степень защиты от одной или нескольких угроз, при этом узлы графа разделяются на начальные, промежуточные и целевые, начальные узлы не содержат входящих в них дуг, совокупность начальных узлов соответствует состоянию такой системы защиты от

рисков, при которой контрмеры отсутствуют, целевые узлы не содержат выходящих из них дуг, при этом каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких

5 начальных узлов к целевому узлу, промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты от рисков, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы;

10 - система содержит С средств хранения показателей контрмер, выполненных с возможностью хранения в составе параметров для каждой контрмеры: стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении

15 каждой угрозы, на нейтрализацию которой эта функция направлена;

- система содержит блок определения стоимости S_{zico}^T набора контрмер z, выполненный с возможностью определения стоимости набора контрмер как суммы стоимостей каждой контрмеры, входящей в набор, при этом информационные входы

20 блока определения стоимости набора контрмер связаны с информационными выходами средств хранения показателей контрмер;

- система содержит блок определения остаточного риска S_{zor}^T для набора контрмер z, выполненный с возможностью определения остаточного риска как суммы

25 по всем свойствам сущностей произведения размера ущерба от нарушения свойства сущности за время, равное прогнозируемому времени нарушения свойства сущности, на сумму по всем угрозам произведения вероятности того, что реализация угрозы приведет к нарушению свойства сущности, на вероятность того, что набор контрмер не сможет снизить ущерб при реализации угрозы, при этом информационные входы

30 блока определения остаточного риска связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средств хранения прогнозируемого времени нарушения свойств сущностей, средства хранения зависимостей между функциями контрмер, средств

35 хранения показателей контрмер;

- система содержит блок определения остаточного ущерба S_{zoy}^T для набора контрмер z, выполненный с возможностью определения остаточного ущерба как суммы по всем сущностям, всем свойствам сущностей и всем угрозам произведения

40 следующих величин:

а) вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

б) вычисленное для всех путей нейтрализации угрозы по графу зависимостей функций контрмер математическое ожидание произведения вероятности того, что для

45 нейтрализации угрозы сработает конкретный путь, на сумму размера ущерба, вычисленного для времени, равного сумме времен срабатывания всех функций контрмер, входящих в этот путь, и суммарной стоимости реализации всех функций контрмер, входящих в этот путь,

50 при этом информационные входы блока определения остаточного ущерба связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер.

Выполнение средства хранения размеров ущерба 1 с возможностью хранения зависимости этого размера от времени, что наблюдается в действительности, повышает точность, с которой определяются остаточный ущерб наборов контрмер. Кроме того, «повышение точности вычисления параметров» достигается за счет того, что система содержит средство хранения 5 зависимостей между функциями контрмер, а также С средств хранения 6 показателей контрмер, которые позволяют учесть взаимное влияние контрмер, а также особенности реализации функций контрмер (возможные затраты в случае использования функций, необходимое на выполнение функции время). В совокупности указанные факторы приводят к повышению точности количественной оценки эффективности набора контрмер.

В заявляемом изобретении заявляемый технический результат «расширение области применения системы минимизации рисков» достигается за счет того, что:

- каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности;

- система содержит средство хранения вероятностей нарушения свойств сущностей угрозами, выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

- система содержит средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

- система содержит средство хранения зависимостей между функциями контрмер, представленных в форме ориентированного графа, в котором каждой дуге графа соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризуемое степенью защиты от одной или нескольких угроз, при этом узлы графа разделяются на начальные, промежуточные и целевые, начальные узлы не содержат входящих в них дуг, совокупность начальных узлов соответствует состоянию такой системы защиты от рисков, при которой контрмеры отсутствуют, целевые узлы не содержат выходящих из них дуг, при этом каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких начальных узлов к целевому узлу, промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты от рисков, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы;

- система содержит С средств хранения показателей контрмер, выполненных с возможностью хранения в составе параметров для каждой контрмеры: стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении каждой угрозы, на нейтрализацию которой эта функция направлена.

В заявляемом изобретении заявляемый технический результат «унификация используемых системой минимизации рисков способов минимизации рисков и зависимостей между ними» достигается за счет того, что:

- каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности;

- система содержит средство хранения вероятностей нарушения свойств сущностей угрозами, выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

5 - система содержит А средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

- система содержит средство хранения зависимостей между функциями контрмер, представленных в форме ориентированного графа, в котором каждой дуге графа 10 соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризующее степень защиты от одной или нескольких угроз, при этом узлы графа разделяются на начальные, промежуточные и целевые, начальные узлы не содержат входящих в них дуг, совокупность начальных узлов соответствует состоянию такой системы защиты от 15 рисков, при которой контрмеры отсутствуют, целевые узлы не содержат выходящих из них дуг, при этом каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких 20 начальных узлов к целевому узлу, промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные состояния системы защиты от рисков, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы;

- система содержит С средств хранения показателей контрмер, выполненных с 25 возможностью хранения в составе параметров для каждой контрмеры: стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении 30 каждой угрозы, на нейтрализацию которой эта функция направлена.

Унификация используемых системой минимизации рисков способов минимизации рисков и зависимостей между ними обеспечивается, в основном, наличием в системе средства хранения 5 зависимостей между функциями контрмер, а также наличием С 35 средств хранения 6 показателей контрмер, которые дают универсальные методы описания эффективности разнообразных контрмер и их использования при оценке уровня риска.

Источники информации

1. Интернет-ресурс <http://www.dsec.ru>. Документация на продукт «Система оценки и 40 управления рисками «ГРИФ» ООО «Диджитал Секьюрети» - наиболее близкий аналог.
2. Интернет-ресурс <http://www.riskwatch.com/>.
3. Интернет-ресурс <http://www.cramm.com>.
4. Интернет-ресурс <http://www.security-risk-analysis.com/riskcon.htm>.

45 Формула изобретения

1. Система минимизации рисков, содержащая

- А средств хранения размеров ущерба;
- блок определения остаточного риска;

50 отличающаяся тем, что каждое средство хранения размера ущерба выполнено с возможностью хранения зависимости размера ущерба от времени, прошедшего с момента нарушения свойства сущности, при этом система дополнительно содержит:

- средство хранения вероятностей нарушения свойств сущностей угрозами,

выполненное с возможностью хранения для каждой угрозы в отношении каждого свойства каждой сущности значения вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

5 - А средств хранения прогнозируемого времени нарушения свойств сущностей в случае реализации угроз;

10 - средство хранения зависимостей между функциями контрмер, представленных в форме ориентированного графа, в котором каждой дуге графа соответствует одна функция какой-либо контрмеры, а каждому узлу графа соответствует состояние вида деятельности, характеризуемое степенью защиты от одной или нескольких угроз, при этом узлы графа разделяются на начальные, промежуточные и целевые, начальные узлы не содержат входящих в них дуг, совокупность начальных узлов соответствует состоянию такой системы защиты от рисков, при которой контрмеры отсутствуют, 15 целевые узлы не содержат выходящих из них дуг, при этом каждый целевой узел соответствует состоянию системы защиты от рисков, при котором одна или несколько угроз полностью нейтрализуются контрмерами, функции которых являются в графе путями от одного или нескольких начальных узлов к целевому узлу, промежуточные узлы содержат входящие и исходящие дуги и характеризуют промежуточные 20 состояния системы защиты от рисков, являющиеся результатом выполнения контрмерами функций, дуги которых входят в эти узлы;

- С средств хранения показателей контрмер, выполненных с возможностью хранения в составе параметров для каждой контрмеры:

25 стоимости контрмеры, значений времен, затрачиваемых на реализацию каждой функции контрмеры, вероятностей того, что контрмера не выполнит свою функцию в отношении угрозы, определяемых для каждой функции контрмеры в отношении каждой угрозы, на нейтрализацию которой эта функция направлена;

- блок определения стоимости $s_{z\text{тс}}^T$ набора контрмер z , выполненный с

30 возможностью определения стоимости набора контрмер как суммы стоимостей каждой контрмеры, входящей в набор, при этом информационные входы блока определения стоимости набора контрмер связаны с информационными выходами средств хранения показателей контрмер;

35 - блок определения остаточного риска $s_{z\text{оу}}^T$ для набора контрмер z выполнен с

40 возможностью определения остаточного риска как суммы по всем свойствам сущностей произведения размера ущерба от нарушения свойства сущности за время, равное прогнозируемому времени нарушения свойства сущности, на сумму по всем угрозам произведения вероятности того, что реализация угрозы приведет к 45 нарушению свойства сущности, на вероятность того, что набор контрмер не сможет снизить ущерб при реализации угрозы, при этом информационные входы блока определения остаточного риска связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средств хранения прогнозируемого времени нарушения свойств сущностей, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

- блок определения остаточного ущерба $s_{z\text{оу}}^T$ для набора контрмер z , выполненный

50 с возможностью определения остаточного ущерба как суммы по всем сущностям, всем свойствам сущностей и всем угрозам произведения следующих величин:

а) вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

б) вычисленное для всех путей нейтрализации угрозы по графу зависимостей функций контрмер математическое ожидание произведения вероятности того, что для нейтрализации угрозы сработает конкретный путь, на сумму размера ущерба, вычисленного для времени, равного сумме времен срабатывания всех функций контрмер, входящих в этот путь, и суммарной стоимости реализации всех функций контрмер, входящих в этот путь,

при этом информационные входы блока определения остаточного ущерба связаны с информационными выходами средств хранения размеров ущерба, средства хранения вероятностей нарушения свойств сущностей угрозами, средства хранения зависимостей между функциями контрмер, средств хранения показателей контрмер;

- блок определения оптимального набора контрмер, выполненный с возможностью определения такого набора контрмер z , для которого величина $S_z = S_{z_{tco}}^T + S_{z_{or}}^T + S_{z_{oy}}^T$

минимальна, при этом информационные входы блока определения оптимального набора контрмер связаны с информационными выходами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба, а управляющий выход блока определения оптимального набора контрмер связан с управляющими входами блоков определения стоимости набора контрмер, остаточного риска и остаточного ущерба;

- средство вывода результатов, вход которого связан с информационным выходом блока определения оптимального набора контрмер.

2. Система по п.1, отличающаяся тем, что каждое средство хранения размера ущерба выполнено в виде набора регистров, реализующего одномерный массив размеров ущерба, индексом которого является время от нарушения свойства сущности.

3. Система по п.1, отличающаяся тем, что каждое средство хранения размеров ущерба выполнено в виде блока хранения, имеющего вход времени и информационный выход размера ущерба.

4. Система по п.1, отличающаяся тем, что средство хранения вероятностей нарушения свойств сущностей угрозами выполнено в виде набора регистров для хранения двумерной таблицы размером $B \times A$, при этом первый индекс в таблице соответствует номеру угрозы, а второй - номеру свойства сущности.

5. Система по п.1, отличающаяся тем, что средство хранения зависимостей между функциями контрмер выполнено в виде массива наборов регистров, в котором каждый набор регистров относится к одной дуге графа и содержит четыре регистра для хранения соответственно:

- номера узла, из которого выходит дуга;
- номера узла, в который входит дуга;
- номера контрмеры;
- номера функции контрмеры, которая соответствует дуге.

6. Система по п.1, отличающаяся тем, что она выполнена в виде процессора и памяти, причем память содержит данные и команды программного обеспечения, исполняемые процессором, для:

- получения для каждого свойства сущности размера ущерба в заданный момент времени от начала нарушения этого свойства сущности;

- получения для каждого свойства сущности в отношении каждой угрозы

вероятности того, что реализация угрозы приведет к нарушению свойства сущности;

- получения для каждого свойства сущности прогнозируемого времени его нарушения в случае реализации угроз в отношении этого свойства;

- получения перечней функций контрмер таких, что каждый перечень соответствует

пути в графе зависимости функций контрмер между двумя заданными узлами;

- получения для каждой контрмеры ее стоимости;

- получения для каждой функции каждой контрмеры стоимости ее реализации для
нейтрализации угроз;

5 - получения для каждой функции каждой контрмеры времени, необходимого на
реализацию этой функции;

- получения для каждой функции каждой контрмеры вероятностей того, что
функция не будет выполнена в отношении каждой из угроз;

10 - генерирования наборов контрмер;

- вычисления на основе упомянутых выше полученных значений для каждого
набора контрмер стоимости набора контрмер;

- вычисления на основе упомянутых выше полученных значений для каждого
набора контрмер остаточного риска;

15 - вычисления на основе упомянутых выше полученных значений для каждого
набора контрмер остаточного ущерба;

- определения такого набора контрмер, для которого сумма стоимости,
остаточного риска и остаточного ущерба минимальна.

20

25

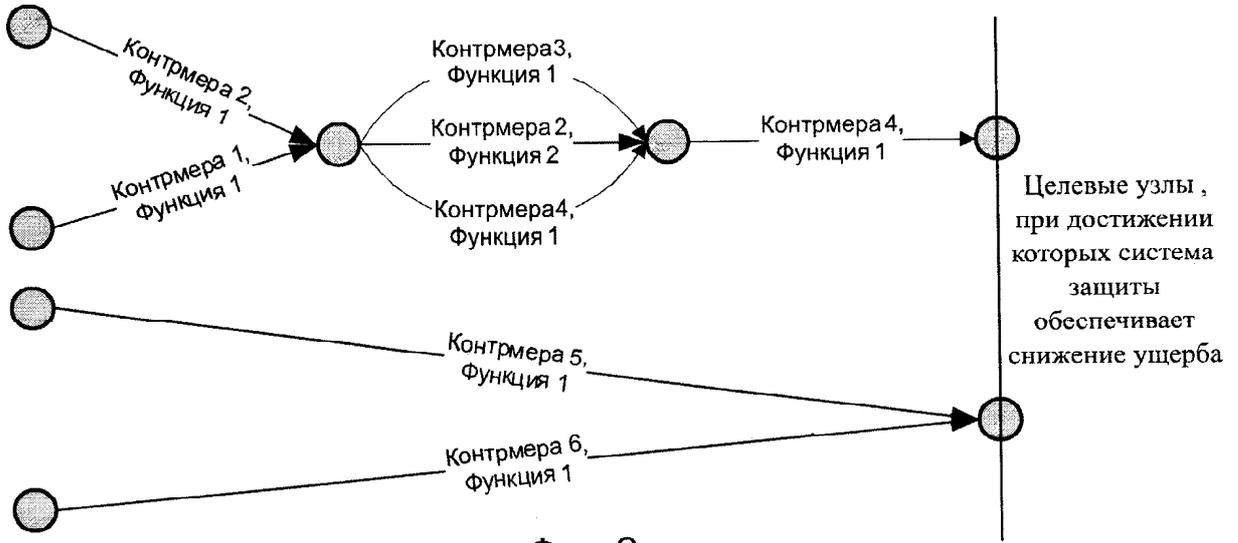
30

35

40

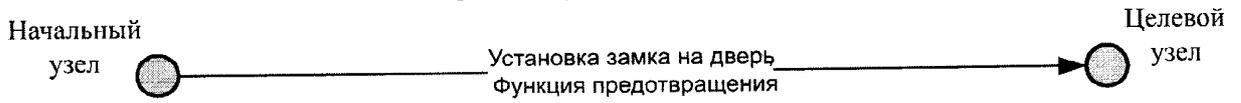
45

50

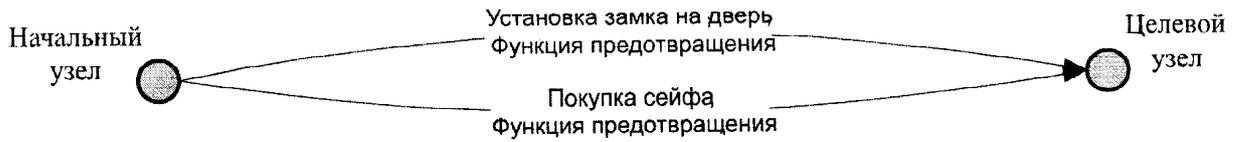


ФИГ. 2

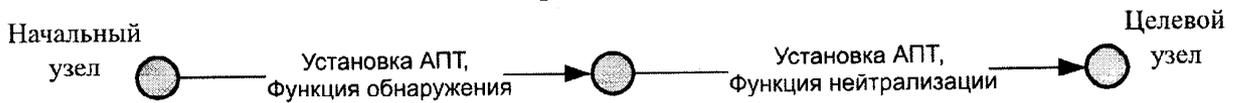
Угроза – Кража компьютера



Угроза – Кража документа



Угроза – Пожар



ФИГ. 3