На правах рукописи

СТЕПАНОВА Екатерина Сергеевна

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Специальность 05.13.19 –
Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Уфа – 2013

Работа выполнена на кафедре
вычислительной техники и защиты информации
ФГБОУ ВПО «Уфимский государственный авиационный технический университет»

Научный руководитель: д-р техн. наук, доцент,
Машкина Ирина Владимировна

Официальные оппоненты: д-р техн. наук, профессор,
Мельников Андрей Витальевич
ФГБОУ ВПО «Челябинский государственный университет», проректор по научной работе

канд. техн. наук, доцент,
Пестриков Владимир Анатольевич
Уфимский филиал Северо-Западного института повышения квалификации Федеральной службы Российской Федерации по контролю за оборотом наркотиков, профессор кафедры специальных дисциплин

Ведущая организация: **Южно-Российский региональный учебно-научный центр по проблемам информационной безопасности в системе высшей школы Южного федерального университета**

Защита диссертации состоится “ 31 ” мая 2013 г. в 10:00 часов
на заседании диссертационного совета Д-212.288.07
при Уфимском государственном авиационном техническом университете
в активом зале корпуса № 1 по адресу: 450000, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке
Уфимского государственного авиационного технического университета.

Автореферат разослан «26» апреля 2013 года

Ученый секретарь
диссертационного совета
д-р. техн. наук, доцент **И.Л. Виноградова**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Для реализации информационных сервисов в современных банковской и финансовой сферах, в сфере государственного управления и промышленного производства широко применяются информационные системы (ИС), обладающие сложной, зачастую распределенной инфраструктурой. Качество реализации сервисов неразрывно связано с вопросами обеспечения безопасности при использовании системы защиты информации (СЗИ).

Международные и национальные стандарты в области информационной безопасности (ИБ) декларируют необходимость управления рисками в СЗИ, не предлагая какой-либо методологии. Основополагающим этапом управления рисками нарушения ИБ является их оценка; значение уровня риска определяется как функция вероятностей реализации угроз защищенности информации и ее ценности с точки зрения последствий для бизнеса. Количественное оценивание уровня риска позволяет определить потенциально возможную величину относительного ущерба информационной системе от реализации угроз и сформировать план обработки риска.

Вместе с тем, известные программные продукты, автоматизирующие процесс оценивания риска, не в полной мере позволяют достоверно оценить уровень риска конкретного объекта защиты (ОЗ). Это связано с определением в них значений вероятностей угроз экспертным путем на основании статистических данных об инцидентах в области ИБ, с отсутствием возможности учесть специфику объекта защиты: особенности топологии сети и технологий обработки информации, сведения об используемых или планируемых средствах защиты (СрЗ) информации, оценить эффективность конкретного набора СрЗ. Как следствие, эти программные продукты могут быть использованы только на этапе эксплуатации, а не при проектировании СЗИ.

При оценке информационных рисков во внимание принимаются целенаправленные угрозы, так как защита от непреднамеренных угроз подразумевает использование организационных мер и средств повышения надежности технических и программных средств. В связи с этим, одной из задач в области оценки рисков нарушения ИБ является получение численной оценки уровней (вероятностей реализации) преднамеренных угроз.

В основе верификации уровней угроз защищенности информации лежит процесс моделирования угроз, воздействующих на информационную систему. Модель угроз, адекватная объекту защиты, построенная с учетом политики безопасности и наиболее полного перечня потенциально возможных угроз, – основа достоверной оценки их уровня. Сложность оценки вероятностей реализации угроз объясняется тем, что на сегодняшний день практически отсутствуют методы оценки, не основанные на статистике по инцидентам ИБ. Все еще мало исследованным при решении вопроса построения модели угроз в информационных системах остается такой перспективный подход, как нечеткие когнитивные карты (НКК).

Критичная ситуация в области оценки рисков усугубляется в связи с отсутствием методов получения параметра «ценность информации», основанных на достоверных сведениях об обрабатываемых на объекте защиты информационных активах (ИА).

Степень разработанности темы. Проблеме оценки рисков нарушения информационной безопасности посвящены работы А. М. Астахова, О. А. Бурдина, П. Д. Зегжды, А. А. Кононова, А. Г. Корченко, И. В. Машкиной, С. А. Нестерова, С. А. Петренко, С. В. Симонова, А. П. Росенко, Е. П. Тумояна, А. А. Шелупанова. Такой аспект, как оценка параметра «ценность критичной информации», отражен в работе А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. Вопросы изучения особенностей реализации атак достаточно подробно рассмотрены в трудах: С. В. Запечникова, Н. Г. Милославской, А. И. Толстого, Д. В. Ушакова, А. Г. Лукацкого, В. А. Сердюка.

На сегодняшний день практически отсутствуют методы, которые можно использовать при проектировании системы защиты информации, адекватность которых не зависит от наличия или отсутствия статистических данных в области инцидентов ИБ, экспертные знания в которых сведены к минимуму или основываются на объективных данных об объекте защиты. Таким образом, для успешного решения проблемы оценки рисков нарушения информационной безопасности необходимы модель угроз, формализованные методы оценки параметра «ценность информации» и уровней риска, а также автоматизированное программное средство, разработанные на основе методов системного анализа и необходимой интеллектуальной поддержки.

Цель работы

Целью работы является повышение эффективности оценивания защищенности (уровня риска) информационной системы от угроз нарушения информационной безопасности в процессе проектирования и эксплуатации системы защиты информации.

Задачи исследования

1. Разработать концептуальную модель преднамеренных угроз нарушения ИБ с использованием НКК для оценки риска в информационной системе.

2. Разработать метод оценки уровня риска в локальных сетевых сегментах (ЛСС) и в ИС в целом, а также IDEF0 модель оценивания, применимые при проектировании и эксплуатации системы защиты информации.

3. Разработать метод количественного оценивания параметра «ценность информационных активов локальных сетевых сегментов».

4. Разработать программный комплекс автоматизированной оценки риска нарушения информационной безопасности, реализующий предложенные модели и методы. Исследовать адекватность предложенных моделей и методов на основе вычислительных экспериментов.

Объектом исследования являются информационная система и протекающие в ней процессы информационного противоборства.

Предметом исследования выступают модели, методы оценки уровня риска нарушения ИБ и определения параметра «ценность информации».

Научная новизна

1. Новизна концептуальной *модели* преднамеренных угроз, *базирующейся* на построении нечетких когнитивных карт, *заключается* в визуализации путей распространения угроз в инфраструктуре информационной системы на основе разработанных матриц угроз, устанавливающих взаимосвязь между каждым источником и объектом атаки, что *позволяет* учесть используемые для осуществления угроз уязвимости коммуникационного оборудования, средств защиты и программного обеспечения при оценивании уровней угроз.

2. Новизна *метода* оценки риска нарушения информационной безопасности, *базирующегося* на построении разработанной концептуальной модели угроз, *заключается* в том, что выявляется зависимость значения риска каждого сегмента от ценности обрабатываемой информации и оценок значимости угроз от множества источников к одному объекту, а именно: значения уровней угроз на путях распространения определяются как произведения вероятности активизации угрозы и полученных нормированием приведенных в международной базе данных величин уязвимостей компонентов инфраструктуры и барьеров, выявляются максимальные значения уровней угроз от каждого возможного источника для вычисления результирующего значения уровня угрозы информационным активам сегмента, – что *позволяет* представить процесс оценивания наглядно в виде функциональной модели, оценить влияние архитектуры сети на значение риска нарушения информационной безопасности, сравнить эффективность различных наборов средств защиты в количественном выражении на стадии эксплуатации и при проектировании системы защиты информации.

3. Новизна *метода* оценивания ценности защищаемых информационных активов локальных сетевых сегментов *заключается* в том, что в качестве исходных данных при оценивании параметра, с использованием аппарата нечеткого логического вывода, принимается количество обрабатываемых в сегментах информационных активов определенных уровней критичности и число возможных видов последствий из перечня, приведенного в стандарте по информационной безопасности, что *позволяет* повысить достоверность оценивания для конкретного объекта защиты, минимизировать субъективность полученных оценок, учесть изменение ценности информации во времени и использовать этот параметр для оценки информационного риска.

4. Новизна программного комплекса, реализующего *метод оценки* уровня риска нарушения информационной безопасности, *заключается* в возможности автоматизированной модификации нечетких когнитивных карт, предусматривающей отображение только тех путей распространения угроз, на которых значения их уровней максимальны, что *позволяет* обосновать выбор контрмер и мест их установки, повысить оперативность и сократить трудозатраты.

Теоретическая и практическая значимость работы заключается:

- в разработанных методах оценки риска нарушения информационной безопасности и оценивания ценности критичной информации, апробированных

на практике при решении задач определения уровня защищенности информационной системы;

- в разработанном с использованием методологии функционального моделирования IDEF0 графическом представлении механизма построения модели угроз, оценивания ценности критичной информации и получения численной оценки уровней рисков нарушения информационной безопасности в локальных сетевых сегментах и в информационной системе в целом;
- в разработанном программном комплексе, позволяющем автоматизировать процесс получения уровня риска в соответствии с предлагаемым методом оценки риска нарушения ИБ.

Практическая значимость разработанных методов и средств заключается в повышении обоснованности выбора конкретного набора средств защиты и определения мест их установки при проектировании и модернизации СЗИ посредством анализа значений уровней риска.

Методология и методы исследования

При решении поставленных в диссертационной работе задач использованы методы системного анализа, теории множеств, теории нечетких когнитивных карт, теории нечетких множеств, методы обработки экспертной информации, а также методология функционального моделирования.

Положения, выносимые на защиту

1. Концептуальная *модель* преднамеренных *угроз* нарушения информационной безопасности в проекции на топологию сети, *базирующаяся* на построении нечетких когнитивных карт, *учитывающая* условия осуществления угроз через эксплуатируемые уязвимости компонентов инфраструктуры и *являющаяся* формой организации и представления знаний об особенностях распространения угроз на конкретном объекте защиты.

2. *Метод оценки* уровня *риска* нарушения информационной безопасности, *основанный* на построении разработанной концептуальной модели угроз, позволяющий представить процесс оценивания наглядно в виде функциональной модели, оценить влияние архитектуры сети на значение риска, сравнить эффективность различных наборов средств защиты в количественном выражении на стадии эксплуатации и при проектировании системы защиты информации.

3. Метод *оценки* параметра «*ценность* защищаемых информационных активов локальных сетевых сегментов», *базирующийся* на использовании достоверных данных об объекте защиты и *учитывающий* изменение ценности информации во времени.

4. Программный комплекс, автоматизирующий процесс оценки риска нарушения ИБ, позволяющий пользователю посредством анализа путей распространения угроз обосновать целесообразность внедрения определенных комплексов средств защиты при проектировании и необходимость внедрения дополнительных СрЗ при модернизации СЗИ.

Достоверность полученных результатов. Полученные в диссертационной работе результаты не противоречат известным теоретическим

положениям и подтверждаются результатами расчетов, апробации и внедрения предложенных в диссертации методов на предприятиях и в учебном процессе Уфимского государственного авиационного технического университета.

Апробация работы

Основные положения, представленные в диссертации, докладывались и обсуждались на научных конференциях. Наиболее значимыми из которых являются: XI, XII Международная научно-практическая конференция «Информационная безопасность», г. Таганрог, ТТИ ЮФУ, 2010, 2012; XVIII, XIX Всероссийская научно-практическая конференция «Проблемы информационной безопасности в системе высшей школы», г. Москва, МИФИ, 2011, 2012; IX Международная конференция «Когнитивный анализ и управление развитием ситуаций (*CASC*`2011)», г. Москва, ИПУ РАН, 2011; XI Всероссийский конкурс-конференция студентов и аспирантов по информационной безопасности SIBINFO-2011, г. Томск, ИСИБ ТУСУР.

Полученные результаты внедрены при модернизации систем защиты информации в сети государственного учреждения и ООО «Промэкспертиза».

Разработанный метод оценки риска нарушения ИБ и программный комплекс, реализующий метод, а также метод оценивания ценности критичной информации внедрены в учебный процесс подготовки студентов Уфимского государственного авиационного технического университета, обучающихся по специальности 090104 «Комплексная защита объектов информатизации».

Публикации

По теме диссертации опубликовано 19 печатных работ, в том числе 5 в рецензируемых журналах из списка ВАК, издано учебное пособие для дипломников, получено свидетельство о регистрации программы для ЭВМ.

Структура работы

Диссертация состоит из введения, четырех глав, заключения, изложенных на 188 страницах, списка литературы из 109 наименований, содержит 49 рисунков и 19 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность проблемы разработки метода оценки риска нарушения информационной безопасности. Формулируются цель и задачи исследования, представлены положения, выносимые на защиту, изложена научная новизна, практическая ценность работы, приводится краткая характеристика и сведения об ее апробации.

Первая глава посвящена анализу современной проблемы оценки риска нарушения информационной безопасности.

Проводится анализ стандартов, руководящих документов, известных публикаций, а также методов оценки информационного риска, реализованных в специализированных программных продуктах.

Рассмотрены методы оценивания ценности критичной информации. Показано, что основным недостатком известных количественных методов является необходимость наличия экспертов – представителей бизнеса с их

знанием бизнес-процессов и способностью выносить адекватные суждения относительно ценности активов. Отмечается необходимость создания метода оценивания ценности информации, в котором знания экспертов формализованы, а оценка обоснована какими-либо достоверными данными об объекте защиты.

Анализируются известные методы оценки уровня риска. В качестве их недостатков отмечаются: необходимость наличия достоверной статистики по инцидентам в области ИБ, ориентация на этап эксплуатации, а также либо чрезмерная обобщенность некоторых методов, что не дает возможности учесть специфику объекта защиты, либо излишняя детализированность, что чрезвычайно усложняет оценку защищенности конкретных ОЗ.

Проанализированы источники, в которых приведены подходы использования нечетких когнитивных карт. Отмечается, что широкие возможности соответствующего математического аппарата по моделированию и оцениванию сложных слабоструктурированных задач, которые практически не реализованы в рассматриваемых приложениях. Общим серьезным недостатком данных подходов является рассмотрение угрозы по принципу «черного ящика», что не позволяет с достаточной степенью детализации исследовать, проанализировать и оценить процесс осуществления сложной многоальтернативной последовательности действий по реализации угроз нарушения ИБ, как следствие оценка риска производится без учета инфраструктуры информационной системы.

Рассматриваются возможности, предоставляемые пользователям современных наиболее популярных программных продуктов, автоматизирующих процесс оценки риска. Отмечаются их недостатки, среди которых можно выделить: необходимость наличия высококвалифицированной группы экспертов, ориентированность на этап эксплуатации ИС, невозможность оценить влияние конкретных средств защиты и архитектуры сети на значение уровня риска нарушения ИБ.

Обосновывается актуальность создания методов оценивания ценности критичной информации и оценки риска нарушения информационной безопасности, свободных от выявленных недостатков. На основе анализа формулируются цель и основные задачи исследования.

Вторая глава посвящена разработке метода оценки риска нарушения информационной безопасности в сети.

При решении проблемы оценки риска нарушения ИБ предложено производить детализацию структуры ИС до уровня локальных сетевых сегментов. В качестве объекта атаки рассматривается локальный сетевой сегмент, в котором обрабатывается множество информационных активов заданных уровней критичности.

На основе теоретико-множественного подхода предлагается описание ИС – объекта защиты. Предлагается представление угрозы в виде кортежа:

$$U = \langle S, v(A), v(З^{С}), v(З^{Х}), v(ПО), O(C) \rangle, \quad (1)$$

где S – источник угрозы – субъект доступа (пользователь-нарушитель внутренний или внешний, злоумышленник или запущенные ими процессы); $v(A)$ – уязвимость оборудования в канале связи (коммутаторы, маршрутизаторы и др.); $v(З^{С})$, $v(З^{Х})$ – уязвимости сервисов безопасности на пути распространения угрозы, соответственно, сетевых и хостовых; $v(ПО)$ – уязвимость программного обеспечения, установленного на хосте-жертве; $O(C)$ – объект доступа в соответствующем сегменте.

Для определения перечня потенциально возможных угроз несанкционированного доступа (НСД) и утечки конфиденциальной информации предлагается построение матриц угроз, получаемых на основе матриц доступа на уровне ЛСС. Матрицы угроз определяют потенциально возможные угрозы, задавая пару «источник атаки» и «объект атаки». При оценке риска учитываются: угрозы НСД к информационным активам в случае, когда нарушитель пытается превысить свои привилегии; угрозы НСД, реализуемые пользователем одного подразделения, уровень доступа которого соответствует уровню критичности информации, обрабатываемой в другом подразделении, не имеющим в соответствии со своими функциональными обязанностями, определенными бизнес-требованиями, права доступа к ней; угрозы НСД, осуществляемые злоумышленниками; а также угрозы неконтролируемого распространения (утечки) информационных активов.

В работе для анализа рисков нарушения ИБ предлагается построение концептуальной модели угроз в виде нечетких когнитивных карт (рис. 1). Использование НКК позволяет произвести моделирование процессов распространения угроз ИС через эксплуатируемые уязвимости компонентов ее инфраструктуры. Разработанная модель предоставляет достаточную степень детализации, позволяет учитывать наличие потенциально большого числа альтернативных сценариев реализации угрозы. На рис. 2 приведена IDEF0 модель построения модели угроз ОЗ.

При анализе рисков во внимание принимается всё возможное множество путей распространения угроз от одного источника к одному объекту атаки. Необходимые для расчетов значения уровней угроз определяются как произведения вероятности активизации угрозы и уровней уязвимостей компонентов инфраструктуры, встречающихся на путях распространения угрозы:

$$P_j = P_{акт} \cdot \underset{z \in Z_j}{T} w_{z,z+1}, \qquad (2)$$

где $P_{акт}$ – вероятность активизации угрозы; $w_{z,z+1}$ – уровень уязвимости компонента инфраструктуры, полученный нормализацией величины, рассчитанной в соответствии с методикой Common Vulnerability Scoring System.

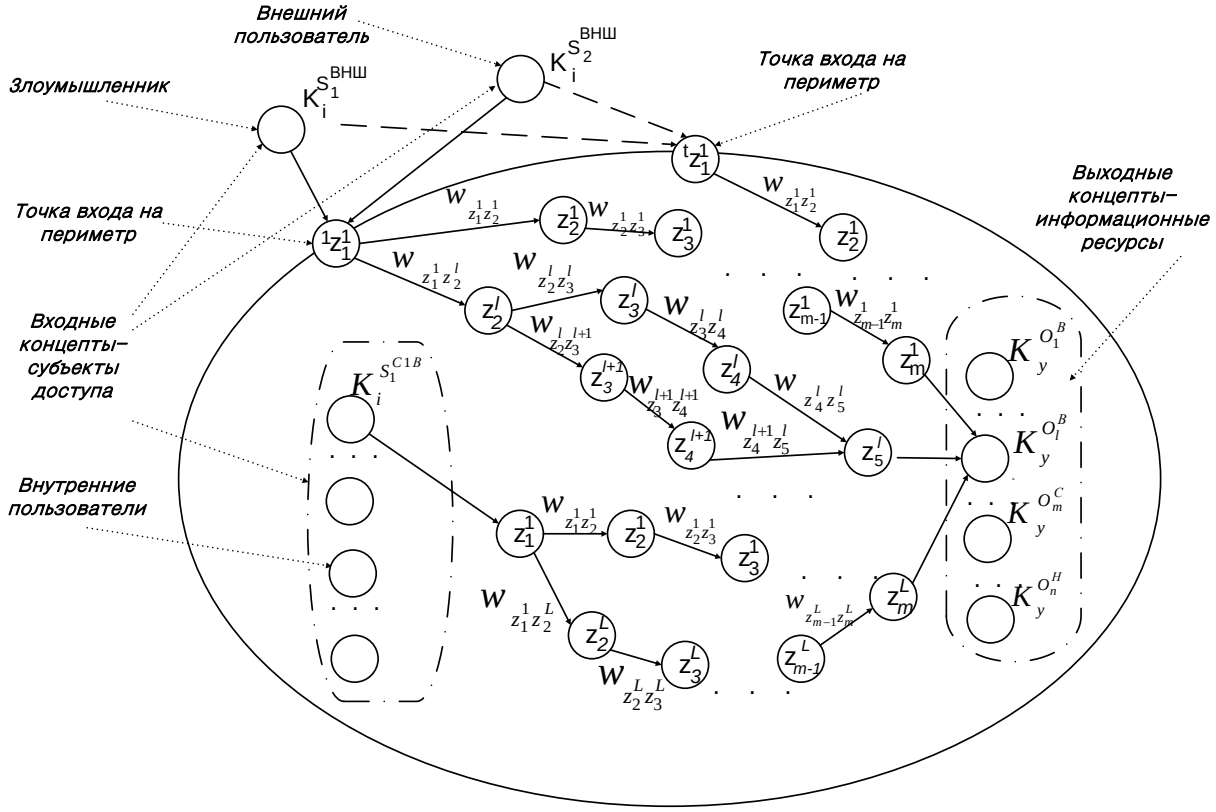

Рисунок 1– Нечеткая когнитивная карта – модель угроз НСД

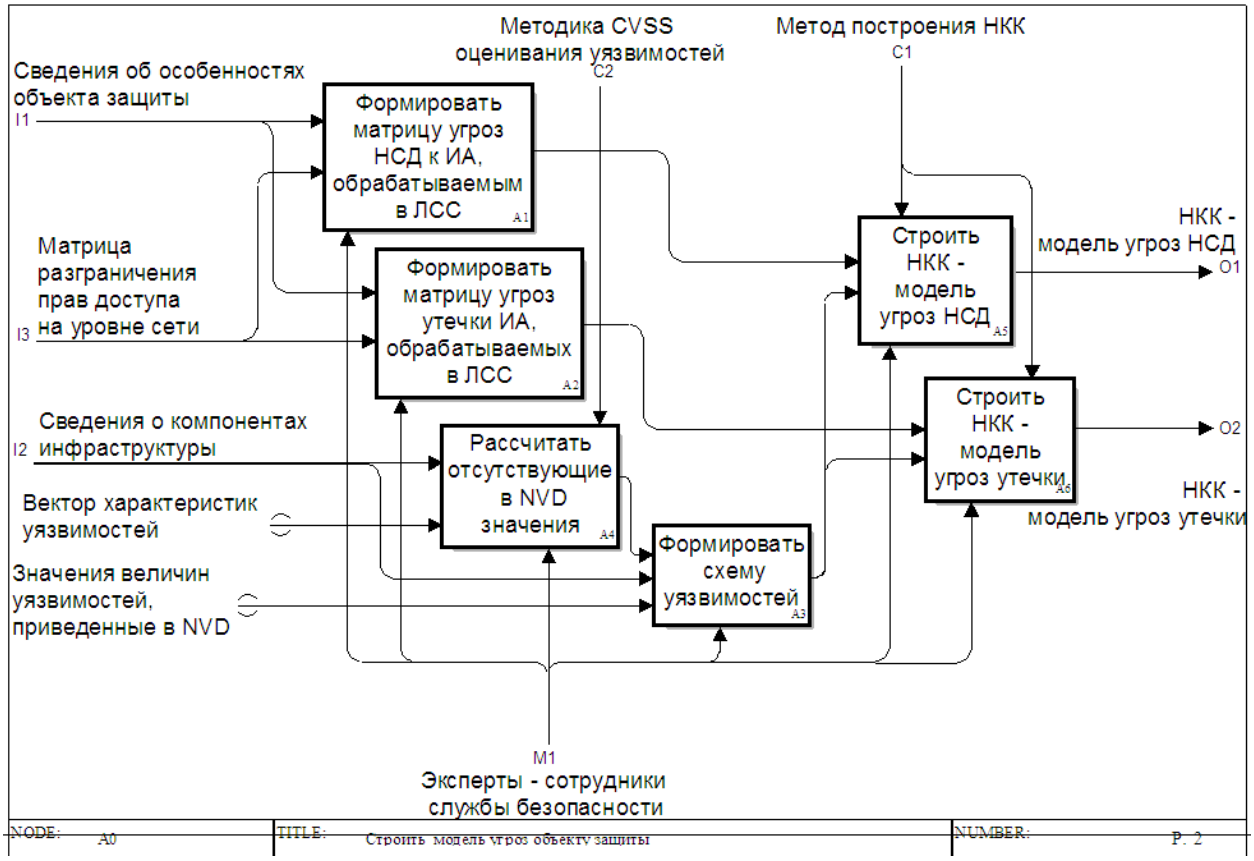

Рисунок 2 – IDEF0 диаграмма построения модели угроз в виде НКК

Оценивается максимальное значение уровня угрозы от одного источника к объекту атаки:

$$P^U(K_i \to K_y) = \max_{j=1...J} P_j . \quad (3)$$

Аналогично оцениваются уровни угроз от всех источников к установленным в модели объектам атак. *Результирующее значение уровня угроз* $P^U_{C_x}$ информационным активам, обрабатываемым в сегменте сети, предлагается вычислять по формуле:

$$P^U_{C_x} = 1 - \prod_{i=1}^{\delta} \left(1 - P^{U_i}\right), \quad (4)$$

где δ – число источников моделируемых угроз обрабатываемым в ЛСС C_x информационным активам, определенное в соответствии с матрицей угроз несанкционированного доступа и матрицей утечки; P^{U_i} – максимальное значение уровня угрозы, соответствующее ячейке матрицы угроз между потенциальным источником атаки и ИА сегмента сети.

Это позволяет оценить уровень риска нарушения информационной безопасности в случае, когда все нарушители и злоумышленники реализуют атаки на все множество защищаемых информационных активов, обрабатываемых в сегментах сети. Таким образом, оценивается *наихудший случай* в результате реализации угроз информационной безопасности.

Величины относительного риска для ЛСС, в которых обрабатываются информационные активы, имеющие наивысшие категории критичности «Н», «С», «В» соответственно, предложено определять по формулам:

$$\overline{R_{C^H}} = \sum_{n=1}^{N} P^U_{C_n^{\text{Н}}} \cdot \frac{Ц_{C_n^{\text{Н}}}}{Ц_{\Sigma}}, \quad \overline{R_{C^C}} = \sum_{m=1}^{M} P^U_{C_m^{\text{С}}} \cdot \frac{Ц_{C_m^{\text{С}}}}{Ц_{\Sigma}}, \quad \overline{R_{C^{\text{В}}}} = \sum_{l=1}^{L} P^U_{C_l^{\text{В}}} \cdot \frac{Ц_{C_l^{\text{В}}}}{Ц_{\Sigma}}, \quad (5)$$

где $n \in \{1,...,N\}$, $m \in \{1,...,M\}$, $l \in \{1,...,L\}$ – число сегментов, в которых обрабатывается информация категорий критичности «*Н*», «*С*», «*В*»; $\frac{Ц_{C_n^{\text{Н}}}}{Ц_{\Sigma}}, \frac{Ц_{C_m^{\text{С}}}}{Ц_{\Sigma}}, \frac{Ц_{C_l^{\text{В}}}}{Ц_{\Sigma}}$ – относительные ценности ИА в ЛСС с наивысшими уровнями критичности обрабатываемой информации «Н», «С», «В» соответственно.

Величину полного относительного риска нарушения ИБ информационной системе предлагается рассчитывать по формуле:

$$\overline{R} = \overline{R_{C^{\text{Н}}}} + \overline{R_{C^{\text{С}}}} + \overline{R_{C^{\text{В}}}} . \quad (6)$$

На основе предложенного метода оценки риска нарушения ИБ разработана IDEF0 модель оценивания. В соответствии с методом, контекстный функциональный блок представлен тремя подпроцессами: «Рассчитать параметр «Ценность информации»», «Рассчитать уровень угроз по ЛСС», «Рассчитать уровень риска нарушения ИБ в ЛСС и в ИС в целом».

Третья глава посвящена разработке метода определения ценности защищаемой информации, обрабатываемой в ЛСС.

Предлагается использовать метод нечеткого логического вывода для определения ценности информационных активов в соответствии с входными

лингвистическими переменными (ЛП): «Количество информационных активов уровня критичности $У$», обрабатываемых в заданном сегменте сети организации, и «Число (с учетом значимости) возможных видов последствий нарушения ИБ» для данной совокупности ИА.

На основе анализа критериев, приведенных в ГОСТ 27005-2010, предложено формировать наборы критериев K, которые с точки зрения описания последствий для бизнеса целесообразно использовать в процессе получения численного значения параметра «Ценность информационных активов уровня критичности $У$», обрабатываемых в заданном сегменте сети:

$$K^{У} = \bigcup_{1}^{E^{У}} k_e , \tag{7}$$

где $E^{У}$ – мощность множества критериев $K^{У}$, приемлемых для оценивания ценности информационных активов.

Предлагается каждому из критериев k_e присвоить ранг θ_e, отражающий степень тяжести последствий, с точки зрения представителей бизнеса. Степень значимости ψ множества $K^{У}$ критериев, приемлемых для определения ценности ИА заданного уровня критичности $У$, обрабатываемых в некотором сегменте сети C_x, предложено определять в соответствии с формулой:

$$\psi_{C_x} = \frac{1}{\Theta} \cdot \sum_{e=1}^{|K^{У}|} \theta_e , \tag{8}$$

где $\Theta = \sum_{1}^{E^{У}} \theta_e$ – значение суммы рангов для всего множества критериев K, приемлемых для оценивания ценности всего множества ИА.

В рассмотрение вводятся нечеткие лингвистические переменные A, B, D с функциями принадлежности (ФП) $\mu_A(V^{У})$, $\mu_B(\psi_{C_x} \cdot E^{У})$, $\mu_D(Ц^{У}_{C_x})$:

$$\begin{aligned} A &= \{(V^{У}, \mu_A(V^{У})) \mid \mu_A(V^{У}) \in [0,1],\ V^{У} \in \mathrm{N}\}, \\ B &= \{(\psi_{C_x} \cdot E^{У}, \mu_B(\psi_{C_x} \cdot E^{У})) \mid \mu_B(\psi_{C_x} \cdot E^{У}) \in [0,1],\ \psi_{C_x} \cdot E^{У} \in Q\}, \\ D &= \{(Ц^{У}_{C_x}, \mu_D(Ц^{У}_{C_x})) \mid \mu_D(Ц^{У}_{C_x}) \in [0,1],\ Ц^{У}_{C_x} \in [0,1]\}. \end{aligned} \tag{9}$$

ФП входных и выходной ЛП строятся экспертом на основе сведений об особенностях обработки информации на *конкретном* объекте защиты. Предлагается равномерное распределение термов по области определения входных и выходных лингвистических переменных. Для задания области определения ЛП «Количество информационных активов уровня критичности $У$» устанавливается сегмент сети, в котором количество информационных активов заданного уровня критичности максимально. В качестве области определения второй входной переменной предложено принимать диапазон $[0, \psi_{C_x} \cdot E^{У}]$, где $E^{У}$ – максимальное число критериев $K^{У}$, приемлемых для определения ценности ИА заданного уровня критичности $У$.

Для выходной ЛП «Ценность информационных активов уровня критичности $У$», обрабатываемых в ЛСС (рис. 3), предложено терм-множество, определенное в соответствии терминами, приведенными в ГОСТ 27005-2010,

для качественного оценивания ценности: «пренебрежительно малая», «очень низкая», «низкая», «средняя», «высокая», «чрезвычайно высокая». Очевидно, что при определении ценности ИА разных уровней критичности должны использоваться различные наборы нечетких множеств, что должно отражаться в продукционных правилах. Область определения выходной ЛП $Ц^{У}_{C_x} = [0,1]$.

Рисунок 3 – ФП выходной ЛП «Ценность ИА уровня критичности *У*»

С использованием методологии функционального моделирования метод определения ценности информации представлен в наглядной форме. На рис. 4 приведен результат декомпозиции функционального блока «Рассчитать параметр «Ценность информации».

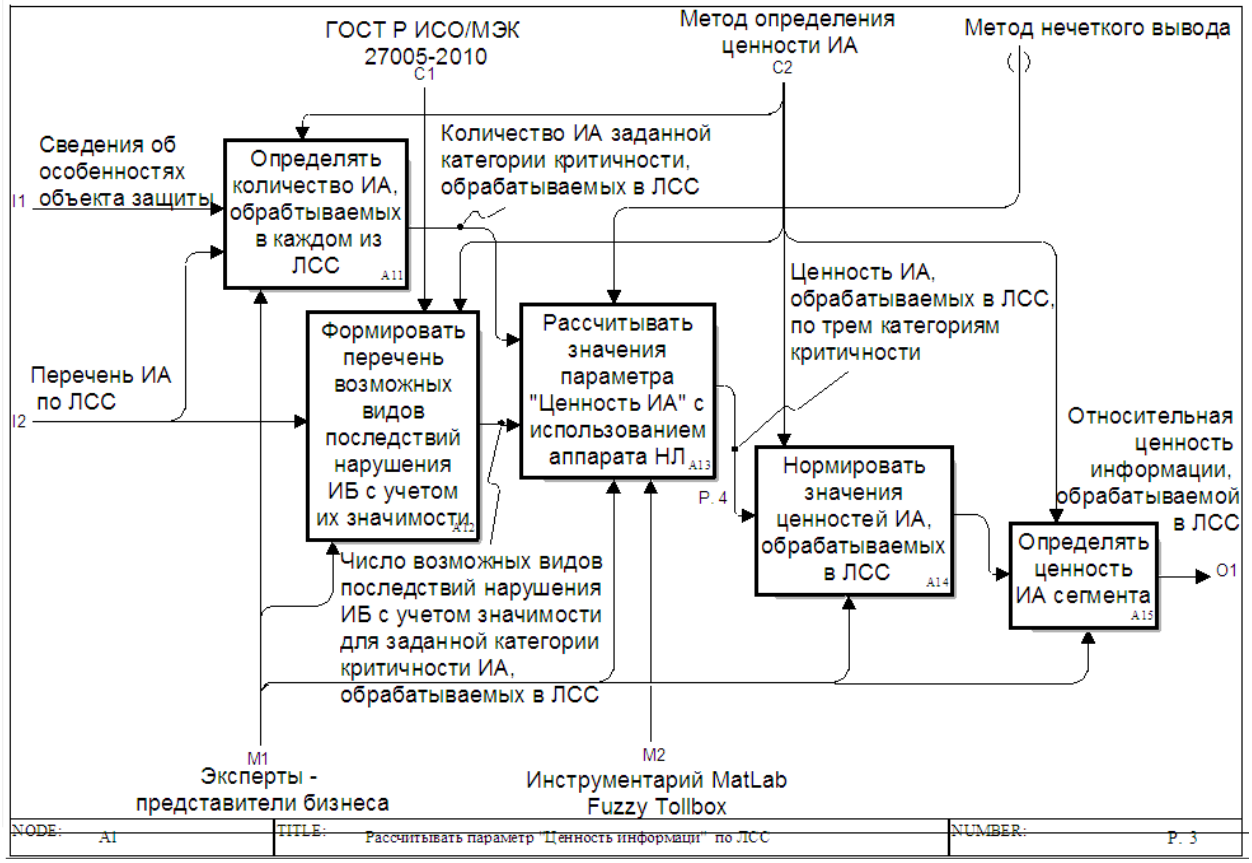

Рисунок 4 – Дочерняя диаграмма диаграммы «Рассчитать параметр «Ценность информации»

Отмечается необходимость нормирования полученных значений $Ц^{У}_{C_x}$. Для этого вычисляется сумма полученных в блоке дефаззификации значений ценностей информационных активов $Ц^{Н}_{C_x}$, $Ц^{С}_{C_x}$, $Ц^{В}_{C_x}$ уровней критичности «Н», «С», «В» соответственно:

$$Ц_{\Sigma} = \sum_{1}^{N} Ц^{Н}_{C_n} + \sum_{1}^{M} (Ц^{Н}_{C_m} + Ц^{С}_{C_m}) + \sum_{1}^{L} (Ц^{Н}_{C_l} + Ц^{С}_{C_l} + Ц^{В}_{C_l}) . \quad (10)$$

При оценке уровня риска, в соответствии с (6), значение ценности информационных активов ЛСС определяется как сумма значений ценностей ИА всех категорий критичности, обрабатываемых в заданном сегменте сети.

Четвертая глава посвящена рассмотрению практических аспектов использования предложенного метода оценки риска нарушения ИБ.

Приводятся блок-схема алгоритма и описание работы с разработанным программным комплексом, реализующим предложенный метод оценки риска.

Позволяя учитывать данные о конкретном объекте защиты (количество локальных сетевых сегментов, ценность критичной информации в ЛСС, наличие доступа в Интернет и информационного взаимодействия с компаниями-партнерами или филиалами, уровни уязвимостей используемых или планируемых компонентов инфраструктуры), программный комплекс предоставляет пользователю возможность моделировать потенциальные угрозы объекту защиты через используемые уязвимости, оценивать риск нарушения ИБ в локальных сетевых сегментах и в ИС в целом, сравнивать различные наборы средств защиты посредством этих оценок.

С использованием программного комплекса произведена оценка уровня риска в сети государственного учреждения до и после модернизации системы защиты информации (табл. 1), расчет значения риска также производился вручную. Результаты показали работоспособность программного комплекса, устойчивость к некорректным входным данным и воспроизводимость полученных результатов.

Таблица 1. Изменение уровня риска в результате добавления контрмер

Номер ЛСС	Ценность ИА категории критичности			Относительная ценность ИА	Уровни угроз ИА, обрабатываемым в ЛСС		Уровень риска нарушения ИБ	
	«Н»	«С»	«В»		до	после	до	после
					модернизации		модернизации	
1	0,059	0,654	0,943	0,271	0,370	0,150	0,100	0,041
2	0,346	0,654	0,943	0,318	0,170	0,064	0,054	0,020
3	0,059	0,538	0	0,098	0,381	0,155	0,037	0,015
4	0,059	0,486	0	0,089	0,370	0,150	0,033	0,013
5	0,346	0,486	0	0,136	0,370	0,150	0,050	0,020
6	0,059	0,486	0	0,089	0,370	0,150	0,033	0,013
	Итого: 6,118			1	Итого:		**0,307**	**0,123**

Благодаря возможности построения модели угроз, адекватной конкретному объекту защиты, произведена оценка влияния топологии сети на уровень риска. В исследуемой ИС исходной топологией установлен лишь периметровый межсетевой экран, использование уязвимости которого позволяет получить доступ к внутренней подсети, а сервера компании, на которых обрабатывается информация, обладающая большой относительной ценностью, расположены в том же сегменте сети, что и почтовый сервер. За счет устранения лишь уязвимостей инфраструктуры с учетом архитектуры безопасности расчетное значение уровня риска для ИС, удается сократить в 3,46 раза меньше, уровень риска составил 8,9%.

Для оценки влияния количества потенциально возможных источников атаки введена характеристика $P_{акт}$ – вероятность активизации угрозы, которая показывает величину отношения той части пользователей-нарушителей и злоумышленников, которая решила совершить атаку на информационную систему, к их общему возможному числу.

Был произведен вычислительный эксперимент, в ходе которого изменялись значения $P_{акт}$ внешнего пользователя-нарушителя и злоумышленника в диапазоне $[0,1]$, при фиксированном значении $P_{акт} = 0$ для внутренних нарушителей, и наоборот, результаты которого представлены на рис. 5.

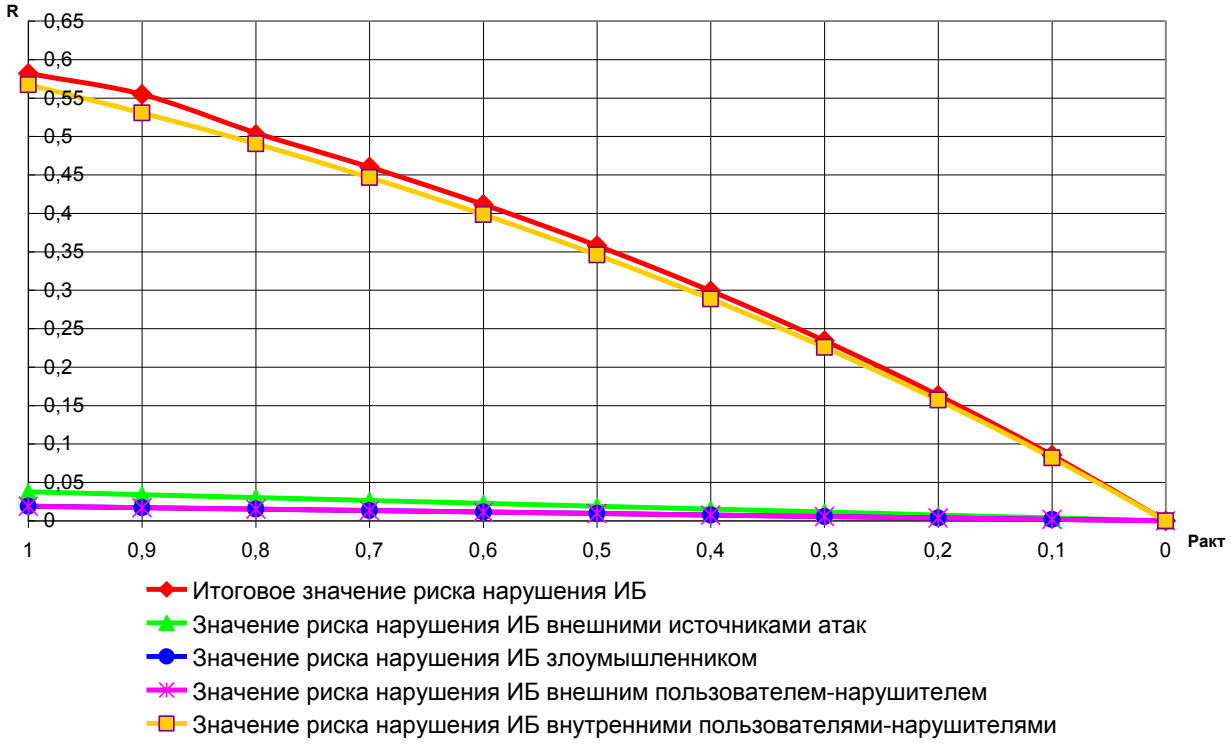

Рисунок 5 – График зависимости влияния $P_{акт}$ на значение риска

Таким образом, оценено и расчетным путем доказано, что угрозы нарушения ИБ, связанные с деятельностью легальных пользователей ИС – внутренних источников угроз, являются наиболее опасными.

На основе проведенных исследований можно сделать выводы об эффективности и целесообразности предложенных моделей и методов оценки риска нарушения информационной безопасности.

Основные результаты и выводы

1. Разработана концептуальная *модель* преднамеренных целенаправленных *угроз* нарушения информационной безопасности, *основанная* на построении нечетких когнитивных карт, *отличающаяся* визуализацией путей распространения угроз в инфраструктуре информационной системы на основе разработанных матриц угроз, устанавливающих взаимосвязь между каждым источником и объектом атаки, что *позволяет* учесть используемые для осуществления угроз уязвимости коммуникационного оборудования, средств защиты и программного обеспечения при оценивании уровней угроз.

2. Разработан метод оценки риска нарушения информационной безопасности, *основанный* на разработанной концептуальной модели угроз и суммировании рисков локальных сетевых сегментов, *отличающийся* тем, что выявляется зависимость значения риска каждого сегмента от ценности обрабатываемой информации и оценок значимости угроз от множества источников к одному объекту, а именно: значения уровней угроз на путях распространения определяются как произведения вероятности активизации угрозы и полученных нормированием приведенных в международной базе данных величин уязвимостей компонентов инфраструктуры и барьеров, выявляются максимальные значения уровней угроз от каждого возможного источника для вычисления результирующего значения уровня угрозы информационным активам сегмента, – что *позволяет* представить процесс оценивания наглядно в виде функциональной модели, оценить влияние архитектуры сети на значение риска нарушения информационной безопасности, сравнить эффективность различных наборов средств защиты в количественном выражении на стадии эксплуатации и при проектировании системы защиты информации.

3. Предложен метод оценивания ценности защищаемых информационных активов локальных сетевых сегментов, *отличающийся* тем, что в качестве исходных данных при оценивании параметра, с использованием аппарата нечеткого логического вывода, принимается количество обрабатываемых в сегментах информационных активов определенных уровней критичности и число, с учетом значимости, возможных видов последствий из перечня, приведенного в стандарте по информационной безопасности, что *позволяет* повысить достоверность оценивания для конкретного объекта защиты, минимизировать субъективность полученных оценок, учесть изменение ценности информации во времени и использовать этот параметр для оценки информационного риска.

4. Разработан программный комплекс, реализующий *метод оценки* уровня риска нарушения информационной безопасности, с помощью которого подтверждена возможность получения воспроизводимых и сравнимых

результатов. Оценка риска нарушения информационной безопасности с использованием программной системы позволила определить, что уровень риска после модернизации СЗИ сократился в 2,5 по сравнению с уровнем риска до модернизации и составил 12,3%. Количественно оценено влияние архитектуры сети, потенциально возможного количества нарушителей и злоумышленников на значение риска нарушения ИБ, а также влияние своевременного устранения уязвимостей программного обеспечения путем установки обновлений.

Перспективы дальнейшей разработки темы. В рамках дальнейших исследований планируется разработка метода оперативного оценивания уровней рисков с использованием интеллектуальных технологий.

СПИСОК ОСНОВНЫХ ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в рецензируемых журналах ВАК:

1. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности / Е. С. Степанова, И. В. Машкина, В. И. Васильев // Известия ЮФУ. Технические науки. Тематический выпуск «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2010. №11(112). С. 31–40.
2. Построение модели угроз с помощью нечетких когнитивных карт на основе сетевой политики безопасности / М. Б. Гузаиров, И. В. Машкина, Е. С. Степанова // Безопасность информационных технологий. №2, 2011. С. 37 – 49.
3. Программный модуль реализации алгоритма численной оценки риска нарушения информационной безопасности / Е. С. Степанова, И. В. Кансафаров // Безопасность информационных технологий. №1, 2011. С. 128 – 130.
4. Метод определения ценности информации с использованием аппарата нечеткой логики / М. Б. Гузаиров, И. В. Машкина, Е. С. Степанова // Безопасность информационных технологий. №1, 2012. С. 18 – 29.
5. Методика оценки стоимости информации на объекте защиты с использованием аппарата нечеткой логики / Е. С. Степанова // Безопасность информационных технологий. №1, 2012. С. 119 – 121.

Свидетельства об официальной регистрации программ для ЭВМ:

6. Свидетельство о государственной регистрации программы для ЭВМ № 2012612377. Расчет численного значения риска нарушения информационной безопасности на основе построения нечетких когнитивных карт в проекцию на топологию сети (RiskAnalyzer) / И. В. Машкина, И. В. Кансафоров, Е. С. Степанова, Р. М. Хабибуллин. М.: Роспатент, 2012.

Другие публикации

7. Разработка модели угроз на основе построения нечеткой когнитивной карты в проекции на топологию сети / Е. С. Степанова, И. В. Машкина, В. И. Васильев // Информационная безопасность: Материалы XI Международной научно-практической конференции Ч. 2. – Таганрог: Изд-во ТТИ ЮФУ, 2010. – С. 232 – 239.

8. Анализ рисков объектов информатизации: учебное пособие / И. В. Машкина, Е. С. Степанова, Т. О. Вишнякова – Уфа: УГАТУ, 2011. – 112с.
9. Анализ баз данных известных уязвимостей / Е. С. Степанова, Л. Р. Тулиганова // Актуальные проблемы науки и техники. Том 1. Информационные и инфокоммуникационные технологии, естественные науки: Сборник трудов VI Всероссийской зимней школы-семинара аспирантов и молодых ученых / Уфимск. гос. авиац. тех. ун-т. – Уфа: УГАТУ, 2011. С. 118 – 122.
10. Метод оценки информационного риска на основе построения модели угроз с использованием нечетких когнитивных карт / Е. С. Степанова, И. В. Машкина, М. Б. Гузаиров // Материалы XIII Международной конференции по компьютерным наукам и информационными технологиям *CSIT*`2011. Том 1 / Уфимск. гос. авиац. тех. ун-т. – Уфа: УГАТУ, 2011. С. 98 – 103. (Статья на англ. яз).
11. Метод численной оценки риска нарушения информационной безопасности на основе построения модели угроз с помощью нечетких когнитивных карт / Е. С. Степанова, И.В. Машкина // Молодежный Вестник УГАТУ № 1 (1) / 2011 С. 22 – 29.
12. Использование нечетких когнитивных карт для анализа процесса информационного противоборства / В. И. Васильев, И. В. Машкина, Е. С. Степанова // Когнитивный анализ и управление развитием ситуаций (*CASC*`2011): Труды IX Международной конференции. – М.: ИПУ РАН, 2011. С. 190 – 193.
13. Анализ методик оценивания ценности информации при анализе рисков нарушения информационной безопасности / Е. С. Степанова // Актуальные проблемы науки и техники. Том 1. Информационные и инфокоммуникационные технологии: Сборник трудов VII Всероссийской зимней школы-семинара аспирантов и молодых ученых/ Уфимск. гос. авиац. тех. ун-т. – Уфа: УГАТУ, 2012. С. 392 – 395.
14. Программная система оценки рисков нарушения информационной безопасности на основе построения нечетких когнитивных карт / Е. С. Степанова, Р. М. Хабибуллин, И. В. Машкина // Информационная безопасность: Материалы XII Международной научно-практической конференции Ч. 1. – Таганрог: Изд-во ТТИ ЮФУ, 2012. – С. 185 – 192.

Диссертант  Е. С. Степанова

СТЕПАНОВА Екатерина Сергеевна

МОДЕЛИ И МЕТОДЫ ОЦЕНКИ РИСКОВ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ НЕЧЕТКИХ КОГНИТИВНЫХ КАРТ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Подписано в печать 25.04.2013. Формат 60×84 1/16.
Бумага обёрточная. Печать плоская. Гарнитура Таймс.
Усл.печ.л. 1,0. Уч.-изд.л. 0,9.
Тираж 100 экз. Заказ № 262
ФГБОУ ВПО «Уфимский государственный авиационный технический университет»
Центр оперативной полиграфии
450000, Уфа-Центр, К.Маркса, 12