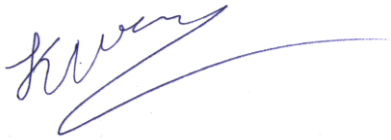
На правах рукописи



Шинаков Кирилл Евгеньевич

МИНИМИЗАЦИЯ РИСКОВ НАРУШЕНИЯ БЕЗОПАСНОСТИ ПРИ ПОСТРОЕНИИ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Специальность: 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Брянск 2017

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Брянский государственный технический университет»

Научный руководитель: Рытов Михаил Юрьевич,
кандидат технических наук, доцент

Официальные оппоненты: Примакин Алексей Иванович, доктор технических наук, профессор, начальник кафедры "Специальных информационных технологий", ФГКОУ ВО «Санкт-Петербургский университет Министерства внутренних дел Российской Федерации»,

Горбачев Игорь Евгеньевич, кандидат технических наук, доцент кафедры Систем сбора и обработки информации ФГБВОУ ВО «Военно-космическая академия имени А.Ф. Можайского» Министерства обороны Российской Федерации (г. Санкт-Петербург).

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича» (СПбГУТ)

Защита диссертации состоится «28» февраля 2018 г. в 14:00 часов на заседании диссертационного совета Д 212.229.31 на базе ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» (ФГАУО ВО СПбПУ) по адресу: 195251, Санкт-Петербург, Политехническая 29, главное здание, ауд 175.

С диссертацией и авторефератом можно ознакомиться в библиотеке и на сайте ФГАОУ ВО «Санкт-Петербургский политехнический университет Петра Великого» (www.spbstu.ru). Автореферат размещен на сайте Минобрнауки России (www.vak.gov.ru)

Автореферат разослан « 18 » января 2018 г.

Ученый секретарь
диссертационного совета
кандидат технических наук  Супрун Александр Федорович

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. С появлением современных средств вычислительной техники и телекоммуникаций не только появились угрозы и уязвимости, специфические для компьютерных систем и сетей, но и произошла трансформация традиционных имущественных и неимущественных преступлений в новые формы. С одной стороны, это обусловлено появлением электронных информационных ресурсов и возникновением систем электронного документооборота, а с другой – ростом числа преступлений, связанных с неправомерным использованием персональных данных (ПДн).

С точки зрения информационных ресурсов к ПДн относятся: данные в системах кадрового и бухгалтерского учета; базы данных клиентов; базы данных контактов юридических лиц-контрагентов (CRM и пр.); контактные данные почтовой системы и почтовых клиентов сотрудников. Преступления в сфере компьютерной обработки информации и персональных данных (ПДн) характеризуются скрытностью, трудностью сбора улик, сложностью доказывания.

Интерес к вопросам сохранности персональных данных, защиты их от случайного и преднамеренного уничтожения, повреждения и несанкционированного получения связан с широким применением информационных систем в различных областях и возможностью дистанционного получения ПДн через терминалы. Стандартность архитектурных принципов построения, оборудования и программного обеспечения информационных систем ПДн, высокая мобильность программного обеспечения и ряд других признаков определяют сравнительно легкий доступ профессионала к ним.

Необходимо отметить, что защита ПДн вызывает дополнительные сложности, обусловленные: трудоемкостью обеспечения безопасности персональных данных (Приказ ФСТЭК России № 21 от 18.02.2013); высокой стоимостью реализации мер защиты (необходимость использования сертифицированных СЗИ – Постановление Правительства РФ № 1119 от 12ноября 2012 г.); увеличением количества контролирующих органов, расширением тематики возможных (плановых и внеплановых) проверок; административной и уголовной ответственностью за утечку ПДн.

Указанные обстоятельства свидетельствуют о наличии противоречия между необходимостью обеспечения целостности, доступности и конфиденциальности персональных данных и недостаточными возможностями защиты этих данных от случайных или преднамеренных негативных воздействий в современных информационных системах. Настоятельная необходимость разрешения указанного противоречия обусловила объект и цель исследований диссертационной работы.

В качестве **объекта исследования** в работе приняты информационные системы персональных данных.

Целью работы является снижение риска нарушения безопасности персональных данных в информационных системах.

Опыт применения информационных систем и исследования показывают, что в современных условиях одним из наиболее перспективных путей достижения этой цели является защита информационных систем персональных данных (ИСПДн) путем применения соответствующего набора контрмер. Формирование рационального набора таких контрмер для минимизации возможного ущерба, минимизации вероятности реализации групп критичных угроз, минимизации риска нарушения безопасности ИСПДн в каждом конкретном случае обеспечивается применением научно-методического аппарата (НМА) обоснования соответствующих решений.

С учетом сформулированной цели исследования и выбранных путей ее достижения в качестве **предмета диссертационного исследования** принят НМА обоснования решений по выбору рационального набора контрмер, включающий модели и методики минимизации возможного ущерба, минимизации вероятности реализации групп критичных угроз, минимизации риска нарушения безопасности ИСПДн.

Степень разработанности темы исследования. Вопросы обеспечения информационной безопасности и защиты информации в различных аспектах исследовались многими учеными. В частности, теоретические проблемы информационного права, правового обеспечения информационной безопасности исследованы в работах И.Л. Бачило, В.А. Копылова, В.Н. Лопатина, В.А. Пожилых, М.М. Рассолова, А.А. Фатьянова, М.А. Федотова, О.А. Федотовой, С.Г. Чубуковой, А.А. Шиверского, В.Д. Элькина и др. Проблемы функционирования систем обеспечения информационной безопасности с точки зрения разработки технических средств и методов защиты исследованы в работах таких ученых как Котенко И.В., Молдовян А.А., Саенко И.Б. А.Л. Балыбердин, М.А. Вус, В.А. Герасименко, А.А. Грушо, С.В. Дворянкин, П.Д. Зегжда, Е.В. Касперский, А.Г. Остапенко, С.А. Петренко, В.Д Курушин, А.А. Малюк, В.А. Минаев, В.Е. Потанин, В.Н. Саблин, С.В. Скрыль, А.П. Фисун и др. Эти ученые внесли значительный вклад в развитие теории и практики безопасности ИС, вместе с тем полученные результаты лишь частично касались проблемы защиты персональных данных, а те публикации, которые включали рассмотрение вопросов регулирования изучаемой сферы, затрагивали только лишь общие проблемы без необходимой конкретизации.

Таким образом в теории обеспечения информационной безопасности и защиты информации имеет место противоречие между потребностью обоснования решений по выбору рационального набора контрмер для защиты ИСПД и отсутствием соответствующего НМА.

Необходимость разрешения этого противоречия определила **научную задачу** диссертационной работы и обусловила ее актуальность.

Суть общей научной задачи заключается в разработке НМА обоснования решений по выбору рационального набора контрмер для

защиты ИСПДн в интересах снижения риска нарушения ее безопасности в условиях случайных или преднамеренных негативных воздействий.

Для решения общей научной задачи исследования в работе поставлены и решены следующие частные задачи:

1. Разработана объектно-ориентированная математическая модель оценки риска нарушения безопасности ИСПДн, основанная на аппарате раскрашенных сетей Петри и разработанных правилах срабатывания переходов.

2. Разработан алгоритм решения задач оценки вероятности реализации угроз и критериев важности обрабатываемых данных в ИСПДн, формирования и сравнения групп актуальных угроз.

3. Разработана методика минимизации риска нарушения безопасности ИСПДн на основе формирования набора контрмер с целью устранения групп критичных угроз.

4.Разработана автоматизированная система оценки рисков безопасности ИСПДн, реализующая возможности производить оценку ущерба от нарушения свойств безопасности ИСПДн, рассчитывать вероятность реализации групп критичных угроз, а также вероятность устранения групп критичных угроз, что позволяет сформировать эффективный набор контрмер для снижения риска ИСПДн.

Методы исследования. Для решения поставленных задач использовались системный анализ, теория вероятностей, теория принятия решений, теория графов, теория математического моделирования, теория многокритериального выбора, методы экспертных оценок, метод аддитивной свертки.

Научная новизна проведенных исследований заключается в том, что разработанный автором НМА позволяет моделировать процессы нарушения безопасности ИСПД и алгоритмизировать выработку предложений по их защите с учетом особенностей функционирования этих систем и тенденций изменения угроз безопасности.

Новизна исследований подтверждается государственной регистрацией программ для ЭВМ

Обоснованность научных результатов диссертации обеспечивается:

- последовательным применением принципов системного подхода при проведении исследования;
- корректностью применения аппарата раскрашенных сетей Петри, математического программирования и теории вероятностей;
- достаточной полнотой учета факторов, влияющих на качество принимаемых решений и мероприятий по обеспечению эффективности защиты информации ИСПДн;
- правильным определением ограничений и допущений при формировании исходных данных для решения общей и частных задач исследования.

Достоверность результатов исследования подтверждается:

- согласованностью результатов теоретических исследований

с результатами практической апробации теоретических результатов в архитектуре и технических решениях при разработке и внедрении автоматизированной системы оценки рисков нарушения безопасности ИСПДн на предприятиях промышленности;

- положительными экспертными оценками результатов диссертационного исследования в ходе их обсуждения на конференциях, семинарах и в рецензиях на публикации основных научных и практических результатов в центральных и ведомственных изданиях.

Теоретическая значимость результатов исследований следует из ее научной новизны и актуальности. Результаты исследования развивают теорию безопасности информационных систем, расширяют арсенал ее методов и моделей. Полученные научные результаты и выводы могут служить теоретической основой для проведения дальнейших исследований по повышению эффективности защиты информации в информационных системах различного назначения.

Практическая ценность работы определяется тем, что реализация разработанных научных положений и рекомендаций позволяет существенно повысить безопасность ИСПДн при одновременном снижении экономических затрат.

Полученные результаты позволили на практике:

- обосновать архитектуру и ряд технических решений разработанной автоматизированной системы оценки рисков нарушения безопасности ИСПД, реализующей возможности производить оценку ущерба от нарушения свойств безопасности ИСПДн,
- рассчитывать вероятности реализации групп критичных угроз для обеспечения безопасности ИСПДн;
- рассчитывать вероятности устранения групп критичных угроз для обеспечения безопасности ИСПДн;
- сформировать эффективный набор контрмер для снижения риска нарушения безопасности ИСПДн;
- внедрить систему оценки рисков безопасности на предприятиях и в органах государственного управления Брянской области.

На защиту выносятся:

1. Объектно-ориентированная математическая модель оценки риска нарушения безопасности ИСПД, основанная на аппарате раскрашенных сетей Петри и разработанных правилах срабатывания переходов.

2. Алгоритм оценки ущерба от нарушения свойств безопасности ИСПД, основанный на экспертно-статистической оценке и алгоритм определения критичной группы угроз путем детализации уязвимостей, основанный на методе аддитивной свертки.

3. Алгоритм оценки эффективности защиты информационных систем персональных данных, опирающийся на сформулированную автором теорему определения условия эффективности.

4. Методика минимизации риска нарушения безопасности персональных данных, основанная на многокритериальной оценке контрмер.

Внедрение результатов работы. Автоматизированная система оценки рисков безопасности ИСПДн опробована и внедрена на предприятиях АО УК «БМЗ»» (акт внедрения АО УК«БМЗ» №28 от 26.01.2017), ФГБОУ ВО «БГТУ» (акт внедрения ФГБОУ ВО «БГТУ» №15 от 05.12.2016), ООО «Рикамби» (акт внедрения ООО «Рикамби» №7 от 8.02.2017).
Результаты работы внедрены в учебный процесс Брянского государственного технического университета на кафедре «Системы информационной безопасности» в дисциплины «Аудит информационной безопасности» и «Защита персональных данных», а также используются в деятельности Контрольно-счетной палаты Брянской области, Управлении Министерства юстиции по Брянской области, Департамента образования и науки Брянской области.

Апробация работы. Основные положения диссертационной работы докладывались и обсуждались на научных конференциях различного уровня, основными из которых являются: региональная научно-практическая конференция «Информационная безопасность и защита персональных данных: проблемы и пути решения» (Брянск, 2013 – 2016), Международная научно-практическая конференция «Достижения молодых ученых в развитии инновационных процессов в экономике, науке, образовании» (Брянск, 2015), Межрегиональная научно-практическая конференция «Инновации и информационные риски» (Воронеж, 2013 – 2015).

Публикации по теме диссертации. По материалам диссертационной работы опубликовано 10 научных статей, из них 5 в изданиях, входящих в перечень ВАК Минобрнауки России**,** 2 свидетельства о государственной регистрации программы для ЭВМ, 2 монографии.

Структура и объем работы. Диссертационная работа состоит из введения, пяти глав, заключения, списка литературы, приложений. Работа изложена на 256 страницах машинописного текста, включающего 43 рисунка, 36 таблиц, список литературы из 99 наименований, 25 приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность выбранной темы диссертации, формулируется цель работы и задачи исследования, указываются применяемые методы исследований и научная новизна, а также дана краткая характеристика диссертации. Приводятся научная и практическая значимость, а также положения, выносимые на защиту.

В первой главе проведен анализ современного состояния задачи оценки и минимизации риска информационной безопасности, в результате которого установлено, что организации зачастую плохо представляют себе существующие риски, которым подвержены персональные данные обрабатываемые в ИСПДн организации, вследствие чего резко увеличиваются затраты на обеспечение информационной безопасности.

Рассмотрена зарубежная и российская нормативно-правовая база в области оценки риска информационной безопасности. Выявлено, что

законодательная база не предлагает однозначных подходов к оценке возможного ущерба от разглашения, удаления, изменения тех или иных категорий ПДн, оценке вероятности реализации угроз, оценке риска безопасности ИСПДн.

В результате сравнительного анализа методов оценки рисков нарушения информационной безопасности выявлено, что для решения поставленной задачи наиболее подходящими являются стратегии анализа риска организации, представленные в ГОСТ Р ИСО/МЭК ТО 13335-3—2007 и ГОСТ Р ИСО/МЭК 27005-2010. Использование комбинированного подхода, представленного в ГОСТ, обеспечивает сочетание анализа высокого уровня риска с базовым подходом и (если необходимо) детальным анализом риска, что обеспечивает большинству организаций наиболее эффективное решение проблем, связанных с разработкой систем защиты ПДн.

Во второй главе сформулирована задача выбора наиболее эффективного состава системы защиты ИСПДн. Для рассмотрения берутся информационные ресурсы объекта с учетом их стоимости, угрозы информационной безопасности, уязвимые звенья, возможные контрмеры для снижения уровня рисков, представленные в рекомендациях ФСТЭК и ФСБ России в области защиты информации. Идентифицированы контрмеры по минимизации выявленных рисков и варианты их выбора с расчетом стоимости их реализации, что позволило обосновывать структуру разрабатываемой модели оценки риска нарушения безопасности ИСПДн.

Проведен анализ существующих подходов к моделированию процесса оценки рисков ИСПДн, в результате которого установлено, что наиболее подходящим для моделирования процессов реализации и устранения угроз является математический аппарат раскрашенных сетей Петри.

В третьей главе для расчета оценки риска разработан **алгоритм оценки ущерба от нарушения свойств безопасности ИСПДн**, основанный на экспертно-статистической оценке, отличающийся применением метода прогнозного графа и позволяющий рассчитать количественные и качественные оценки потенциального ущерба персональным данным.

В работе проведен анализ возможного ущерба от реализации угроз целостности, доступности и конфиденциальности с точки зрения возможной суммы штрафов за нарушение требований соответствующих нормативно-правовых актов и стоимости восстановления информации в случае наступления деструктивных последствий (табл.1). Таким образом, процесс оценки ущерба от реализации угроз в формализованном виде можно представить как:

$$S = S_{vst} + Y + S_2, \quad (1)$$

где S_{vst}– стоимость восстановления для группы угроз, определяется по формуле

$$S_{vst} = \sum S_1,$$

где S_1 - стоимость восстановления от угрозы; S_2–стоимость возмещения ущерба субъектам ПДн$S_2 = Y_4 * n$, где n– количество исков от субъектов ПДн;

Y–значение максимального штрафа согласно законодательству РФ.

$$\boldsymbol{Y = \{Y_1, Y_2, Y_3, Y_4\}},$$

где $\boldsymbol{Y_1} = \{Y_{11}, Y_{12}, Y_{13}, Y_{14}, Y_{15}\}$ (Статья 13.11, КоАП РФ),

Y_{11}= 50000 (Статья 13.11 п.1, КоАП РФ, максимальный штраф 50000 рублей),Y_{12} = 75000 (Статья 13.11 п.2, КоАП РФ, максимальный штраф 75000 рублей),Y_{13}= 45000 (Статья 13.11 п.5, КоАП РФ, максимальный штраф 45000 рублей),Y_{14} = 50000 (Статья 13.11 п.6, КоАП РФ, максимальный штраф 50000 рублей),Y_{15} = 6000 (Статья 13.11 п.7, КоАП РФ, максимальный штраф 6000 рублей);$\boldsymbol{Y_2}$= $\{Y_{21}, Y_{22}, Y_{23}\}$ (Статья 13.12, КоАП РФ),где Y_{21} = 25000 (Статья 13.12 п.2, КоАП РФ, максимальный штраф 25000 рублей),Y_{22}= 25000 (Статья 13.12 п.5, КоАП РФ, максимальный штраф 25000 рублей),Y_{21} = 15000 (Статья 13.12 п.6, КоАП РФ, максимальный штраф 15000 рублей);$\boldsymbol{Y_3}$= 5000 (Статья 13.14, КоАП РФ, штраф 5000 рублей);$\boldsymbol{Y_4}$= 300000 (Статья 137, УК РФ, штраф 300000 рублей).

Таблица 1 - Сравнение ущерба для видов ПДн

	ПДн			
	S_{vst}*(руб.)*	*Y(руб.)*	S_2*(руб.) (рассмотрен объект, на котором работают 10 сотрудников)*	*S (руб.)*
Конфиденциальность	269252	421000	3 000000	3 690 252
Целостность (Изменение)	115166	421000	3 000000	3 536 166
Целостность (Удаление)	782478	421000	3 000000	4 203 478
Доступность	705034	421000	3 000000	4 126 034

Для определения значений критичного ущерба для предприятий произведено категорирование объектов защиты, в результате которого получены значения критичного ущерба для видов ПДн и организаций.

Оценка вероятности реализации выявленных и оцененных угроз проводится экспертным методом (2).

$$V_{ry} = \sum_{i=1}^{n} k_i * a_i, \quad (2)$$

где:k_i – ответ на i вопрос опросника, a_i– коэффициент важности определяющийся экспертным методом и удовлетворяющий условию (3).

$$\sum_{i=1}^{n} a_i = 1. \quad (3)$$

На втором этапе целесообразно выявить актуальные угрозы и определить вероятность реализации угрозы. Для данной процедуры разработаны специализированные опросники, представленные в Приложениях к тексту диссертационной работы. Вопросы в данной опросной системе сформулированы и скомпонованы таким образом, чтобы обеспечить возможность фильтрации неактуальных, для рассматриваемого объекта угроз, и определить значения коэффициентов, используемых для последующих расчетов.

Для наглядности метода было взято предприятие ООО «Рикамби» с некими актуальными для него угрозами и соответствующими уязвимостями.

Вычисление вероятности реализации угрозы рассмотрим на примере угрозы «Утечка акустической информации» (табл.2). *Полный текст таблицы представлен в Приложении 2 Таблицы 2 текста диссертационной работы.*

Таблица 2 - Определение возможности реализации угроз на примере угрозы «Утечка акустической информации»

№	Угроза	Определение возможности			возможность реализации угрозы Vry
		Уязвимость	Ответ k_i	Коэффициент важности α_i	
1	Угрозы утечки акустической информации	Отсутствуют шумогенераторы	0	0,5	0,3
		Индекс звукоизоляции дверей менее 40 дБ	1	0,3	
		Переговорные не проходили аттестацию (проходили более 5 лет назад)	0	0,2	

V_{ry} для данной угрозы вычисляется следующим образом:

$$V_{ry} = (0*0,5) + (1*0,3) + (0*0,2) = 0,3.$$

Для адаптации полученных значений под требования ГОСТ Р ИСО/МЭК 27005-2010 и последующего расчета меры риска (таблица 3), переведем количественный показатель возможности реализации угрозы (V_{ry}) в качественный показатель возможности возникновения угрозы *(ПВВУ)*, таким образом, что:

0 – 0,4 *(V_{ry})* = «Низкий» *(ПВВУ);*

0,5 – 0,7 *(V_{ry})* = «Средний» *(ПВВУ);*

0,8 – 1*(V_{ry})* = «Высокий» *(ПВВУ).*

Данный переход от количественного показателя к качественному обоснован требованиями расчета риска в соответствии с матрицей, представленной в таблице 3, в которой значения для определения риска возможны только по качественным показателям.

Ценность активов определена согласно промежуточным денежным значениям вероятного ущерба ***S,*** подробно рассмотренного в главе 3 текста диссертационной работы, где «0» - 0 – 5000 рублей; «1» - 5000 – 10000 рублей; «2» - 10000 – 50000 рублей; «3» - 50000 – 100000 рублей; «4» - свыше 100000 рублей.

Таблица 3 - Матрица определения риска информационной безопасности

ПВВУ		Низкий			Средний			Высокий		
Простота использования		Н	С	В	Н	С	В	Н	С	В
Ценность активов	**0**	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Определение параметров риска рассмотрим на примере угрозы утечки акустической информации:

Последствия (ценность актива) определяем согласно соответствующей шкале: Возможный ущерб - 0,00 рублей, соответственно ценность актива «0».

Показатель возможности возникновения угрозы также определяем по соответствующей шкале: 0,3 – «Низкий».

Для определения меры риска необходимо воспользоваться таблицей 3 «Матрица определения риска информационной безопасности» и выбрать строку со значением ценности актива - «0» и вероятностью реализации угрозы – «Низкая».

Для определения простоты использования рассмотрим уязвимости, относящиеся к данной угрозе и значения их коэффициентов важности. Следует учитывать, что рассматриваем только актуальные уязвимости. Для выбранной угрозы актуальна только одна уязвимость с коэффициентом важности - 0,3. Согласно соответствующей шкале получаем, что значение простоты использования – «Низкая». По результату пересечения строки ценности актива и столбца простоты использования получаем значение меры риска.

Таблица 4 – Значение меры риска

Показатель возможности возникновения угрозы		Низкий		
Простота использования		***H***	С	В
Ценность активов	***0***	**0**	1	2

В случае если угроза имеет несколько актуальных уязвимостей, процедура проводится для каждой из них, и полученные значения суммируются для определения значения меры риска.

Таблица 5 - Определение меры риска угроз, согласно ГОСТ Р ИСО/МЭК 27005-2010. Ранжирование угроз посредством мер риска

Идентификатор угрозы (*a*)	**Последствия (ценность актива) (*b*)**	**Показатель возможности возникновения угрозы (c)**	**Мера риска (*d*)**
Угрозы утечки акустической информации	0	0,3	0
Угрозы утечки видовой информации	0	0,9	8
…	…	…	…
Общее	***32***	***19,53***	***191***

На следующем этапе происходит формирование групп угроз - «Конфиденциальность», «Целостность (Изменение)», «Целостность (Удаление)», «Доступность». Для каждой из групп определяются значения ценности активов и меры риска для группы, а также возможный ущерб. Общие значения получаются суммированием значений каждого столбца.

Таблица 6 - Угрозы «Конфиденциальность»

Конфиденциальность			
Идентификатор угрозы (*a*)	Последствия (ценность актива) (*b*)	Показатель возможности возникновения угрозы (*c*)	Мера риска (*d*)
Угроза утечки информации по каналам ПЭМИН	0	0,8	6
Кража физических ресурсов	2	0,72	12
Кража носителей информации	0	0,77	5
Кража ключей доступа	0	0,55	2
Кража, модификация, уничтожение информации (физ. доступ)	2	0,78	12
…	…	…	…
Общее	***16***	***15,47***	***127***

На основе полученных данных, разработан метод формирования критичной группы угроз. Данный метод реализован путем детализации уязвимостей, основан на методе аддитивной свертки, и отличается от известных тем, что для выявления групп критичных угроз применен метод Акоффа-Черчмена, позволяющий определить набор наиболее критичных угроз.

Степень критичности групп угроз предлагается определять на основе расчетного значения коэффициента риска:

$$K_d = \frac{b}{N_y}, \quad (4)$$

где K_d– коэффициент риска; b – последствия от реализации угрозы (ценность актива); N_y– количество угроз в группе.

Следующим этапом является сравнение показателей для групп угроз. Сравниваются альтернативы α_i по каждому показателю и производится ранжирование групп угроз. $\alpha_i = \{b, c, d\}$;

$\alpha_i(b) = \{74,42,66,42\} \rightarrow \alpha_i(b) = \{74,66,42,42\}$;

$\alpha_i(c) = \{15,47; 8,25; 12,63; 8,4\} \rightarrow \alpha_i(c) = \{15,47; 12,63; 8,4; 8,25\}$;

$\alpha_i(d) = \{292,154,243,149\} \rightarrow \alpha_i(d) = \{292,243,154,149\}$.

Критическая группа угроз определяется по коэффициенту риска, для этого сравниваются оценки альтернатив $\varphi(\alpha_i)$.

$\varphi(\alpha_i) = \{K_d\}$.

$\varphi(\alpha_i\ (K_d)) = \{17,33; 17,02; 17,86; 16,61\} \rightarrow \varphi(\alpha_i\ (K_d)) = \{17,86; 17,14; 17,33; 16,61\}$;

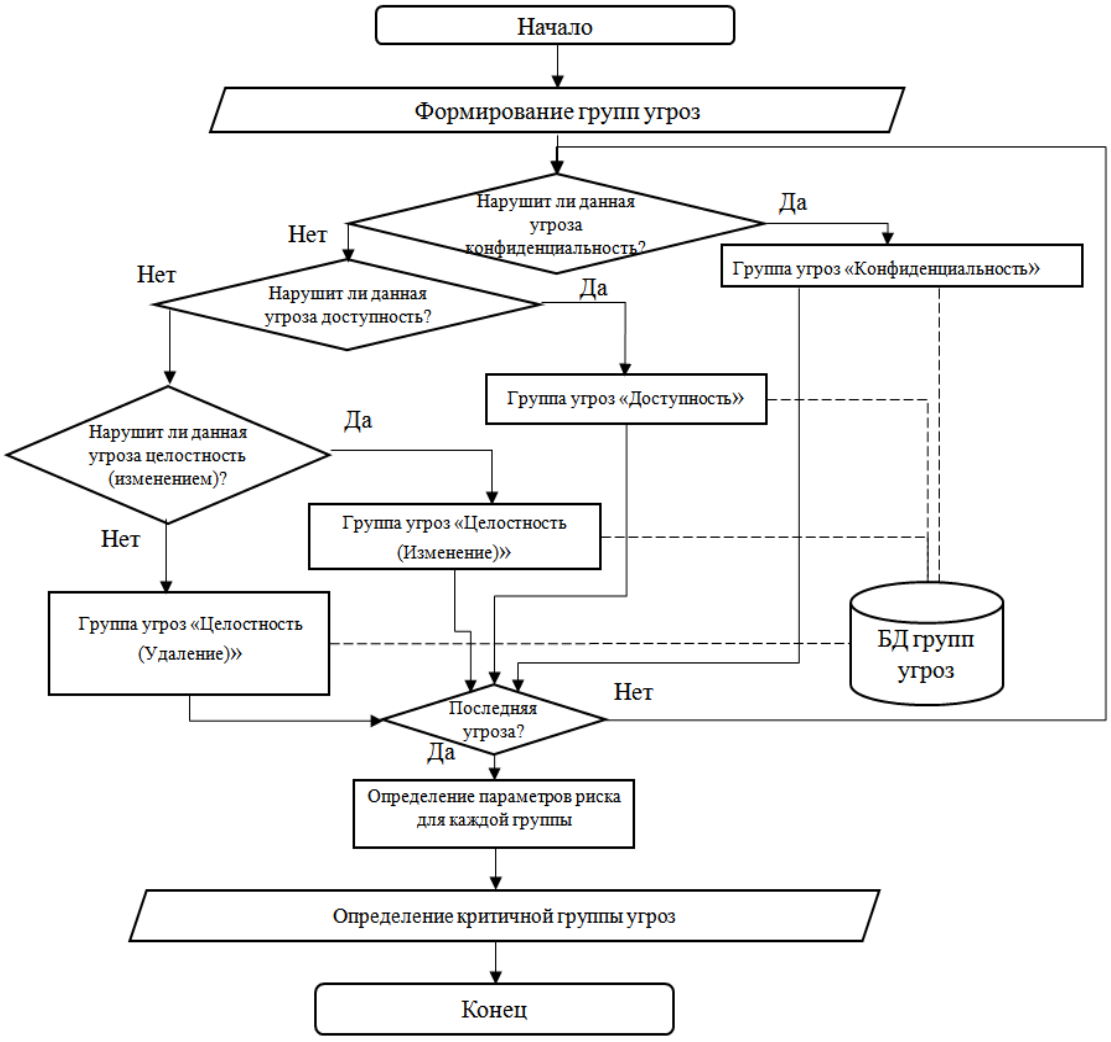


Рис. 2. Алгоритм определения критичной группы угроз

Полученные результаты (табл. 7) показали, что наибольшее значение коэффициента риска для рассматриваемого объекта имеет группа угроз «Целостность (Удаление)», таким образом, данная группа угроз расценивается как критичная.

Таблица 7 - Сравнение показателей для групп угроз

Группы Угроз	Последствия (ценность актива) (b)	Показатель возможности возникновения угрозы (c)	Мера риска (d)	Коэффициент риска K_d
Исходные значения	32	19,53	191	7,07
Конфиденциальность	16	15,47	127	5,77
Целостность (Изменение)	10	8,25	67	5,58
Целостность (Удаление)	30	12,63	140	7,77
Доступность	23	8,4	92	7,66

Разработана объектно-ориентированная модель оценки риска безопасности ИСПДн, основанная на аппарате раскрашенных сетей Петри, отличающаяся разработанными правилами срабатывания переходов и позволяющая учитывать меру риска ИСПДн, а также вероятности реализации и отражения угроз безопасности персональных данных.

В работе предлагается способ формального задания математической объектно-ориентированной модели оценки риска, построенной на базе раскрашенных сетей Петри:

$$R = < P, V_{ry}, T, I, O >, \quad (5)$$

где P – множество состояний сети Петри, V_{ry}– множество вероятностей реализации угроз, T–множество переходов определяющих правила изменения состояний сети, I – входные позиции (множество параметров угроз и контрмер), O – выходные позиции (множество значений остаточного риска).

Структура разработанной модели представлена на рис. 3.

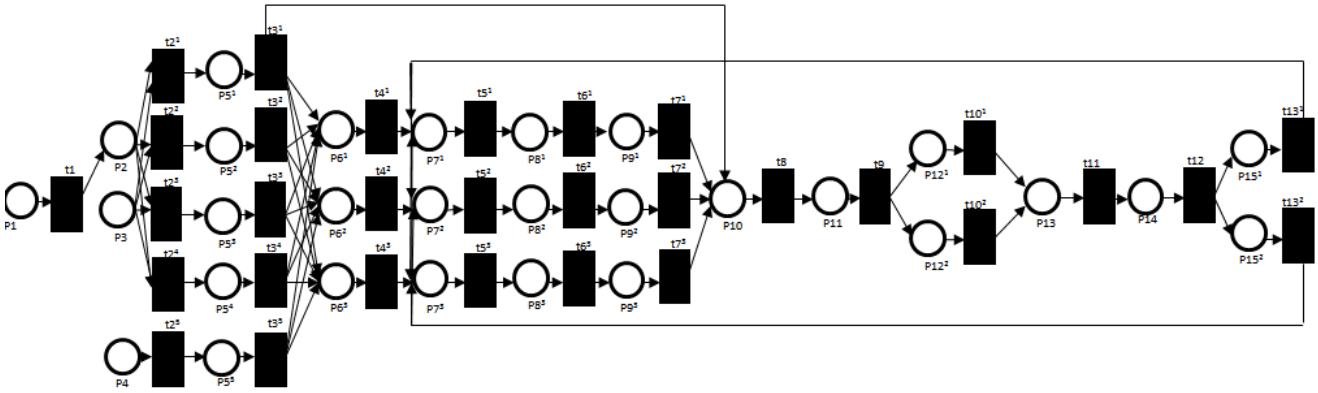


Рис. 3. Модель оценки риска нарушения безопасности ИСПДн

Расшифровка модели оценки риска нарушения безопасности $ИСПД_Н$ представлена в табл. 8.

Таблица 8 - Состояния модели оценки риска нарушения безопасности ИСПДН

P1	Ресурсы предприятия	P6	Критичность ущерба	P11	Определение контрмер (сопоставление, сравнение и определение вероятности устранения угрозы)
P2	Угрозы безопасности ПДн	P7	Определение вероятности возникновения угрозы для каждой из групп (уязвимости и данные анкетирования по ним)	P121 /2	Наборы контрмер
P3	Стоимость восстановления ресурса предприятия от угроз ПДн	P81/2/3	Определение меры риска (Ценность, вероятность возникновения, простота использования)	P13	Определение коэффициента мультипликативности
P4	Оборот предприятия	P9	Определение коэффициента риска (Мера риска и кол-во угроз в группе)	P14	Применение контрмер
P51/ …/4	Списки угроза-ущерб для 4х групп	P10	Критичная группа угроз	P151 /2	Угроза устранена/ не устранена

Для моделирования реагирования контрмер на угрозы безопасности фишки в данной сети определены на множестве $Color = \{red, blue\}$, причем фишки $Color = red$ соответствуют угрозам безопасности, а фишки $Color = blue$ контрмерам. При этом в позициях отражающих актуальные угрозы $\{P2, P3, P5, P6, P7, P8\}$ могут находиться только фишки $Color = red$, а в позициях, отражающих внедряемые контрмеры, $\{P1, P4, P9, P10, P11, P12\}$ – только фишки типа $Color = blue$.

Для записи в формализованном виде каждого из способов срабатывания перехода $T = \{t1, t2, t3, t4, t5, t6, t7, t8, t9, t10, t11, t12, t13\}$ введены дополнительные операнды и параметры:

$F(P_i)$ – функция, отражающая наличие фишки в позиции P_i;

$\varphi(P)$ – функция, отражающая совершение/отражение угрозы с вероятностью P;

P_{threat} – вероятность совершения угрозы;

$P_{reaction}$ – вероятность устранения угрозы.

На основе исходных данных по защищаемому объекту была предложена сеть Петри.

Правила срабатывания задаются с помощью терминальных языков описания сетей Петри:

$$P1_i \rightarrow \tau_i = t1_i(F_{P1i}),\ t2_i(F_{P2i}, F_{p3i}),\ t3_i(F_{P5i}),\ t4_i(F_{P6i}, \varphi(P_{threati})),\ t5_i(F_{P7i}, \varphi(P_{threati})),\ t6_i(F_{P8i}),\ t7_i(F_{P9}),\ ),\ t8(F_{P10}, \varphi(P_{reactioni})),\ t9(F_{P11}),\ ),\ t10_i(F_{P12i}, \varphi(P_w)),\ t11(F_{P13}),\ t12(F_{P14}),\ t13_i(F_{P15i}, \varphi(P)) \rightarrow P7^i. \quad (6)$$

Достоинством разработанной модели является реализация следующих возможностей: вероятностная сеть позволяет учесть, как реализацию рисков ПДн, так и контрмеры по их отражению за счет настройки вероятностей совершения переходов. Раскраска сети Петри позволяет идентифицировать фишки, ассоциируемые с рисками ПДн и контрмерами, а также обеспечивает реализацию механизма снижения уровня рисков при внедрении контрмер.

Разработанная сеть является динамической, так как, на каждом цикле просчета математической модели происходит ее адаптация к изменяющимся свойствам системы защиты персональных данных. Данный процесс можно представлен на рис. 4.

Рис.4. Алгоритм адаптации сети Петри

Для формирования набора контрмер по минимизации рисков ИСПДн предложены и реализованы способы определения и сравнения контрмер, расчета вероятности устранения угроз предложенными контрмерами и сформулирована теорема определения условия эффективности (*если рассчитан такой набор контрмер, при котором остаточный риск от их внедрения стремится к нулю, то их эффективность стремится к единице).*

Формируемый набор контрмер *(V)* можно представить в виде кортежа:

$$V =< K_d, T, Su >, \quad (7)$$

где:

K_d – величина остаточно риска, достигнутая применением сформированного набора контрмер; T – коэффициент отношения нейтрализованных угроз к общему числу угроз, Su – стоимость сформированного набора контрмер.

Таким образом, задача моделирования сводится к поиску такого набора контрмер, у которого остаточный риск $K_d \rightarrow 0$, $T \rightarrow 1$, при приемлемом значении суммарной стоимости данного набора контрмер.

В четвертой главе проведен анализ алгоритмов комплексного исследования объектов и выявления угроз ИСПДн. Определены основные этапы исследования объектов, включающие определение стоимости информационных ресурсов, выявление актуальных угроз и определение ущерба от их реализации,

определение вероятности реализации и устранения угроз, а также формирование критичных групп угроз.

Разработан **алгоритм оценки эффективности защиты ИСПДн** основанный на разработанных алгоритмах оценки ущерба и вероятности реализации угроз, а также на разработанной математической модели, позволяющий рассчитать показатели эффективности наборов контрмер для снижения риска ИСПДн (рис. 5).

Предложен алгоритм определения остаточных рисков для оценки эффективности внедренного набора контрмер и оптимизации принимаемых проектных решений.

Разработана **методика оценки и минимизации риска безопасности персональных данных**, основанная на многокритериальной оценке контрмер, представленная в виде следующей последовательности шагов:

Шаг 1. Комплексное исследование рассматриваемого объекта, включающее выявление и оценку стоимости информационных ресурсов, определение потенциального ущерба и вероятности реализации угроз. Результатом данного шага являются расчетные показатели, стоимости каждого вида конфиденциальной информации обрабатываемой на объекте исходя из суммы наносимого ущерба и стоимости их восстановления, а также коэффициенты реализуемости угроз и вероятности их реализации.

Шаг 2. Формирование групп угроз и выявление критичной группы угроз. На данном этапе происходит формирование групп угроз, что позволяет классифицировать наносимый ими ущерб, а также определить параметры риска для каждой группы угроз, провести ранжирование и выявить критичную группу угроз. В результате данного шага определяется группа угроз и величина риска безопасности ИСПДн, что позволяет определить контрмеры, необходимые для минимизации этого риска.

Шаг 3. Построение математической модели на основе раскрашенных сетей Петри, оперирующей показателями вероятности реализации и отражения угроз контрмерами, позволяющей рассчитать степень снижения уровня риска ИСПДн в результате внедрения наборов контрмер.

Шаг 4. Выбор эффективного набора контрмер для минимизации уровня рисков ИСПДн, исходя из сравнительного анализа полученных в результате просчета математической модели показателей суммарной стоимости наборов контрмер и рассчитанного уровня остаточного риска, отражающего их эффективность.

Особенностью разработанной методики является возможность оценки уровня остаточного риска от внедрения предложенного набора контрмер и определить степень влияния отдельных средств и методов защиты на общую защищенность ИСПДн.

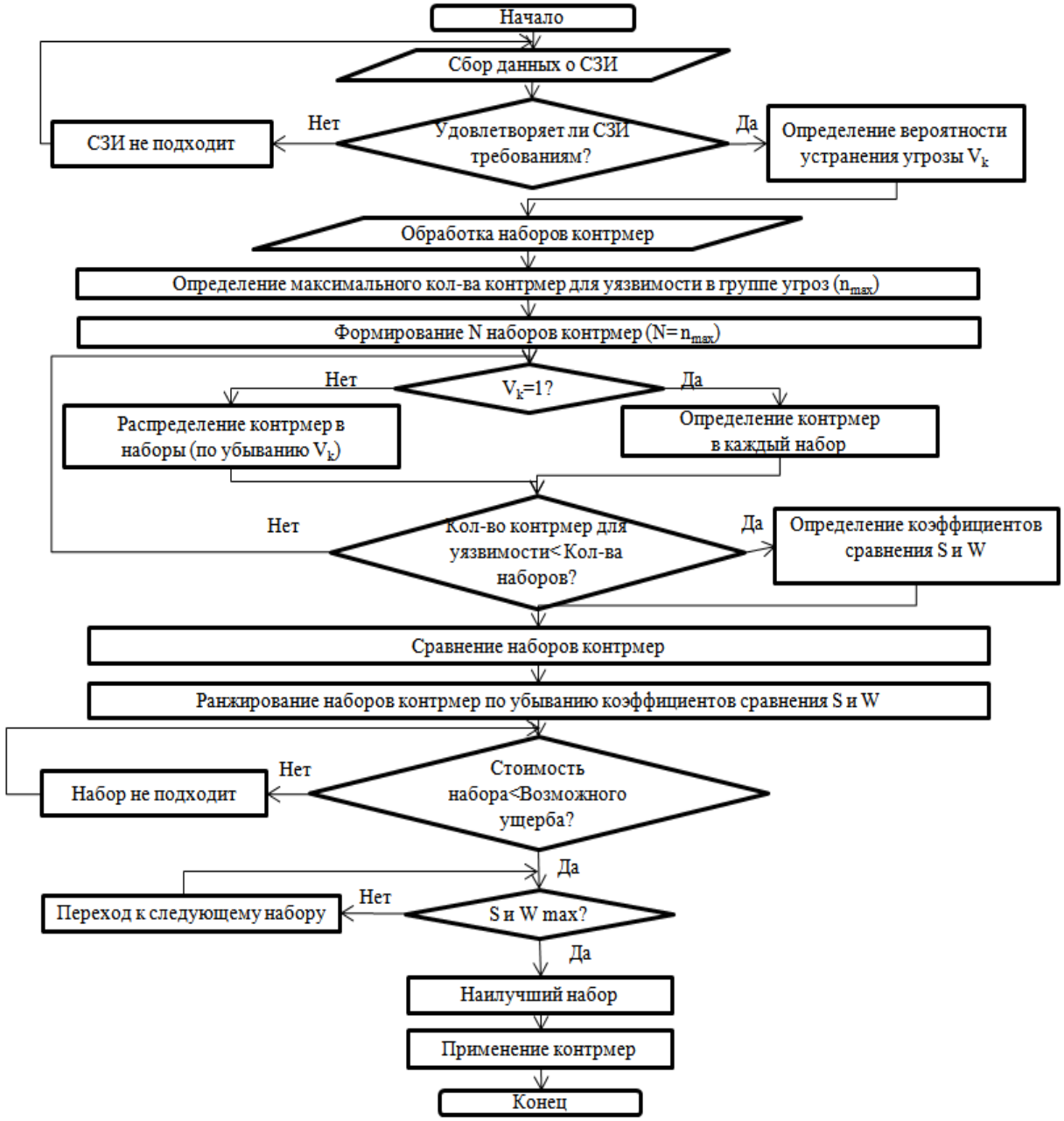


Рис.5. Алгоритм оценки эффективности защиты ИСПДн

В пятой главе разработана структура и состав основных компонентов автоматизированной системы оценки рисков безопасности ИСПДн.

Для обеспечения реализации функций, заложенных в архитектуру разрабатываемой автоматизированной системы, разработаны базы данных нормативно-правовых документов, определяющих размеры штрафов за нарушения безопасности ПДн и других видов конфиденциальной информации и БД контрмер для минимизации уровня рисков.

Разработана автоматизированная система оценки рисков безопасности ИСПДн, реализующая возможности производить оценку ущерба от нарушения свойств безопасности ИСПДн, рассчитывать вероятность реализации групп критичных угроз, а также вероятность устранения групп критичных угроз, что позволяет сформировать эффективный набор контрмер для снижения риска ИСПДн. Модульная схема работы разработанной АС представлена на рис.6.

Сформулированы требования к техническому обеспечению разработанной АС, позволяющие выбрать персональный компьютер для ее эффективной работы.

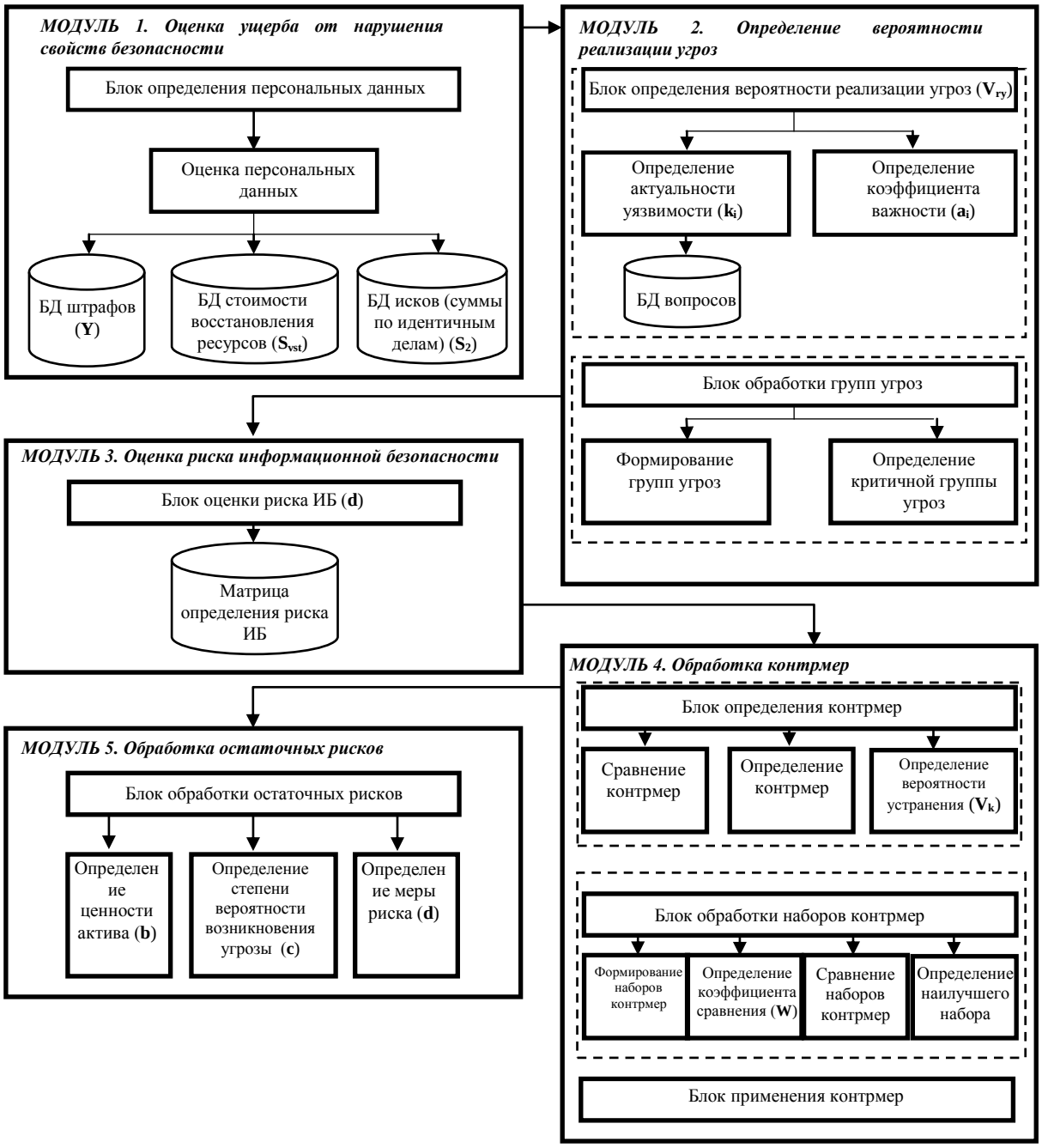


Рис.6. Модульная схема работы автоматизированной системы оценки рисков безопасности ИСПДн

Применение разработанной автоматизированной системы возможно как в научных целях, так и для построения эффективных систем защиты ИСПДн различных предприятий и организаций.

В результате применения разработанной автоматизированной системы для решения задач оценки и минимизации риска безопасности персональных данных уровень риска после внедрения контрмер, предлагаемых автоматизированной системой, снизился, в среднем на 85% (рис. 7).

Рис.7. Остаточный риск после устранения критичной группы угроз

В заключении сформулированы основные выводы и результаты работы.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработана модель оценки риска нарушения безопасности ИСПД, основанная на аппарате раскрашенных сетей Петри и разработанных правилах срабатывания переходов, отличающаяся учетом вероятностей реализации и отражения угроз и позволяющая учитывать меру риска ИСПДн в динамике протекающих процессов. Достоинством разработанной модели является реализация следующих возможностей: вероятностная сеть позволяет учесть, как реализацию рисков ПДн, так и контрмеры по их отражению за счет настройки вероятностей совершения переходов; раскраска сети Петри позволяет идентифицировать фишки, ассоциируемые с рисками ПДн и контрмерами, а также обеспечивает реализацию механизма расчета снижения уровня рисков при внедрении контрмер.

2. Разработан комплексный алгоритм расчёта вероятности реализации и отражения угроз нарушения безопасности персональных данных включающий алгоритм оценки ущерба от нарушения свойств безопасности ИСПД, основанный на экспертно-статистической оценке и алгоритм определения критичной группы угроз путем детализации уязвимостей, основанный на методе аддитивной свертки, отличающийся применением метода прогнозного графа и позволяющий рассчитать количественные и качественные оценки потенциального ущерба персональным данным. Разработан алгоритм выявления критичной группы угроз путем детализации уязвимостей, основанный на методе аддитивной свертки, отличающийся от известных тем, что для выявления групп критичных угроз применен метод Акоффа-Черчмена, и позволяющий определить набор наиболее критичных угроз.

3. Разработан алгоритм оценки эффективности защиты информационных систем персональных данных, опирающийся на сформулированную автором теорему определения условия эффективности.

4. Разработана методика оценки и минимизации риска нарушения безопасности персональных данных, основанная на многокритериальной

оценке контрмер, отличающаяся от известных применением метода аддитивной свертки при получении итогового значения вероятности устранения угроз и позволяющая сформировать эффективный набор контрмер для обеспечения безопасности ИСПДн.

Получены результаты экспериментальной апробации разработанной в ходе исследования автоматизированной системы по оценке рисков безопасности ИСПДн, показывающие экономию стоимости внедряемого набора контрмер в размере 50%, а так же сокращение временных затрат в 2,5 раза по сравнению с неавтоматизированным подходом к минимизации рисков.

Основные публикации по теме диссертации

Статьи в рецензируемых журналах, рекомендованных ВАК Минобрнауки РФ:

1. **Шинаков, К.Е.**Разработка автоматизированной системы аудита и построения модели объекта защиты с использованием технологии 3-D прототипирования [Текст]+[Электронный ресурс] /О.М.Голембиовская, К.Е.Шинаков, М.В.Терехов//Информация и безопасность.-Воронеж,№3, 2013.С.415-419.
2. **Шинаков, К.Е.**Оценка рисков информационной безопасности на основе анализа национального стандарта российской федерации ГОСТ Р ИСО/МЭК 27005-2010 [Текст] / О.М.Голембиовская, К.Е.Шинаков, М.М.Голембиовский // Информация и безопасность.– Воронеж, № 3, 2014.С. 31-37.
3. **Шинаков, К.Е.**Оценка риска информационной безопасности на основе интерпретации методики FRAP[Текст]+ [Электронный ресурс] /О.М.Голембиовская, К.Е.Шинаков//Информация и безопасность.-Воронеж,№4, 2015.С.430-434.
4. **Шинаков,К.Е.** Формализация процесса оценки рисков информационной безопасности на основе методики OCTAVE[Текст] + [Электронный ресурс] / О.М.Голембиовская, К.Е.Шинаков//Вестник БГТУ.-Брянск, 2015.-№3(47).-С.175-179.
5. **Шинаков, К.Е.** Оценка риска безопасности информационных систем, обрабатывающих конфиденциальную информацию [Текст] + [Электронный ресурс] / Шинаков К.Е., Рытов М.Ю., Голембиовская О.М., Чиркова К.Ю. // Вестник БГТУ.-Брянск, 2016.-№1(48).-С.193-200.

Монографии:

6. **Шинаков, К.Е.** Формализация подходов к обеспечению защиты персональных данных [Текст]+[Электронный ресурс]: монография/О.М.Голембиовская, М.Ю.Рытов, К.Е.Шинаков – Брянск: БГТУ, 2014. – 182 с.
7. **Шинаков К.Е.** Анализ рисков безопасности информационных систем персональных данных [Текст]+[Электронный ресурс]: монография / К.Е.Шинаков, М.Ю.Рытов, О.М.Голембиовская– Брянск: БГТУ, 2017. – 220 с.

Публикации в других изданиях, включая труды международных научно-технических конференций:

8. 8.**Шинаков, К.Е.**Формализация процесса определения класса защищенности информационных систем, не обрабатывающих сведений, составляющих

государственную тайну [Текст]/О.М.Голембиовская, К.Е.Шинаков, М.М.Голембиовский// Материалы Всероссийской научно-практической конференции (Воронеж, 22 ноября 2013 г.).-Воронеж: Руна, 2013.-№1.С.167-170.

9. **Шинаков, К.Е.**Подход к однозначному определению степени ущерба в соответствии с приказом № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [Текст + Электронный ресурс] / Шинаков К.Е., Голембиовская О.М., Кузнецова Е.В.// Материалы VII Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения» (28 апреля 2014 года).-Брянск, 2014.С. 39-42.
10. **Шинаков, К.Е.**Правовая защита персональных данных работников в Российской Федерации [Текст + Электронный ресурс] / Рытов М.Ю., Шинаков К.Е., Шпичак С.А. // Материалы VII Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения» (28 апреля 2014 года).-Брянск, 2014.С. 125-128.
11. **Шинаков, К.Е.**Оценка ценности информации посредством расчета стоимости восстановления ресурсов [Текст + Электронный ресурс]/ К.Е.Шинаков, О.М.Голембиовская// Материалы VII Межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных. Проблемы и пути их решения» (28 апреля 2015 года).-Брянск, 2015.С. 54-56.

Зарегистрированные программы для ЭВМ:

12. Автоматизированная система оценки уровня защищенности объектов информатизации № 2016615705/М.Ю.Рытов, А.П.Горлов, С.А.Шпичак, П.А.Ковалев, **К.Е.Шинаков**. Зарег.в реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (РОСПАТЕНТ) от 27 мая 2016 года;
13. Автоматизированная система оценки рисков безопасности информационных систем персональных данных №2017611715/ **К.Е. Шинаков**, М.Ю.Рытов, В.В.Аниканов - Зарег.в реестре программ для ЭВМ Федеральной службы по интеллектуальной собственности, патентам и товарным знакам (РОСПАТЕНТ) от 08 февраля 2017 года.

Подписано в печать 21.12.17. Формат 60х84 1/16.
Бумага типографическая №2. Офсетная печать. Т. 100 экз.

Брянский государственный технический университет,
241035, г. Брянск, бульвар 50 лет Октября, д.7.
Лаборатория оперативной полиграфии БГТУ, ул. Институтская, 16.