Федеральное государственное бюджетное учреждение науки
Санкт-Петербургский институт информатики и автоматизации
Российской академии наук
(СПИИРАН)

На правах рукописи

Носаль Ирина Алексеевна

Обоснование мероприятий информационной безопасности социально-важных объектов

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

Диссертация на соискание ученой степени
кандидата технических наук

Научный руководитель
д.т.н., профессор
Осипов В.Ю.

Санкт-Петербург – 2015

ОГЛАВЛЕНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированное рабочее место

БД – база данных

ЗИР – защищаемые информационные ресурсы

ИБ – информационная безопасность

ИС – информационная система

ИТ – информационные технологии

ОИ – объект информатизации

ОС – операционная система

ПД – персональные данные

ПО – программное обеспечение

ПФР – Государственное учреждение – Пенсионный фонд Российской Федерации

СВО – социально-важный объект

СЗИ – средства защиты информации

СИБ – система информационной безопасности

СМИБ – система менеджмента информационной безопасности

СУИБ – система управления информационной безопасностью

СОИБ – система обеспечения информационной безопасности

СППР – система поддержки принятия решений

СУБД – система управления базой данных

ТЗ – техническое задание

ФСБ – Федеральная служба безопасности Российской Федерации

ФСТЭК – Федеральная служба по технически-экспортному контролю России

В настоящей работе используются термины в соответствии со стандартами ГОСТ Р 52143-2013 [1], ГОСТ Р 50922-2006 [2], ГОСТ Р 53114-2008 [3], ГОСТ Р 51898-2002 [4], ГОСТ Р 51897-2002 [5], ГОСТ Р ИСО/МЭК 27001—2006 [6], ГОСТ Р ИСО/МЭК 13335-1-2006 [7], а также ФЗ РФ № 178-ФЗ [8], ФЗ РФ № 165-ФЗ [9] ФЗ РФ № 149-ФЗ [10], ФЗ РФ № 98-ФЗ [11], ФЗ РФ № 152-ФЗ [12]).

ВВЕДЕНИЕ

Для организаций, достигших определённого уровня зрелости [13] и нуждающихся в гарантиях непрерывности и качества выполнения своих задач и функций, обеспечение информационной безопасности является неотъемлемой частью основных рабочих процессов. Успешность современной деятельности во многом зависит и от эффективности использования имеющихся активов. Чаще всего организации становятся перед выбором между ущербом от нарушения состояния информационной безопасности (ИБ) и ценой реализации мероприятий ИБ. Решение этого вопроса при отсутствии соответствующих инструментов становится нетривиальной задачей. Набирающая обороты информатизация вносит свои коррективы в постановку задачи поиска мероприятий информационной безопасности. Такие мероприятия должны быть гибкими, адаптивными и масштабируемыми, должны учитывать комплексность и системность требований по защите, а также требования всех заинтересованных лиц.

Следует заметить, что подход к выбору мер информационной безопасности (ИБ) отражает отношение руководства к обеспечению ИБ и, кроме того, определяет всю дальнейшую политику ИБ организации. Поиск и обоснование мероприятий по ИБ может осуществляться для достижения следующих целей:

– приведение в соответствие требованиям регуляторов либо требованиям индустрии;

– адаптация системы ИБ к изменениям в самой организации и её окружающей среде;

– создание системы защиты в уже существующей инфраструктуре;

– создание новой информационной инфраструктуры с интеграцией мер безопасности;

– устранение последствий нарушения ИБ организации.

Все эти задачи были и остаются крайне актуальными для современных компаний, как частных, так и государственных. Однако для организаций и структур, которые относятся к социально-важным объектам (СВО), особенно важно уметь успешно решать такие задачи.

Основной целью СВО является предоставление государственных услуг населению и обеспечение конституционных прав граждан. Поэтому нарушение или прерывание работы СВО может привести к нарушению нормальной жизнедеятельности социально-незащищённых слоёв населения, возникновению общественных волнений, дестабилизации политической ситуации и в целом негативно отразиться на социально-экономической системе государства.

Информационная безопасность для социально-важных объектов – одно из главнейших условий надлежащего предоставления качественных государственных услуг населению. ИБ СВО является частью системы национальной безопасности и внутренней политики, а также влияет на безопасность личности, общества и государства. Для государства обеспечение информационной безопасности СВО – это гарантия надлежащего исполнения своих функций (обязательств перед населением).

В отличие от государственной безопасности, для обеспечения ИБ СВО предоставляется значительно меньше инструментов и ресурсов, однако предъявляется много требований, как со стороны государства, так и со стороны населения. Поскольку каждый субъект этой системы имеет свой круг интересов и задач, решаемых при помощи СВО, разнятся и предъявляемые требования.

При этом, отсутствует представление какой в целом должна быть система обеспечения информационной безопасности (СОИБ) СВО [14]. Основным подходом, который используется при построении СОИБ СВО, становится выполнение требований регуляторов, что недостаточно для комплексного обеспечения информационной безопасности. Требования разных регуляторов зачастую дублируются или вступают в противоречие друг с другом, не учитывают особенности, специфику работы, охватывают узкий перечень защищаемых ресурсов. Как следствие, это грозит нарушениями или затруднением деятельности СВО, увеличением нагрузки на персонал, усложнением документооборота, дублированием документации, мер и методов защиты. Поскольку технический прогресс вносит свои коррективы в построение СОИБ быстрее, чем регулирующий орган успевает внести изменения в законодательство, такие требования

устаревают. Главный недостаток этого решения – отсутствие комплексного подхода, что может привести к появлению уязвимостей в системе защиты, утечкам защищаемой информации и нарушению непрерывности основных деловых процессов.

Поэтому система информационной безопасности СВО остро нуждается в удобных, эффективных и надёжных методах поиска и обоснования мероприятий ИБ.

Известны многочисленные методы такого поиска и обоснования, однако в них не учитывается ряд особенностей, свойственных реальным процессам обеспечения ИБ СВО, в частности связанных с многократностью проводимых мероприятий, с изменением внешних и внутренних условий, целей защиты информации. Используемые модели и подходы к обоснованию мероприятий ИБ не в полной мере адекватны возможным ситуациям на объектах защиты, несовершенны методы управления ИБ СВО, нормативное, информационное и программное обеспечение процессов обоснования мероприятий ИБ.

Главный недостаток существующих методов заключается в том, что область их использования ограничена и распространяется на противодействие именно техническим и сетевым атакам или основывается исключительно на оценке экономической эффективности мероприятий. Выстраиваемая таким образом СОИБ не в полной мере обладает требуемыми свойствами: системность, интегрируемость, комплексность, прозрачность, адекватность, оптимальность и подконтрольность. Поэтому необходимо совершенствование соответствующего научно-методического аппарата.

Основной **целью** диссертационного исследования является повышение уровня информационной безопасности социально-важных объектов.

Решаемая научно-техническая задача: разработка новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, повышающих уровень их ИБ.

Для решения сформулированной научно-технической задачи в ходе выполнения диссертационных исследований предусматривались:

1) анализ известных структур систем и мероприятий ИБ СВО, выявление критичных ресурсов и существующих угроз ИБ СВО;

2) анализ существующих методов обоснования мероприятий ИБ и применимость их для целей ИБ СВО;

3) разработка метода управления СОИБ СВО на основе комплекса оптимизационных моделей, включая метод определения начальных состояний процессов;

4) поиск возможных оптимизационных моделей обоснования мероприятий ИБ СВО;

5) разработка модели функционирования СВО;

6) разработка моделей основных защищаемых деловых процессов ИБ СВО;

7) разработка моделей основных типовых процессов нарушения ИБ СВО;

8) апробация предложенных методов и моделей применительно к структурам ПФР;

9) обоснование состава пакета прикладных программ для специалиста, отвечающего за ИБ на СВО;

10) выработка методических рекомендаций по использованию предложенных моделей, методов и программных средств;

11) выработка практических рекомендации по совершенствованию организации информационной безопасности социально-важных объектов.

При выполнении диссертационного исследования использованы **методы** системного анализа, теории вероятности, алгебры, математический аппарат марковских процессов, теории графов и дифференциальных уравнений.

Объектом исследования являются основные деловые процессы и процессы нарушения информационной безопасности социально-важных объектов.

Предметом исследования выступает научно-методический аппарат обеспечения информационной безопасности социально-важных объектов.

Основные положения, выносимые на защиту:

1. Метод управления информационной безопасностью социально-важных объектов на основе комплекса оптимизационных моделей.

2. Метод обоснования мероприятий информационной безопасности по критерию минимума интегральных потерь.

3. Модели защищаемых и дезорганизующих процессов применительно к информационной безопасности социально-важных объектов.

4. Обоснованные рекомендации по повышению эффективности информационной безопасности социально-важных объектов.

Суть и новизна первого научного результата. Управление информационной безопасностью социально-важных объектов предложено осуществлять на основе нового комплекса оптимизационных моделей, ориентированных на широкий круг возможных ситуации. Учитываются структурные особенности защищаемых деловых процессов, ценность защищаемых информационных ресурсов, потенциальная информированность злоумышленников на текущий момент времени, ограничения на имеемые ресурсы и другие факторы. Предложенный метод развивает циклическую модель управления Шухарта-Деминга, являющегося стандартом в области обеспечения ИБ [5]. Новый метод подразумевает разработку новых или использование готовых моделей защищаемых деловых процессов СВО, а также оптимизационных моделей мероприятий защиты. Использование заранее разработанных моделей позволяет значительно повысить скорость поиска альтернативных мероприятий ИБ и скорость принятия решений. Предложенные оптимизационные модели охватывают комплекс условий и задач, которыми специалист по ИБ может руководствоваться при поиске оптимальных мероприятий ИБ. Особенность их построения заключается в способности задавать комбинации необходимых условий оптимальности мероприятий ИБ. На их основе могут быть выработаны наиболее адекватные поставленной задаче рекомендации. Теоретическая база метода позволяет использовать его не только при защите информационных систем СВО, но и обеспечении ИБ самого объекта.

Оригинальность второго научного результата заключается, прежде всего, в комбинации нескольких известных подходов к оценке рисков, ценности информационных ресурсов, к построению моделей дезорганизующих процессов и

поиску целесообразных мероприятий информационной безопасности. Обоснование мероприятий ИБ, согласно предлагаемому методу, рекомендуется осуществлять, исходя из минимума общих потерь, среди которых ключевое место занимают потери из-за снижения ценности защищаемых информационных ресурсов. Новизна предлагаемого метода состоит в новой совокупности условий, при которой предлагается обосновывать мероприятия ИБ. Отдельные положения метода могут быть применимы также при решении частных задач ИБ. В целом предлагаемый метод расширяет взгляды на обоснование мероприятий ИБ в различных условиях.

Третий научный результат представляет собой комплекс марковских моделей, формализующих типовые для СВО деловые процессы и комплекс марковских моделей, описывающих типовые наборы действий нарушителей, компонуя которые можно формализовать большинство атак на ИБ СВО. Новизна этих комплексов и самих моделей состоит, прежде всего, в предмете моделирования. С применением математического аппарата марковских процессов разработаны новые модели, отражающие типовые деловые процессы для СВО и типовые распространённые нарушения ИБ СВО. Каждая из этих моделей имеет свой смысл, выявленный на основе обширного профессионального опыта, а их структуры отражают реальную ситуацию в моделируемой области. Разработанные модели учитывают потенциальную многократность санкционированного и несанкционированного доступа к защищаемым информационным ресурсам, возможность пересмотра мероприятий защиты, а также блокирования доступа в случаях нарушения ИБ. Благодаря этому можно оценивать систему в различных условиях и осуществлять поиск целесообразных вариантов реализации мероприятий ИБ.

Четвёртый научный результат – это научно обоснованные рекомендации по повышению ИБ СВО. В рамках этих рекомендаций предложена архитектура комплекса программных средств обоснования мероприятий ИБ СВО. Этот комплекс позволяет формулировать рекомендации и управлять организационными мероприятиями по защите, вырабатывать политики высокого уровня и стратегию

обеспечения ИБ, формировать и обосновывать предложения по организации деловых процессов и построению самих объектов защиты. Предложены новые правила тестирования систем поддержки принятия решений (СППР) для СОИБ СВО. Разработаны методические рекомендации по использованию предложенных методов и моделей при решении типовых задач обеспечения ИБ СВО. Сформулированы предложения по совершенствованию организации ИБ СВО, в части развития нормативно-правовой базы, оценки рисков, предотвращения типовых нарушений.

В целом, теоретическая значимость полученных научных результатов состоит в развитии научно-методического аппарата обоснования мероприятий информационной безопасности социально-важных объектов.

Практическая значимость этих результатов заключается в возможности, путём их реализации, повысить уровень ИБ СВО, осуществлять оперативный поиск целесообразных мероприятий ИБ. Помимо повышения общего уровня безопасности ИБ СВО, предложенные решения могут найти применение при проектировании новых информационных инфраструктур социально-важных объектов и разработке интеллектуальных систем управления информационной безопасностью.

Обоснованность и достоверность научных положений обеспечены анализом текущего уровня исследований в данной области, корректным использованием апробированного математического аппарата, подтверждаются результатами вычислительных экспериментов и сверкой полученных результатов с реальным положением дел, а также апробацией на научных конференциях.

Апробация и реализация результатов. Основные положения диссертационной работы представлялись на международной научно-практической конференции «Перспективные информационные технологии (ПИТ 2014)» (г. Самара, 30 июня – 4 июля 2014г.) [14], всероссийской научно-практической конференции с международным участием «Комплексная защита объектов информатизации и измерительные технологии» (Санкт-Петербург, 16-18 июня 2014 г.) [136] и межрегиональной научно-практической конференции

«Информационная безопасность и защита персональных данных: Проблемы и пути их решения» (г. Брянск, 28 апреля 2014г.) [21].

Результаты диссертационной работы использованы при обеспечении информационной безопасности государственного учреждения - Отделения Пенсионного фонда Российской Федерации по Республике Коми. Они реализованы в НИР «Эстафета» (2014 г.).

Личный вклад соискателя. Все выносимые на защиту результаты получены лично автором. Автором лично разработан метод управления ИБ СВО на основе комплекса оптимизационных моделей. Существенно развит метод обоснования мероприятий ИБ по критерию минимума интегральных потерь. Лично разработаны модели защищаемых и дезорганизующих процессов применительно к ИБ СВО, обоснованы новые рекомендации по повышению ИБ СВО.

Основные результаты диссертации изложены в 7-ми публикациях, в том числе, в 4-х статьях, опубликованных в ведущих рецензируемых журналах, входящих в перечень ВАК, в материалах одной международной и двух российских конференций.

Диссертационная работа изложена на 159-ти машинописных страницах, включает 4 главы, 13 рисунков, 18 таблиц и список литературы (151 наименование).

1. АНАЛИЗ ПРОЦЕССА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО-ВАЖНЫХ ОБЪЕКТОВ

1.1. Цели, задачи и возможности систем информационной безопасности социально-важных объектов

Под социально-важным объектом (СВО) в данной работе подразумевается социально-ответственный институт, не входящий в систему государственных органов власти. Основной целью СВО является предоставление государственных социально-экономических услуг населению и обеспечение конституционных прав граждан в области социальной защиты, государственной социальной помощи и обязательного социального страхования. Примеры таких организаций – Фонд социального страхования, Фонд обязательного медицинского страхования, Пенсионный фонд Российской Федерации. Все эти организации по форме образования и расходования денежных средств являются внебюджетными государственными фондами, имеют схожие цели, задачи, принципы работы, административно-управленческую структуру и все они являются крупнейшими операторами персональных данных.

Информационная безопасность для СВО это одно из главнейших условий надлежащего предоставления ими качественных государственных услуг населению. Нарушение или прерывание работы СВО может привести к нарушению нормальной жизнедеятельности социально-незащищённых слоёв населения, возникновению общественных волнений, дестабилизации политической ситуации и в целом негативно отразиться на социально-экономической системе государства.

ИБ СВО является частью системы национальной безопасности и внутренней политики, а также влияет на безопасность личности, общества и государства. Для государства обеспечение ИБ СВО – это гарантия надлежащего исполнения своих функций (обязательств перед населением). В отличие от государственной безопасности, для обеспечения ИБ СВО предоставляется значительно меньше инструментов и ресурсов, однако предъявляется достаточно много требований, как

со стороны государства, так и со стороны населения. Поэтому система ИБ СВО – это система с множеством взаимозависимых субъектов и объектов защиты. Каждый субъект в ней может быть классифицирован исходя из задач, которые он решает с помощью СВО, а значит требований, которые он предъявляет к ИБ [14].

Целью ИБ СВО является обеспечение безусловного выполнения свойственных ему задач и функций. В условиях активной информатизации государства и населения (следовательно, повышения требований к скорости предоставления услуг) эту цель можно уточнить как обеспечение непрерывности качественного выполнения возложенных на СВО задач и функций.

Не следует забывать также, во имя чего СВО осуществляют свои задачи и функции: обеспечение благосостояния граждан и социально-экономического развития государства – этот принцип нигде не постулируется. При этом определение «качественное» подразумевает соответствие стандартам, регламентам и требованиям законодательства, в том числе законодательства по информационной безопасности. В таких условиях, к примеру, административный регламент предоставления государственной услуги является описанием эталонного выполнения задачи или функции СВО, а соответствие ему – показатель качества предоставленной услуги.

Перед системами ИБ СВО ставятся следующие задачи:

– реализация комплекса мер по обеспечению безопасности информационных ресурсов СВО;

– своевременное обнаружение фактов НСД и предотвращение деструктивного воздействия на информационные ресурсы;

– недопущение нарушающих функционирование воздействий на технические средства обработки и хранения информации;

– обеспечение восстановления информационных ресурсов в приемлемые сроки (в сроки, не приводящие к срыву возложенных на СВО основных задач).

На практике в качестве отдельных объектов защиты на СВО выступают их информационные ресурсы, среда обработки, сама система защиты. В

формулировке же целей и задач ИБ СВО защита других входящих в них объектов, помимо информационных ресурсов, не декларируется.

Решение существующих задач, как правило, направлено на своевременное обнаружение фактов нарушений, но не разработку мер превентивного предотвращения угроз безопасности.

Основное отличие ИБ СВО – это частичная принадлежность к системе обеспечения государственной безопасности. Во-первых, это слияние и наследие принципов и способов ИБ, используемых при обеспечении государственной безопасности, а во-вторых – жёсткий контроль государственных регуляторов. При этом, отсутствует представление, о том какой вообще должна быть система обеспечения информационной безопасности (СОИБ) СВО. Основным подходом, который используется при построении СОИБ СВО становится выполнение требований регуляторов, что недостаточно для комплексного обеспечения информационной безопасности. Требования разрабатываются без учета особенностей организации (специализации). Зачастую противоречивы, в основном охватывают узкий перечень защищаемых ресурсов. Поскольку технический прогресс вносит свои коррективы быстрей, чем регулирующий орган в законодательство, такие требования устаревают.

Требования разных регуляторов часто дублируются или вступают в противоречие друг с другом. Как следствие, это грозит нарушениями или затруднением деятельности СВО, увеличением нагрузки на персонал, усложнением документооборота, дублированием документации, мер и методов защиты. Главный недостаток этого решения – отсутствие комплексного подхода, что может привести к появлению «дыр» в системе защиты, утечкам защищаемой законом информации и нарушению непрерывности основных производственных процессов. Наличие отраслевого стандарта значительно продвинуло бы развитие ИБ СВО.

Отсутствует баланс между организационными и техническими мерами. Зачастую хорошо проработана техническая часть при отсутствии

поддерживающих, дублирующих и компенсирующих организационно-правовых мер.

Все это следствие низкоуровневого подхода к ИБ СВО, где целью ставится защита ресурсов, а не процесса в целом. В связи с чем, предлагается внести следующие коррективы в заявленные задачи ИБ СВО:

– реализация комплекса мер по защите активов и процессов СВО от воздействий, приводящих к нарушению непрерывности, снижению качества или срыву выполняемых СВО задач и функций, в том числе осуществляемых за счет превышения должностными лицами СВО своих полномочий (инцидентов информационной безопасности);

– превентивное предотвращение инцидентов информационной безопасности;

– обработка инцидентов информационной безопасности, предупреждение и обработка неблагоприятных последствий при возникновении инцидентов информационной безопасности, в сроки, не приводящие к срыву возложенных на СВО задач и функций;

– обеспечение восстановления активов СВО после инцидентов информационной безопасности в сроки, не приводящие к срыву возложенных на СВО задач и функций.

Система информационной безопасности должна работать на опережение, когда реализованы не только своевременное обнаружение нарушений и меры превентивного предотвращения угроз, но и составлено общее представление, о том, какой должна быть эта система. В системе управления должны предусматриваться пересмотр существующих и обоснование новых мероприятий. В интересах этого необходим предварительный анализ защищаемых объектов, вероятных угроз и ущербов.

1.2. Защищаемые информационные ресурсы социально-важных объектов и существующие угрозы

В процессе своей деятельности СВО используют большие объёмы разнородных данных, специфическое программное и аппаратное обеспечение, обширную информационно- вычислительную инфраструктуру [15]. Стандартами в области ИТ и ИБ зафиксированы такие определения, как ресурс (актив) и информация, однако термин «информационный ресурс» на текущий момент нормативной документацией не закреплён. Остановимся на том, что информационный ресурс – это совокупность данных, организованных для достоверного получения информации и извлечения знаний (источник знаний). Программное и аппаратное обеспечение – это среда функционирования и взаимодействия с информационными ресурсами, это средства обработки данных и информации в широком смысле. С другой стороны, структура базы данных, программный код, информационная технология и информационный сервис сами являются информацией (информацией об алгоритмах, функциях и операциях), зачастую уникальной и могут являться предметом гражданско-правовых сделок.

Учитывая, представленные выше ограничения перечислим типовой набор информационных ресурсов СВО. Сюда входят:

– документированная нормативная (управленческая, административная) информация;

– информационные ресурсы, используемые для предоставления услуг (выполнения конкретных задач СВО);

– информационные ресурсы, используемые для осуществления собственной хозяйственной деятельности СВО;

– информационные продукты на правах патентов, изобретений, регистраций в отраслевых фондах, прочие информационные объекты авторского права;

– информационные системы (управления, организации различных сервисных и производственных процессов СВО).

К информационным ресурсам СВО, помимо стандартных требований к целостности и доступности, а также конфиденциальности информации ограниченного доступа, предъявляются требования аутентичности, достоверности и неотказуемости. Рассмотрим их подробнее.

Доступность [1] – свойство, при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно. Требование, обязательно предъявляемое ко всем защищаемым ресурсам СВО. Документированная нормативная информация содержит всю информации о целях, задачах и методах работы СВО – такая информация должна быть открыта и общедоступна для ознакомления не только контролирующим и взаимодействующим с СВО организациям, но и любым гражданином. Нарушение доступности информационных ресурсов, используемых для предоставления услуг, может привести к снижению качества, прерыванию или срыву выполняемых СВО задач и функций. Обеспечение доступности информационных ресурсов, используемых для осуществления собственной хозяйственной деятельности СВО, должно осуществляться в соответствии с законодательством и оно влияет на непрерывность выполнения основных задачи функций СВО.

Целостность [1] – свойство сохранения правильности и полноты, при котором исключается любое изменение объекта, либо изменение осуществляется только субъектами, имеющими такое право. Требование, обязательно предъявляемое ко всем защищаемым ресурсам СВО. Для информационных ресурсов, используемых для предоставления услуг, оно обеспечивает внесение только преднамеренных изменений (не нарушающих достоверность информации), а также своевременное восстановление исходных данных. Угрозы нарушения целостности информации могут приводить к нарушению всех остальных её свойств.

Конфиденциальность [6] – свойство информации быть недоступной и закрытой для неавторизованного индивидуума, логического объекта или процесса, то есть свойство, при котором к объекту имеют доступ только те субъекты, которым такие права предоставлены. Это требование предъявляется к

ограниченному набору документированной нормативной информации и информационных ресурсов, используемых для осуществления собственной хозяйственной деятельности СВО, а также практически ко всем информационным ресурсам, обеспечивающим предоставление услуг. Из-за специфики выполняемых функций, СВО обрабатывают персональные данные и сведения, содержащие коммерческую тайну. При работе с такой информацией государством накладывается ответственность за нарушение её конфиденциальности и предъявляется (в лице регуляторов в области информационной безопасности[1]) определённый набор требований по созданию систем защиты.

Неотказуемость [6] – способность удостоверять имевшее место действие или событие так, что эти события или действия не могли быть позже отвергнуты. Выполнение этого свойства требуется для документированной нормативной информации, информационных ресурсов, используемых для предоставления услуг и информационных ресурсов, используемых для осуществления собственной хозяйственной деятельности СВО.

Поскольку управляющие органы СВО обладают определённого рода ответственностью при принятии решений и принимаемые решения имеют материальные последствия (материальную зависимость), обеспечение юридической значимости всех обрабатываемых данных и выполняемых с ними действий играет большую роль в работе этих объектов.

Должна зафиксироваться всеми сторонами достоверность данных, вносимых в системы СВО, и дальнейшая их неизменность, подотчётность выполняемых с ними действий. Также должна осуществляться фиксация обязательств и ответственности за выполнение того или иного действия.

Достоверность [6] – свойство соответствия предусмотренному поведению или результату, реальному положению дел. Требование, обязательное только для информационных ресурсов, используемых для предоставления услуг, поскольку

[1] Государственные регуляторы в области информационной безопасности – ФСБ, ФСТЭК, Роскомнадзор – ссылки на ФЗ.

для СВО характерна высокая скорость устаревания обрабатываемых данных. От наличия достоверной информации зависит правильность принятия решений, а значит выполнение основных задач СВО, правильность расходования средств и качество предоставления государственных услуг.

Аутентичность [6] – свойство, гарантирующее, что объект или субъект идентичны заявленным. Это свойство учитывается только для информационных ресурсов, используемых для предоставления услуг. Обеспечивает точность идентификации лиц, в отношении которых СВО принимает решения и однозначность соотнесения введённых данных идентифицированному лицу. Аутентичность касается специфики СВО обрабатывать большие объёмы разнородных персональных данных. Выполнение этого требования обеспечивает однозначную идентификацию субъекта персональных данных.

Таким образом, мы можем заключить, что качество предоставляемых СВО услуг определяется не только соответствием Регламенту, но также и качеством входных данных – их целостностью, аутентичностью, достоверностью и неотказуемостью.

Согласно принципам комплексности и системности обеспечения информационной безопасности к защищаемым ресурсам следует относить не только информационные ресурсы, но среду их функционирования, включая средства обработки и защиты.

Для СВО характерны следующие типы активов, относящиеся к среде функционирования информационных ресурсов:

- линии связи и сети передачи данных;
- инфраструктурные активы, обеспечивающие аппаратные и аппаратно-программные средства;
- программно-технические комплексы информационных систем;
- прикладное и общесистемное программное обеспечение;
- файлы, базы, хранилища данных;
- носители информации, в том числе бумажные;
- помещения, здания, сооружения и другие.

К среде использования информационных ресурсов предъявляются требования целостности и доступности, а также конфиденциальности тех активов, которые задействованы в обработке информации ограниченного доступа.

На СВО распространена ситуация, когда для обработки информации используется разработанное собственными силами ПО, поскольку набор выполняемых СВО функций специфичен и требует от производителя глубокого понимания автоматизируемых процессов. Такое ПО обладает рядом недостатков: неотслеживаемость изменений; моральное устаревание; отсутствие возможности интеграции и гарантий обеспечения свойств, предъявляемых к информационным ресурсам; возможность внесения закладок и другие.

Для работы с информационными ресурсами СВО при предоставлении услуг применяются программно-технические комплексы (ПТК) [11, 16, 17, 18]. Предусматривается наличие централизованного хранения и обработки ресурсов в рамках одного программно-технического комплекса, при возможном дублировании информации в разных комплексах, многопользовательский тип доступа, унифицированность и взаимосвязанность форматов представления информации, возможность экспорта, импорта и слияния ресурсов из других ПТК.

Возможность извлечения и использования информационных ресурсов в других информационных системах диктуется необходимостью информационного взаимодействия с другими СВО, органами государственной власти и государственными организациями. Также следует учитывать, что одни и те же информационные ресурсы, необходимые для выполнения разных задач, могут одновременно использоваться в разных ПТК. Эти особенности одновременно угрожают нарушению достоверности и аутентичности информации.

Для производителей ПТК могут ставиться требования обеспечения гарантий высокого уровня. Во избежание рисков производители поставляют полностью укомплектованный аппаратно-программный продукт. Такие ПТК часто однозначно определяют способ представления информации, а в некоторых случаях, он сильно зависит и от аппаратных средств (IBM менфреймы и др.).

Таким образом, можно сделать вывод, что любые ресурсы СВО, контактирующие с защищаемой информацией (средства обработки, управления, средства защиты), могут использоваться для нарушения информационной безопасности организации, поэтому их защита входит в компетенцию служб информационной и физической безопасности.

В общем виде, опираясь на структуру органов Пенсионного фонда Российской Федерации, можно представить типовую информационно-организационную структуру СВО следующим образом – рисунок 1. Используемые на рисунке 1 обозначения представлены в таблице 1.

Представленный ниже рисунок иллюстрирует центричность и иерархичность организационно-управленческой и информационной структуры СВО. Наличие многоуровневой структуры обусловлено спецификой обработки информации и необходимостью мониторинга и контроля при принятии решений. Центральное место в этой структуре отведено подразделению персонифицированного учёта, поскольку именно здесь осуществляется синтез всех информационных потоков и баз данных СВО. Следующий уровень представляет собой подразделения, осуществляющие анализ и контроль, планирование работ и мониторинг основных деловых процессов СВО, в рамках чего взаимодействуют с внешними организациями на уровне руководства – при создании стратегий, организации партнёрских программ и т.п., участвуют в администрировании ПТК и баз данных, предоставляют методическую помощь подведомственным подразделениям по направлениям работ. Второй уровень представлен непосредственно теми подразделениями, которые и выполняют основную часть работы, являются ядром делового процесса. И последний уровень, расположившийся по периметру, осуществляет непосредственное взаимодействие с внешними организациями и клиентами, а также подготовку и первичную обработку поступающей информации.

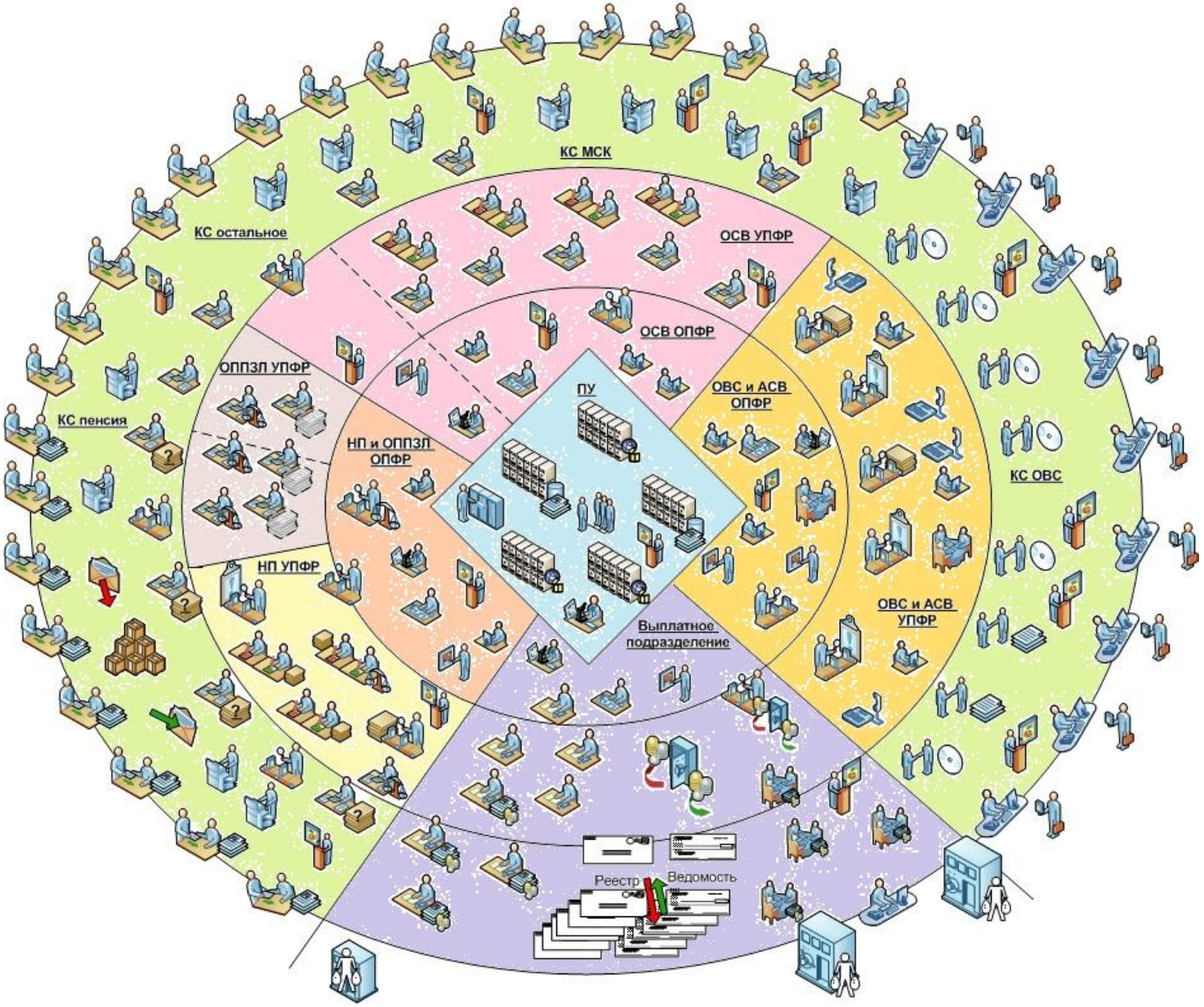


Рисунок 1 – Информационно-организационная структура СВО

Таблица 1. Обозначения, используемые на рисунке 1

Обозначение	Расшифровка
УПФР	Районный уровень СВО
ОПФР	Региональный уровень СВО
ПУ	Персонифицированный учёт граждан
ОСВ	Осуществление социальных выплат
КС	Клиентская служба
МСК	Материнский семейный капитал
ОППЗЛ	Оценка пенсионных прав застрахованных лиц
НП	Назначение пенсии
ОСВ и АСВ	Взаимодействие со страхователями и администрирование страховых выплат
Реестр и ведомость	Выплатные документы
	Персонал отдела
	Система персонифицированного учёта (базы данных, репликации, синхронизации и т.п.)
	Администрирование баз данных
	Приём граждан
	Копирование и сканирование документов, формирование электронных макетов дел
	Контроль (проверка правильности, соответствия и т.д.)
	Камеральная проверка страховых выплат
	Документальная проверка страховых выплат
	Направление запроса в другие организации
	Анализ выплатного дела
	Анализ документов
	Юридическая оценка документов
	Подготовка макета выплатного дела по предварительной работе с гражданами
	Принятие решения об удовлетворении заявления в выдаче МСК
	Принятие решения об удовлетворении заявления в выплате пенсии
	Разъяснительная работа с гражданами и другими организациями
	Разъяснительная работа и методическая помощь подведомственному отделу

	Оформление договорённостей с партнёрами (доставочными организациями, другими фондами и правительственными организациями)
	Планирование и отчёты
	Анализ и оценка текущей работы
	Расчёт сумм к выплате
	Мониторинг движения денежных средств
	Движение денежных средств (начисление к выплате, формирование доставочных документов)
	Доставочные организации (почта, банки)
	Взаимодействие со страхователем
	Сдача отчётности страхователем в электронном виде
	Сдача отчётности страхователем в бумажном виде
	Поиск недобросовестных страхователей (невыплатников)
	Оформление договорённостей со Страхователями и правительственными организациями

Представленная выше структура характерна для территориального подразделения СВО и одновременно в целом описывает принцип работы СВО на федеральном уровне. Обозначенные здесь ПТК обычно реализуют справочные, информационно-поисковые и расчётные функции. Однако всегда возникает необходимость в выделении модулей, обеспечивающих выполнение специфичных функций. Географическая распределённость потребителей услуг и распределённость внутренней структуры СВО требует создания нескольких взаимодействующих между собой опорных центров обработки данных.

Поэтому невозможен полный переход на централизованный вид обработки информации, всегда будет иметь место некоторая распределённость структуры хранения и обработки данных, наличие многих точек информационного слияния и обмена с ресурсами других организаций, в том числе вышестоящих и

выполняющих сопутствующие задачи. Здесь нельзя не упомянуть о необходимости организации и поддержки защищённых каналов связи, например, на базе технологии виртуальных частных сетей, для обеспечения защищённого межсетевого взаимодействия внутри системы СВО и с организациями – партнёрами.

Являясь частью системы предоставления государственных услуг населению, СВО остро нуждаются в развитии и поддержке системы электронного документооборота между всеми своими узлами и сталкиваются с необходимостью принимать активное участие при реализации систем государственного межведомственного документооборота.

Такие системы взаимодействия (виртуальные частные сети, электронный документооборот) могут быть реализованы при наличии в составе территориальных органов СВО удостоверяющих центров и органов криптографической защиты. Имея в своём составе аккредитованный удостоверяющий центр, СВО получает возможность не только развернуть полноценную систему юридически-значимого электронного документооборота, но также обеспечивать юридическую значимость совершаемых действий и вносимых изменений в различных целевых ПТК.

Ещё одна особенность – это большие объёмы обрабатываемой информации ограниченного доступа и многопользовательский доступ к ПТК. Такая особенность влечёт за собой ряд угроз информационной безопасности [19], которые требуют разрешения проблемы обеспечения легитимности/правомерности, обоснованности, своевременности и прозрачности предоставления доступа к информационным ресурсам.

Для каждого типа ресурсов должна существовать своя методика оценки ценности в зависимости от специфических характеристик. Ресурсы можно классифицировать по ряду признаков, указывающих на определённую особенность при оценке их стоимости (ценности):

- по уникальности (заменимости, наличию аналогов);
- по участию в процессе предоставления услуги (решению задач) СВО;

– по степени критичности соответствия стратегическим приоритетам предприятия (повышению эффективности, экономии);

– по сроку службы (устареванию, актуальности);

– по увеличению прибыли (дефициту, перерасходу ресурсов).

Указанные выше подгруппы могут объединяться, либо являться аналогами друг друга для разных типов ресурсов.

Каким образом, например, уникальность ресурса влияет на оценку его ценности? Допустим, в организации оценка физических ресурсов производится с учётом стоимости их замены или восстановления работоспособности. Программные ресурсы оцениваются тем же способом, что и физические - на основе определения затрат на их приобретение или восстановление. Однако, в такой ситуации как у СВО, когда программное и аппаратное обеспечение определяет способ представления информации, величина ущерба от нарушения работы самостоятельного разработанного и приобретённого коммерческого ПО заметно отличается. В частности, обеспечиваемыми гарантиями и ресурсами, затрачиваемыми на восстановление. Сложность (читай стоимость) перехода на широко распространённый коммерческий аналог будет тем выше, чем специфичней образ представления данных. Стоит также отметить, что, в некоторых случаях, представление информации сильно зависит и от аппаратных средств, если ПО ПТК было разработано таким образом (IBM менфреймы и др.). Информация, в свою очередь, может и вовсе не иметь аналогов, следовательно, и стоимость её должна заметно отличаться. Следует заметить, что ценность информационных ресурсов снижается при потере свойств, которыми они должны обладать.

Учитывая специфику обрабатываемых СВО информационных ресурсов, можно выделить характерные для них источники угроз. Будем исходить из того положения, что самым слабым звеном в системе ИБ является человеческий фактор и потому наибольший интерес и коэффициент полезности имеет анализ угроз антропогенного характера.

Для описания угроз такого типа необходимо рассмотреть вероятные для СВО виды нарушителей и преследуемые ими цели, объекты нападения, используемые для этого каналы.

Для классификации нарушителей по типу мотивации были использованы категории, предлагаемые стандартом обеспечения безопасности сетей электросвязи [20], поскольку перечень, представленный в этом стандарте, по сравнению с другими стандартами обеспечения безопасности, является наиболее полным. Итак, к таким категориям относятся: месть, достижение денежной выгоды (в том числе конкурентное преимущество), хулиганство и любопытство, профессиональное самоутверждение, политика и идеология.

Из ресурсов, доступных нарушителю следует выделить стандартный набор оборудования, которое требуется для совершения атаки – когда нарушителю достаточно иметь в своём распоряжении персональный компьютер средней мощности, а используемое программное обеспечение может быть частью самого защищаемого объекта (например, отладчик в операционной системе) или легко получено. Например, скрипты для использования широко известных уязвимостей, генераторы паролей и другое программное обеспечение (ПО) для взлома, которое можно найти в Интернете.

Следующий уровень - специализированное оборудование, которое может быть приобретено, либо доступ к которому может быть получен с использованием некоторых усилий, привлечение специалистов. В основном - высоко производительное оборудование и ПО для идентификации уязвимостей и нападения. Также сюда можно отнести разработку собственных скриптов и сценариев нападения.

И последний вариант – для совершения атаки требуется заказное оборудование, не доступное широкому кругу в силу высокой стоимости, либо настолько специализировано, что может потребоваться его специальная разработка, либо связанное с обеспечением безопасности государства, так что его распространение является контролируемым и, возможно, даже ограниченным. К ним можно отнести бот-неты, анализаторы радиоспектра, криптолаборатории и

т.д., а также необходимость привлечения высококвалифицированных специалистов из смежных областей.

По обладанию компетентностью можно выделить:

– эксперты хорошо знакомы с основными алгоритмами, протоколами, аппаратными средствами, структурами и т.п., реализованными в типе продукта или системы, а также с применяемыми принципами и концепциями безопасности;

– профессионалы хорошо осведомлены в том, что касается режима безопасности продукта или системы данного типа;

– непрофессионал слабо осведомлён по сравнению с экспертом или профессионалом и не обладает специфической компетентностью.

По обладанию информацией об объекте (информированность):

– отсутствие информации об объекте, кроме его назначения и общедоступной информации, полученной из открытых источников;

– внутренняя информация, для служебного пользования, кроме информации о системе защиты СВО;

– чувствительная информация об объекте (информации о системе защиты СВО, позволяющая совершить атаку и получить большие объёмы внутренней информации).

В качестве внутренних нарушителей информационной безопасности СВО могут выступать различные категории сотрудников этих объектов. Прежде всего, к ним относятся лица, имеющие определённую квалификацию и доступ к защищаемым ресурсам.

Таблица 2. Характеристики внутреннего нарушителя СВО

Категория\Хар-ка	**Мотивация**	**Ресурсы**	**Компетенция**	**Информированность**
Персонал выполняющий основные деловые процессы (ДП)	-достижение денежной выгоды; хулиганство и любопытство; месть	Стандартное	Эксперт, профессионал, Не профессионал	Чувствительная, Внутренняя
Персонал выполняющий вспомогательные ДП	-достижение денежной выгоды; хулиганство и любопытство; месть	Стандартное	Не профессионал	Внутренняя
Персонал служб, осуществляющих собств.хоз.деятельность	-достижение денежной выгоды; хулиганство и любопытство; месть	Стандартное	Не профессионал	Общая
Административно-управляющий персонал (АУП)	-достижение денежной выгоды;	Стандартное	Не профессионал	Чувствительная, Внутренняя
ИТ и ИБ специалисты	- проф. самоутверждение; достижение денежной выгоды; хулиганство и любопытство; месть	Специализированное и заказное	Эксперт, профессионал	Чувствительная
Обслуживающий персонал	-достижение денежной выгоды; хулиганство и любопытство; месть	Стандартное	Не профессионал	Общая

Резюмируя, можно сказать, что из внутренних нарушителей наиболее опасны специалисты служб ИТ и ИБ - они имеют доступ к широкому спектру оборудования и хорошо осведомлены о работе информационных систем. Специалисты, работающие в службах ИТ и ИБ, кроме того, обладают чувствительной информацией об объекте нападения, его уязвимостях. В свою очередь пользователи информационных ресурсов имеют доступ к большим объёмам персональных данных, а также от правильности и слаженности их действий зависит непрерывность выполнения основных деловых процессов СВО.

С другой стороны, персонал служб, осуществляющих собственную хозяйственную детальность, не имеет санкционированного допуска к ресурсам, но при наличии соответствующей мотивации может получить физический доступ.

Таблица 3. Характеристики внешнего нарушителя СВО

Категория \ Хар-ка	Мотивация	Ресурсы	Компетенция	Информированность
Граждане, которым СВО оказываются услуги	-достижение денежной выгоды; хулиганство и любопытство; месть	Стандартное	Не профессионал	Общая
Организации, которым СВО оказываются услуги	-достижение денежной выгоды; месть			
Организации (ИТ и ИБ направленности), которым СВО оказываются услуги		Специализированное и заказное	Эксперт, профессионал	Общая
Организации, с которыми СВО состоит в межведомственном взаимодействии	-достижение денежной выгоды; политика; идеология	Стандартное	Не профессионал	Общая
Бывшие сотрудники УВШ	-достижение денежной выгоды; месть	Стандартное	Не профессионал эксперт, профессионал	Чувствительная, внутренняя
Бывшие сотрудники УВШ, по направлениям ИТ и ИБ	-проф. самоутверждение; достижение денежной выгоды; месть	Специализированное и заказное	Эксперт, профессионал	Чувствительная
Взломщики программных продуктов	-проф. самоутверждение; достижение денежной выгоды; идеология			Общая
Поставщики и провайдеры ИТ ИБ услуг	-достижение денежной выгоды; месть	Специализированное и заказное	Эксперт, профессионал	Чувствительная
Криминальные структуры	-достижение денежной выгоды; политика	Специализированное и заказное	Эксперт, профессионал	Общая
Террористы	- политика; идеология			
Спецслужбы				

Что касается внешних нарушителей, здесь наиболее опасны в плане силы мотивации и обладания ресурсами криминальные структуры, террористы, спецслужбы. Мотивированный нарушитель, обладая достаточными ресурсами, обязательно приобретёт необходимую компетентность и информированность для успешного осуществления атаки. В то же время следует заметить, что вероятность возникновения мотивации для террористов и спецслужб значительно меньше, чем для криминальных структур, хакеров, бывших сотрудников, поставщиков и провайдеров ИТ и ИБ.

Наиболее опасными из них следует назвать лиц с высокой квалификацией в области ИТ и ИБ. Криминальные структуры тоже попадают в этот список, но вследствие сложности получения денежной выгоды реже становятся нарушителями ИБ СВО.

Виды угроз, которые могут быть реализованы в отношении СВО, обусловлены возможностями нарушителя [21] (квалификацией, осведомлённостью, имеемыми ресурсами) и мотивацией. От последней зависят ресурсы, которые могут быть атакованы данным злоумышленником, а также степень деструктивного воздействия (утечка информации, нарушение доступности, целостности, фальсификация, публикация самого факта и т.д). Цели нарушителя влияют на то, какие свойства информационных ресурсов, либо процессов, СВО будут нарушены и какой ущерб будет нанесён.

Поскольку все описанные выше факторы специфичны для разных организации, для каждого СВО должна быть разработана своя модель нарушителя и модель угроз, которые должны пересматриваться с определённой периодичностью, обеспечивающей актуальность разработанных моделей.

Стремительное развитие информационных технологий и повышение осведомлённости населения в этой области способствуют распространению специальных средств и инструментов, которые могут быть использованы для осуществления атак. Это повышает возможности потенциального нарушителя и появления все новых и новых видов атак. Такая адаптируемость угроз к мероприятиям защиты приводит к необходимости постоянно отслеживать актуальность этих угроз для СВО, пересматривать эффективность существующих мероприятий по защите и вырабатывать своевременные обоснованные решения.

Модель угроз должна строиться также на основании оценки ценности ресурсов, критичности нарушения деловых процессов и опасности реализации той или иной угрозы для организации (стейкхолдеров, заинтересованных лиц). Исходя из представленных данных, и в результате анализа и оценки деловых процессов СВО, представленных в параграфах 3.1 и 3.3 настоящей работы, в параграфе 3.3

будут подробно рассмотрены и проанализированы типовые для СВО угрозы нарушения информационной безопасности.

1.3. Анализ известных структур систем и мероприятий информационной безопасности социально-важных объектов

Отношение организации к состоянию «безопасности» определяет, в конечном счёте, структуру её системы информационной безопасности. К примеру, для государственной безопасности отсутствие контроля над защищаемым объектом на какой угодно малый промежуток времени уже является реализованной атакой (значимым инцидентом равносильным утечке). Не требуется доказательство факта утечки, достаточно одного только подозрения в этом, т.е. бесконтрольного пребывания объекта.

Для АСУ ТП в промышленности важно – был ли факт нарушения производственного процесса и насколько критичны последствия (причинён ущерб только установке, зданию, заводу, концерну, региону, государству, населению). Для банковского сектора важны репутация (не огласка инцидента), размер денежных потерь банка (насколько он критичен), вне зависимости от того, была ли реализована или остановлена атака (угроза). Для СВО важно – был ли нанесён в результате ущерб населению или государству (прямой или косвенный) и его размер.

Для коммерческой организации риск-менеджмент подход соответствует ценностям бизнеса. Сами по себе расходы (ущерб от реализации атаки) не являются чем-то негативным, при условии, что расходы не должны превышать доходы. То есть мы пытаемся предотвратить нанесение ущерба только тогда, когда его предотвращение стоит дешевле, чем его реализация.

Государственная безопасность оперирует другими понятиями о безопасности. Здесь неопределённость и вероятностный подход не применяется в принципе. В отличие от государственной безопасности, для обеспечения

информационной безопасности СВО предоставляется значительно меньше инструментов и ресурсов.

У СВО отличное от вышеназванных организаций понимание «информационной безопасности». Риск-менеджмент вполне приемлем для СВО, если не брать во внимание, что здесь ущерб рассчитывается не по отношению к СВО, а к его клиентам (остановка/нарушение работы этого объекта наносит ущерб населению). Для этого требуется определять ценность той или иной информации для каждого конкретного человека и обобщать её.

Следует отметить, что СВО очень подвержены атакам третьего поколения [22], как находясь в положении жертвы, так и будучи задействованным в качестве третьего лица (посредника). В ситуации, когда СВО подвергается атаке третьего поколения, урон информационным ресурсам СВО может быть не на нанесён вовсе, однако репутационные риски могут быть очень велики.

Поскольку информационная безопасность СВО защищает интересы населения, все риски, в том числе и репутационные, и нанесённый ущерб мы должны рассчитываться в отношении населения. С другой стороны, СВО являясь инструментом государственного регулирования социальной жизни страны, воспринимается населением как орган государственной власти и отношение населения к СВО имеет прямое влияние на репутацию государства и состояние национальной безопасности. В этом разрезе сохранение положительной репутации СВО очень важно в рамках внутренней безопасности государства.

Существует также дополнительное следствие - восприятие СВО населением как части государственной власти приводит к тому, что репутация государственной власти в равной степени распространяется на СВО. К примеру, если какой-либо из органов понёс репутационный ущерб и потерял определённый процент доверия населения, эта потеря скажется на всей системе государственной власти и СВО в том числе.

Такой специфичный подход к оценке ущерба СВО накладывает определённые ограничения при обосновании управляющих решений по обеспечению ИБ.

Система информационной безопасности СВО – это система с множеством взаимозависимых субъектов и объектов защиты. Она строится по принципу «периметровой защиты», пришедшему из государственной безопасности, и иерархична. При этом на каждом из уровней имеется некий пул, диапазон свобод в принятии решений. В связи с последним в регионах наблюдается очень большие девиации структуры и подходов к организации ИБ.

Неизменным остаётся следующее – для существующих систем ИБ СВО характерно «надстраивание» над общей системой работы с информацией. Отсутствие требований по информационной безопасности на этапе планирования систем обработки можно объяснить тем, что формирование СВО в том виде, в каком они существуют сейчас, и автоматизация основных процессов СВО пришлись на период нестабильности, «переходного» внутреннего состояния государства. СВО создавались на местах, руками работающих там людей и, когда пришёл этап структуризации и приведения систем СВО к текущему виду, приходилось работать с тем что есть. В настоящий момент специалистам приходится работать с устоявшимися системами, поэтому работы по управлению системой ИБ производится скорее «заплаточным» методом, чем системным с использованием процессного подхода.

Декларируемые сегодня СВО требования ИБ можно подвергнуть всевозможной критике в плане отсутствия комплексности подхода и «системы» в полном её понимании, со всеми вытекающими недостатками - недостаточно масштабируемой, не предсказуемой, не управляемой и т.п. Однако даже существующие требования не выполняется в полном объёме, как по причине отсутствия квалифицированных специалистов на местах, так и не предоставления механизмов их реализации и отсутствия внутреннего контроля.

Большие колебания осознания ИБ руководством, компетенции в области безопасности, квалификации специалистов приводят к неравномерному развитию СОИБ СВО на региональном уровне. Отстающие регионы попросту не выполняют в полной мере установленные требования, а регионы – лидеры не могут двигаться вперёд, не имея достаточно средств и полномочий. Для решения этой проблемы все

сложные функции должны быть либо автоматизированы, либо централизованы на федеральном уровне.

Элементы системы территориально удалены друг от друга и на один из первых планов выходит обеспечение доступности всех региональных и районных подразделений. Безопасность центров обработки данных (ЦОДов) – это новое направление обеспечения ИБ СВО, принципы и подходы которого коренным образом отличаются от децентрализованной обработки данных. Именно такой подход обещает сократить затраты на защиту информации, ограничить перечень вероятных угроз и уязвимостей системы защиты, снизить риски ИБ, нормализовать и структурировать систему информационной безопасности СВО.

Работа с «периметрами» подразумевает наличие разных зон и типов доступа, необходимость классификации объектов и субъектов доступа, необходимость систематизировать, отслеживать и контролировать порядок предоставления доступа к разным типам ресурсов.

В условиях очень большого разброса в подходах к организации ИБ и свободы в принятии решений на уровне регионов структура системы доступа на основе дискреционной модели становится слабо отслеживаемой, неструктурированной и неконтролируемой на федеральном уровне. Это большая системная проблема, к решению которой СВО ещё предстоит приступить. И здесь наиболее рациональным будет осуществить переход от дискреционного подхода к предоставлению доступа к ролевой модели. Основными её достоинствами являются так необходимые СВО: интегрируемость, иерархичность, универсальность, гибкость, подконтрольность и простота дальнейшего отслеживания. Недостаток использования ролевой модели – должен быть чётко определён круг предполагаемых пользователей ресурса, их должностные полномочия и обязанности. Этот недостаток превращается в достоинство тогда, когда основные функции организации регламентированы или требуют регламентации. Пример: разработка и утверждение административных регламентов на все основные государственные услуги.

Все это следствие низкоуровневого подхода к организации ИБ СВО, где целью ставится защита ресурсов, а не процесса в целом. Также отсутствует унифицированность походов и понятие «системы управления информационной безопасностью» (СУИБ). При этом управление ИБ должно быть частью корпоративного управления СВО и ориентировано на содействие достижению целей деятельности организации через обеспечение защищённости её информационной сферы.

По аналогии с работой [23] в СОИБ СВО можно выделить четыре уровня мероприятий такой безопасности. Это юридические мероприятия, административный контроль, использование физических средств защиты, применение технических (аппаратных и программных) средств. На административный контроль возлагаются функции слежения за корректностью использования защищаемых ресурсов. Могут выполняться процедуры проверки аппаратных залов – ЦОДов и серверных, самих средств автоматизации, программ, порядка доступа обслуживающего персонала, пользователей. Административный контроль может распространяться далеко за пределы центров обработки данных, затрагивая прикладные отделы, общее управление. К средствам физической защиты относят охрану, защитную сигнализацию, замки и т.п. В качестве технических средств защиты применяют специальные электронные и механические устройства, программные средства. Средства защиты в составе аппаратно-программных комплексов включают в себя защиту дисков и находящейся на них информации, аппаратуры, изменение функций штатных устройств и др.

Выделяют средства защиты с запросом информации, с помощью которых реализуются методы разграничения доступа и методы криптографической защиты.

Существуют средства активной и пассивной защиты. Активные средства инициализируются при возникновении особых обстоятельств – вводе неправильного пароля, указания неправильной даты и т.п.

Программные средства сами могут иметь собственные механизмы защиты. Для выявления и устранения последствий нарушения ИБ могут использоваться специальные программы.

В качестве основных требований, которых рекомендуется придерживаться для обеспечения ИБ на различных автоматизированных объектах, в том числе на СВО, выделяются:

1. Пользователи прежде, чем начать работать с аппаратно-программными комплексами должны идентифицировать себя.
2. Система должна иметь возможность контролировать, правомочны ли действия пользователей.
3. Над их действиями должен осуществляться мониторинг для того, чтобы можно было обнаружить неверные действия.
4. Данные, аппаратуру, программы следует защищать от физического разрушения.
5. Данные должны быть восстанавливаемыми, резервируемыми.
6. Система должна быть защищена от злоумышленников.
7. Передачи по каналам связи должны быть защищены от ошибок, при ошибках и отказах сообщения не должны пропадать, обрабатываться дважды, искажаться.
8. Передачи должны быть конфиденциальными. Некоторые из них должны быть защищены шифрованием.

Трудно оценить вклад каждого мероприятия и СОИБ в целом. Не всегда можно однозначно сказать: какой модуль не справляется, устарел или вышел за рамки общего вектора работы; насколько актуален и эффективен набор используемых защитных мер и средств; на каком этапе развития системы мы находимся сейчас; какими ресурсам обладаем и что нужно сделать для улучшения общего состояния.

Система ИБ СВО в настоящий момент занимается только решением постоянно возникающих проблем в оперативном режиме, чем занимает значительную часть рабочего времени специалиста по ИБ. Такая зацикленность на

низкоуровневом управлении инцидентами влечёт за собой принятие беспорядочных компенсационных мер, что в дальнейшем усложняет и снижает прозрачность СОИБ, ведёт к росту неоптимальных нагрузок, снижению эффективности ИБ и, в конце концов, увеличению числа инцидентов.

К поиску и принятию мероприятий по ИБ необходим системный, стратегический подход, а значит необходим контроль эффективности и принятия мер по устранению причин отклонений от запланированного результата, анализ и внесение соответствующих изменений в планировании и распределении ресурсов ИБ. Поэтому в ближайшее время актуальнейшим вопросом станет необходимость разработки и внедрения системы управления информационной безопасностью СВО, а значит и поиск подходящих для СВО инструментов оценки и обоснования управляющих решений по обеспечению ИБ.

Приемлемость для СВО тех или иных подходов к обоснованию мероприятий информационной безопасности рассмотрена в следующем параграфе.

1.4. Анализ известных методов обоснования мероприятий информационной безопасности

Поиск и обоснование мероприятий по ИБ может осуществляться для достижения следующих целей:

– приведение в соответствие требованиям регуляторов либо требованиям индустрии;

– адаптация системы ИБ к изменениям в самой организации и её окружающей среде (нехватка кадров, сокращения расходов на ИБ, реструктуризация, кризис и т.п.);

– создание/проектирование системы защиты в уже существующей инфраструктуре;

– создание/проектирование новой информационной инфраструктуры с интеграцией мер безопасности;

– устранение последствий нарушения ИБ организации (закрытие «дыр» по факту).

Мотивация в достижении тех или иных целей может исходить из разных источников в зависимости от того, кто выступает инициатором и заинтересованным лицом. Следует заметить, что практически каждый сотрудник в организации является заинтересованным лицом, при этом интересы и ожидания в отношении мероприятий ИБ у каждого разные. К примеру, для бухгалтерской службы при реализации мероприятий ИБ важно уложиться в бюджет; для подразделения информатизации – что бы их внедрение в существующую инфраструктуру прошло с минимальными кадровыми и временными затратами; для пользователей они должны быть удобными в повседневном использовании; для руководства – помимо минимизации затрат и рисков, должны облегчать или хотя бы не нагружать процесс управления, быть понятными и отслеживаемыми. В то время как регуляторы в области ИБ будут оценивать соответствие мероприятий требованиям законодательства и эти требования могут не коррелировать с ожиданиями и интересами других заинтересованных лиц. Поэтому при поиске и обосновании мероприятий ИБ необходимо подвести баланс всех интересов, об этом ниже.

Инициаторами в этой области могут выступать одно или несколько следующих лиц: специалист или руководитель подразделения ИБ, руководитель подразделения ИТ, высшее руководство, владельцы организации либо курирующая организация, в зависимости от уровня осознания потребности в системе ОИБ. Инициаторами здесь следует называть кадровые единицы, готовые потратить максимальное количество своих ресурсов на реализацию СОИБ.

Обычно во главу угла при обосновании мероприятий ИБ ставятся требования, которые предъявляются инициатором принятия решения. Но для реализации тех или иных решений «своих» ресурсов иногда не хватает. Тогда инициатор должен обращаться к обладающему соответствующими ресурсами лицу, гарантировав реализацию также и его требований при принятии решения, делая его заинтересованным лицом.

Как мы уже убедились: предъявляемые к мероприятиям по ИБ требования разнятся для каждого участника защищаемого делового процесса, в зависимости от интересов. Таким образом, кроме непосредственно защиты ресурсов и процессов от угроз, принимаемые решения в области ИБ должны выполнить ряд других задач, чтобы считаться действительно эффективными. Такой высокий уровень согласованности мер обеспечения ИБ обуславливается самой природой обеспечения ИБ. Поскольку ИБ – это состояние защищённости, а ИБ организации – это состояние защищённости всех её компонентов, то при поиске оптимальных мероприятий ИБ и определении их эффективности необходимо учитывать заведомо широкий круг факторов, либо оговаривать область, для которой рассчитывается эффективность.

С учётом этого, оценка эффективности и оптимальности решения может проводиться по разным критериям в зависимости от задач оценки, которые ставит целевая аудитория. Во-первых, оценка эффективности должна учитывать задачи и интересы аудитории, которую эти мероприятия затрагивают. Во-вторых, необходимо понять, какие цели преследует СОИБ именно для этой аудитории. В итоге необходимо показать достижение этих целей. Рассмотрим в указанных выше категориях существующие на сегодняшний день и активно использующиеся на практике и не имеющие широкой апробации методы обоснования мероприятий ИБ.

Прежде всего, следует сказать, что обоснование мероприятий ИБ входит в комплекс мероприятий по управлению СОИБ, поэтому очень часто подход к обоснованию раскрывается в стандартах и лучших практиках (англ. best practice) в области обеспечения ИБ. Обоснование мероприятий требует осуществления следующих предварительных шагов:

– идентификация ресурсов (активов);

– оценка ценности/критичности ресурса, идентификация и характеристика его уязвимостей;

– идентификация угроз нарушения безопасности ресурсов;

– оценка критичности реализации угрозы (получаемый ущерб, оценка рисков);

– идентификация (поиск) интересующих показателей эффективности (возможно на основе ценности ресурса, вероятности угрозы и критичности её выполнения, экономической эффективности);

– идентификация (поиск) контрмер, мероприятий ИБ по заданным показателям.

И поскольку первые четыре шага являются нетривиальными задачами для специалиста по ИБ и могут выполняться не только в целях обоснования мероприятий ИБ, но и для решения других вполне конкретных узких задач, для этого было разработано огромное количество подходов и методик. Согласно исследованию, именно полученные в ходе оценки угроз и оценки рисков результаты используются специалистами по ИБ при обосновании мероприятий ИБ. Рассмотрим методы идентификации активов, применяемые существующими известными подходами обоснования мероприятий ИБ.

Методика CRAMM [24] - одна из первых в ИБ методик оценки риска, где физические, программные и информационные ресурсы идентифицируются самостоятельно и классифицируются по заданной методике, строится дерево связей используемых ресурсов. Построенная модель позволяет выделить критичные элементы, соответствующие угрозам. Оценка рисков производится на количественном и качественном уровне.

Методика FRAP [25]: здесь ресурсы могут выделяться опросным путём, автоматическими средствами анализа (сканирование сети), изучения документации. Использует оценку риска, основываясь на сборе данных экспертным опросом. Оценка производится на качественном уровне (по шкале «высокий», «средний», «низкий»).

Согласно методике OCTAVE [26, 27] строят «деревья вариантов» (сочетание угрозы и ресурса), проводят практическую проверку возможности реализации этих угроз на инфраструктуре. Как результат получают уязвимости с градацией влияния на активы (нет вероятностной оценки, оценивают финансовый ущерб).

Методика RiskWatch [28, 29]: в зависимости от типа организации может автоматически выдаваться список ресурсов (активов), который необходимо

конкретизировать, а потом конкретно описать. При оценке риска использует количественную методику (риск оценивается через размер ожидаемых годовых потерь).

Согласно Information Security Forum. Standard of Good Practice (ISF – “SoGP” 2007) [30] в интересах идентификации ресурсов здесь выделяются 6 аспектов ИБ, сконцентрированных на бизнес-процессах. ISF – “SoGP” 2011 имеет модульную структуру и включает в себя серию из 118 тем, которые сгруппированы в 26 высокоуровневые области, а они в свою очередь объединяются в 4 широких категории.

Методика Microsoft [31, 32, 33]: Активами считается все, что представляет ценность для организации. К материальным активам относится физическая инфраструктура (например: центры обработки данных, серверы и имущество). К нематериальным активам относятся данные и другая ценная для организации информация, хранящаяся в цифровой форме (например: банковские транзакции, расчёты платежей, спецификации и планы разработки продуктов). В некоторых организациях может оказаться полезным определение третьего типа активов – ИТ-сервис. ИТ-сервис представляет собой сочетание материальных и нематериальных активов. Например, это может быть сервис корпоративной электронной почты. Существует также разработанная Microsoft модель угроз и методы DREAD и STRIDE, которые используются для оценки рисков.

ГОСТ ИСО/МЭК 13335-1 – 2006 [6], ГОСТ Р ИСО/МЭК ТО 13335-3 – 2007 [34], где ресурсы включают в себя (но не ограничиваются): материальные активы (например: вычислительные средства, средства связи, здания); информацию (данные) (например: документы, базы данных); программное обеспечение; способность производить продукт или предоставлять услугу; людей; нематериальные ресурсы (например: престиж фирмы, репутацию).

Следует упомянуть также существующие методики моделирования угроз и нарушителя. Все они используют различные подходы к оценке вероятности угроз, потенциалу нарушителя и результативности его воздействия, такие как: экспертные опросы, статистика, эмпирические методы (pentest, попытка взлома,

сканирование сети, проверка по показателям), оценивание потенциала нарушителя, основываясь на принципах квалиметрии и теории эффективности целенаправленных процессов, теории графов. Самый известный пример - теоретико-множественная модель защищённой системы Клементса – модель системы безопасности с полным перекрытием [35], к которой восходят большинство методик оценки риска. А также: алгоритм Digital Security [36], методика OWASP [37], Trike [38], N-Softgoal [39], GARNET [40] и другие [41, 42]. Затем, полученные в ходе оценки угроз и оценки рисков результаты в итоге используются специалистами при обосновании мероприятий ИБ.

Так, в большинстве случаев, при обосновании эффективности тех или иных мер чаще всего применяются методы экспертных оценок с применением различного математического аппарата из раздела математической статистики и статистического анализа для улучшения качества обработки результатов [43, 44, 45, 46, 47, 48, 49]. При этом предлагается использовать в качестве входных данных, в лучшем случае, показатели общемировой статистики либо статистики по отрасли. Затем, основываясь на этих данных, предлагается выстраивать собственную систему защиты, что влечёт за собой все недостатки и проблемы использования экспертных методов оценивания [50, 51, 52].

Однако, следует заметить, что даже методы, использующие хорошо адаптированные для этих целей математические инструменты оценки, такие как: теория графов, деревья атак [53, 54, 55, 56, 57, 58, 59, 60], близкие к ним когнитивное моделирование [61, 62, 63], метод анализа иерархий [64, 65, 66] и другие методы ситуационного анализа [67, 68], а также нечёткие множества, нечёткая логика и искусственные нейронные сети [69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80], теория игр [81, 82, 83], теория конечных автоматов [84, 85] и другие требуют учёта специфики формализуемой предметной области. Но все известные методы, в конечном счёте, также опираются на опыт и субъективные мнения экспертов, поскольку начальные, входные данные, используемые для моделирования и анализа чаще всего получены именно таким путём.

Рассмотрим отдельно существующие подходы, использующие математический аппарат марковских процессов [86, 87, 88, 89, 90, 91, 92, 93]. Для них также присущи указанные выше недостатки, однако есть и ряд достоинств. В первую очередь, можно говорить о том, что теоретический аппарат марковских процессов хорошо разработан, поскольку были достигнуты значительные успехи в исследовании теории марковских процессов в целом, а также были получены хорошие результаты использования метода при решении практических задач в интересующей и смежных областях. Математический аппарат обеспечивает достаточно высокую точность расчётов, позволяет исследовать моделируемый процесс на любых интервалах времени, показывает зависимости интересующих показателей от любых заданных параметров и условий и также позволяет анализировать их изменение во времени.

Кроме того, вероятности нахождения процесса в тех или иных состояниях являются аналитическими критериями оценки и не обладают недостатками статистических показателей (Росенко А.П. (2010), стр. 17-23) [91]. Существенной проблемой при этом становится отсутствие адекватных математических моделей оцениваемых систем. Разработка таких моделей является перспективных направлением исследований.

При обосновании мероприятий ИБ следует учитывать:

- требования государственных регуляторов в области ИБ [94, 95, 96, 97, 98, 99, 100, 101],

- отраслевые стандарты ИБ: Payment Card Industry Data Security Standard (PCI DSS) [102], СТО БР ИББС-1.0.-2010 [103] и соответствующая ему методика оценки соответствия: СТО БР ИББС-1.2-2009 [104],

- универсальные международные стандарты ИБ: ISO/IEC 27001 – 2006 [5] и соответствующая ему методика оценки соответствия: ISO/IEC 27004 – 2009 [105], ISO/FDIS 31000:2009(E) [106], IEC/FDIS 31010:2009(E) [107], ГОСТ ИСО/МЭК 13335-1 – 2006, ГОСТ Р ИСО/МЭК ТО 13335-3 – 2007, ГОСТ Р ИСО/МЭК 15408-3-2008, ISACA Introduction to the Business Model for Information Security [108], COBIT for Information Security [109], ISM3 [110].

- зарубежные государственные стандарты ИБ: BSI- Standard 100 - 1 [111], BSI-Standard 100 – 1 [112], NIST Special Publication 800-53 [113] [114].

Все они в той или иной мере раскрывают подходы, которыми должна руководствоваться организация при выборе мероприятий ИБ, чаще предлагают, основываясь на предложенной методике, выбрать из ограниченного списка соответствующие контрмеры, а иные и вовсе тоталитарно требуют выполнения конкретных мер. Но все стандарты по большей части основываются на предыдущем опыте и субъективном мнении экспертов. В итоге, обоснование мероприятий ИБ сводится к тому, что их выполнение обязательно в соответствии со стандартом. Тогда как построение системы ИБ СВО на основе только требований многочисленных регуляторов грозит нарушениями или затруднением деятельности СВО, увеличением нагрузки на персонал, усложнением документооборота, дублированием документации, мер и методов защиты. Использование стандартов имеет и другие недостатки: во-первых, вся специфика работы (организация бизнес-процессов, перечень и ценность ресурсов, особенности производственного цикла) обязательно должна быть учтена при разработке дизайна системы защиты, поэтому стандарт должен быть «подогнан» под конкретную организацию – а это зачастую нетривиальная задача. Отсюда исходит второй недостаток - для реализации стандарта необходимо осознание руководством такой необходимости, выделения соответствующего финансирования и высококвалифицированных специалистов, которые смогут эффективно и с пониманием внедрить требования стандарта в существующую систему. В-третьих, как показали результаты расчётов, опубликованные в работе [46], даже «подогнанный» ISO/IEC 27001 – 2006 (универсальный стандарт по ИБ для организаций любых типов, размеров, отраслей) не отражает всей картины, не охватывает уникальные для конкретной организации детали и не гарантирует адекватность и обоснованность выстроенной системы защиты.

Известны также другие экономические и математические методы решения этой задачи [115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127]. Все их можно представить в виде таблицы.

Таблица 4. Научно-методическое обеспечение в области обоснования мероприятий информационной безопасности

Подходы к обоснованию мероприятий ИБ	Публикации
Экономические подходы к обоснованию мероприятий ИБ	Методика OCTAVE – Storms A. (2003) Методика RiskWatch Ажмухамедов И.М., Ханжина Т.Б. (2011) Петренко С.А., Попов Ю.И. (2003) Обухов А.А. (2013)
Статистический анализ и экспертная оценка	Методика CRAMM - Central Computer & Telecommunications Agency (UK) (1993) Методика FRAP - Peltier (2001) Методика Microsoft - Shostack A. (2008) Трояков И.Б. (2010) Заболотский В.П., Юсупов Р.М. (2006) Молдованин Т.В. (2007) Методика OCTAVE – Alberts C., Dorofee A. (2002) Миронов В. В., Носаль И.А. (2011)
Теоретико-множественная модель защищённой системы Клементса - модель системы безопасности с полным перекрытием (дерево атак, дерево событий, дерево отказов)	Хоффман, JI.Д. (1980) Schneier B. (1999) Burgess M., Canright G., Engo-Monsen K. (2004) Alberts C., Dorofee A. (2002) Осипов В.Ю. (1996) Dewri R., Ray I., Poolsappasit N., Whitley D. (2012) Мальцев Г.Н., Теличко В.В. (2008) Абрамов Е.С., Кобилев М.А., Крамаров Л.С., Мордвин Д.В. (2014) Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р., Голембиовская О. М. (2011) Воробьев В.И. (2011, 2013) Аграновский А.В., Хади Р.А., Фомченко В.Н., Мартынов А.П., Снапков В.А.(2002) Williams L., Lippmann R. and Ingols K. (2008) Козленко А. В., Авраменко В. С., Саенко И. Б., Кий А. В. (2012) Wang L., Yao C., Singhal A., Jajodia S. (2008) Котенко Д. И., Котенко И. В., Саенко И. Б. (2012) Синещук Ю.И., Филиппов А.Г., Терехин С.Н., Николаев Д.В., Саенко И.Б. (2011)
Метод анализа иерархий	Куземко С. М., Мельничук В. М. (2010) Бикмаева Е.В., Баженов Р.И. (2014) Чусавитин М.О. (2013)
Методы с использованием нечётких множеств, нечёткой логика и искусственных нейронных сетей	Круглов В. В. Дли М. И. Голунов Р. Ю. (2001) Васильев В.И., Савина И.А., Шарипова И.И. (2008) Sodiya A. S., Onashoga S. A., Oladunjoye B. A.(2007) Чечулин А.А. (2013) Ingle M., Atique M., Dahad S. O.(2011) Маслобоев А.В. Путилов В.А.(2010) Котенко И. В., Уланов А. В. (2006) Файзуллин Р. Р., Васильев В. И. (2013) Shang K. Hossen Z. (2013) Sun L., Srivastava R.P., Mock T.J. (2006)

	Котенко И.В., Шоров А.В., Нестерук Ф.Г. (2011)
Теория игр	Вахний Т.В. Гуц А.К.(2009) Арьков П.А. (2008) Белый А.Ф.(2008)
Теория марковских процессов	Ерохин С.С. Голубев С.В.(2007) Росенко А.П. (2009, 2010) Иванов К.В. Тутубалин П.И. (2012) Осипов В.Ю., Ильин А.П., Фролов В.П., Кондратюк А.П. (2006) Попов С.В., Шамкин В.Н. (2012) Каштанов В.А., Зайцева О.Б.(2013) Осипов В.Ю. (2013)
Ситуационный анализ и когнитивное моделирование	Борзенкова С.Ю., Чечуга О.В., Наседкин М.Н., Селищев В.А. (2010) Воробьев В.И., Монахова Т.В. (2005) Борзенкова С.Ю., Чечуга О.В.(2013) Данилюк С.Г. Маслов В.Г.(2008) Кудрявцева Р.Т. (2008) Рытов М.Ю., Рудановский М.В. (2010) Ажмухамедов И.М. (2010)
Теория конечных автоматов	Шлыков Г.Н. (2011) Меньших В. В., Петрова Е.В. (2010)
Требования государственных регуляторов в области ИБ	Приказ ФСТЭК России от 11 февраля 2013 г. N 17 Приказ ФСТЭК России от 18.02.2013 г. N 21 Методические рекомендации ФСБ России от 21.02. 2008 № 149/54-144 Методика определения актуальных угроз безопасности ФСТЭК России от 14.02.2008 и т.д.
Отраслевые стандарты по ИБ	СТО БР ИББС-1.0.-2010 СТО БР ИББС-1.2-2009 PCI DSS
Международные стандарты по ИБ	Information Security Forum. Standard of Good Practice. ГОСТ ИСО/МЭК 13335-1 – 2006 ГОСТ Р ИСО/МЭК ТО 13335-3 – 2007 ISO/IEC 27001 – 2006 ISO/IEC 27004 – 2009 ISO/FDIS 31000:2009(E) - IEC/FDIS 31010:2009(E) BSI- Standard 100 – 1 (2008) BSI- Standard 100 – 3 (2008) COBIT for Information Security (2015) NIST Special Publication 800-53 (2013)

Однако во всех этих работах не в полной мере учитывается ряд особенностей, свойственных реальным процессам обеспечения ИБ СВО, в том числе связанных с многократностью проводимых мероприятий, с изменением внешних и внутренних условий, целей защиты информации. Несовершенны также методы анализа программ деструктивного воздействия с циклами. В каждом конкретном случае необходимо рассматривать свои модели ИБ СВО. Не во всех случаях при

обосновании мероприятий по защите можно обойтись одним и тем же основным показателем эффективности. Условия его расчёта так же могут существенно отличаться.

Главный недостаток многих известных методов в том, что область их использования ограничена и распространяется либо на противодействие именно техническим и сетевым атакам, либо основывается исключительно на оценке экономической эффективности мероприятий. В первом случае – большинство методов исходит из того, что объектом защиты является информационная система, не рассматривается безопасность всего объекта информатизации, непрерывность деловых процессов, не учитываются интересы владельцев бизнеса и информации. Во втором случае не учитывается широкий ряд других важных параметров, о которых говорилось ранее – удобство для пользователей, интегрируемость в текущую инфраструктуру, контролируемость и т.п. Выстраиваемая таким образом СОИБ не обладает требуемыми свойствами: системность, интегрируемость, комплексность, прозрачность, адекватность, оптимальность и подконтрольность.

Поэтому необходимо совершенствование соответствующего научно-методического аппарата. И решение задачи разработки новых эффективных методов обоснования целесообразности принятия решений и мероприятий ИБ, учитывающих все особенности объекта защиты, его деловых процессов, внешней и внутренней среды функционирования, позволит повысить уровень информационной безопасности СВО в целом.

1.5. Постановка задачи

Анализ исследуемого процесса и существующих методов обоснования мероприятий ИБ позволяет утверждать о необходимости совершенствования процесса управления ИБ СВО. Требуется поиск новых подходов к обоснованию мероприятий по обеспечению ИБ СВО. От успешности такого обоснования во многом зависят как расходы на обеспечение ИБ, так и потери от её нарушения. Не эффективные (излишние) мероприятия по защите информации в общем случае

повлекут дополнительные временные и материальные расходы. При недооценке необходимости тех или иных мер велика вероятность нарушения ИБ, возможны потери ценности ЗИР. Для обоснования мероприятий ИБ СВО нужны соответствующие модели и методы. Как отмечено в п. 1.4 известные методы и подходы не в полной мере применимы для целей ИБ СВО, поскольку эти методы не учитывают ряд особенностей, свойственных реальным процессам обеспечения ИБ СВО, в том числе связанных с многократностью проводимых мероприятий, с изменением внешних и внутренних условий, несоответствием целям и объектам защиты.

Необходимо решить научно-техническую задачу по разработке новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, повышающих уровень их ИБ.

В качестве исходных данных о СВО и их системах ИБ в общем случае могут быть известны:

– реализуемые цели и решаемые задачи;

– обрабатываемые и защищаемые информационные ресурсы;

– физические и логические структуры;

– алгоритмы функционирования;

– возможные каналы нарушения ИБ (уязвимости);

– реализуемые элементами системы функции, мероприятия, в том числе ИБ;

– возможности элементов по реализации этих функций;

– исходные и конечные состояния;

– внешние условия.

Исходными данными о злоумышленниках могут выступать:

– преследуемые цели и решаемые задачи;

– уровень мотивации;

– сведения о наличии необходимого оборудования, информационного и программного обеспечения для нарушения ИБ;

– каналы НСД, которыми злоумышленники могут воспользоваться;

– типовые функции, реализуемые злоумышленниками;

– возможные временные и материальные затраты на нарушение ИБ и другие.

Новый подход к управлению ИБ должен учитывать циклическую модель управления Шухарта-Деминга, являющегося стандартом в области обеспечения ИБ [5]. Это позволит использовать метод на разных уровнях проекции, и в качестве объекта защиты рассматривать всю организацию в целом, а не только её информационную систему, может встраиваться в существующие деловые процессы организации, учитывать спектр интересов всех заинтересованных лиц. Выстраиваемая таким образом СОИБ обладает всеми требуемыми свойствами: системность, интегрируемость, комплексность, прозрачность, адекватность, оптимальность и подконтрольность.

Для решения сформулированной научно-технической задачи в ходе выполнения диссертационных исследований необходимо провести:

– анализ известных структур систем и мероприятий ИБ СВО, выявление критичных ресурсов и существующих угроз ИБ СВО;

– анализ существующих методов обоснования мероприятий ИБ и применимость их для целей ИБ СВО;

– разработку метода управления СОИБ СВО на основе комплекса оптимизационных моделей, включая метод определения начальных состояний процессов;

– поиск возможных оптимизационных моделей обоснования мероприятий ИБ СВО;

– разработку модели функционирования СВО;

– разработку моделей основных защищаемых деловых процессов ИБ СВО;

– разработку моделей основных процессов нарушения ИБ СВО;

– апробацию предложенных методов и моделей применительно к структурам ПФР;

– обоснование состава пакета прикладных программ для специалиста, отвечающего за ИБ на СВО;

– выработку методических рекомендаций по использованию предложенных моделей, методов и программных средств;

– выработку практических рекомендации по совершенствованию организации информационной безопасности социально-важных объектов.

При моделировании деловых процессов и процессов нарушения ИБ СВО предлагается рассмотреть их как марковские, что позволит использовать соответствующий математический аппарат: составить графы состояний и соответствующие им системы дифференциальных уравнений, описывающие анализируемый процесс, и решать их, получая искомые вероятности нахождения процесса в каждом из состояний. В итоге можно рассчитать по заданным данным любые интересующие параметры.

Использование теории марковских процессов в моделировании различных бизнес-процессов не ново, однако следует отметить, что ранее деловые процессы таких объектов так подробно ещё не изучались и в существующей литературе не было обнаружено каких-либо материалов, касающихся формализации деловых процессов СВО. Кроме того, составленные модели должны иметь прикладной характер, учитывать многократность санкционированного и несанкционированного доступа к ЗИР, возможность пересмотра мероприятий защиты, а также блокирования доступа в случаях нарушения ИБ, благодаря чему можно будет изучать систему в различных условиях и осуществлять поиск наиболее оптимальных вариантов реализации мероприятий ИБ.

Разработка типовых оптимизационных моделей позволит значительно повысить скорость поиска альтернативных мероприятий ИБ и скорость принятия решений. Эти модели должны быть ориентированы на широкий круг возможных ситуаций обеспечения ИБ, учитывать ценности ЗИР и потенциальной информированности злоумышленников на текущий момент времени.

Выводы по первой главе

В настоящей главе проведён анализ известных структур систем и мероприятий ИБ СВО, по результатам которого были обнаружены критические места и направления, требующие наибольшего внимания.

Выявлены наиболее критичные защищаемые ресурсы, процессы и угрозы ИБ СВО, на основании которых в дальнейшем могут быть выделены основные защищаемые деловые процессы СВО и типовые процессы нарушения ИБ СВО.

Анализ существующих методов обоснования мероприятий ИБ показал, что в этих работах не учитывается ряд особенностей, свойственных реальным процессам обеспечения ИБ и ИБ СВО в частности, в том числе связанных с многократностью проводимых мероприятий, с изменением внешних и внутренних условий, целей защиты информации.

Главный недостаток многих известных методов заключается в том, что область их использования ограничена и распространяется либо на противодействие именно техническим и сетевым атакам, либо основывается исключительно на оценке экономической эффективности мероприятий. Выстраиваемая таким образом система обеспечения ИБ не обладает требуемыми свойствами, а значит существующие методы неприменимы для целей ИБ СВО. Сформулирована научно-техническая задача диссертационного исследования: разработка новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, повышающих уровень их ИБ.

2. МЕТОДЫ ОБОСНОВАНИЯ ЦЕЛЕСООБРАЗНЫХ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО-ВАЖНЫХ ОБЪЕКТОВ

2.1. Метод управления информационной безопасностью социально-важных объектов на основе комплекса оптимизационных моделей

События, возникающие в деловых процессах, имеют массовый и случайный характер. Часто они обладают свойством статистической устойчивости, что позволяет использовать в процессе принятия решений эффективные математические методы теории случайных процессов и, в частности, одного из её разделов - теории марковских процессов. Опираясь на предельную теорему теории вероятностей для потоков событий, в большинстве случаев, защищаемый процесс можно рассмотреть как марковский, где дугам графа могут быть поставлены в соответствие интенсивности переходов из состояния в состояние. Опираясь на это положение, а также на результаты более ранних исследований [128], предлагается новый метод управления информационной безопасностью СВО на основе комплекса оптимизационных моделей. В обобщённом виде его можно представить в виде следующей последовательности шагов (рисунок 2). Цикличность этого алгоритма объясняется цикличной природой управления ИБ. Дело в том, что системы защиты информации гарантируют безопасность защищаемого объекта только на определённом промежутке времени, к примеру, пока не разработаны новые системы и методы обхода этой защиты. Потому главным принципом обеспечения ИБ является непрерывность пересмотра мероприятий по защите, что и отражено в представленном методе.

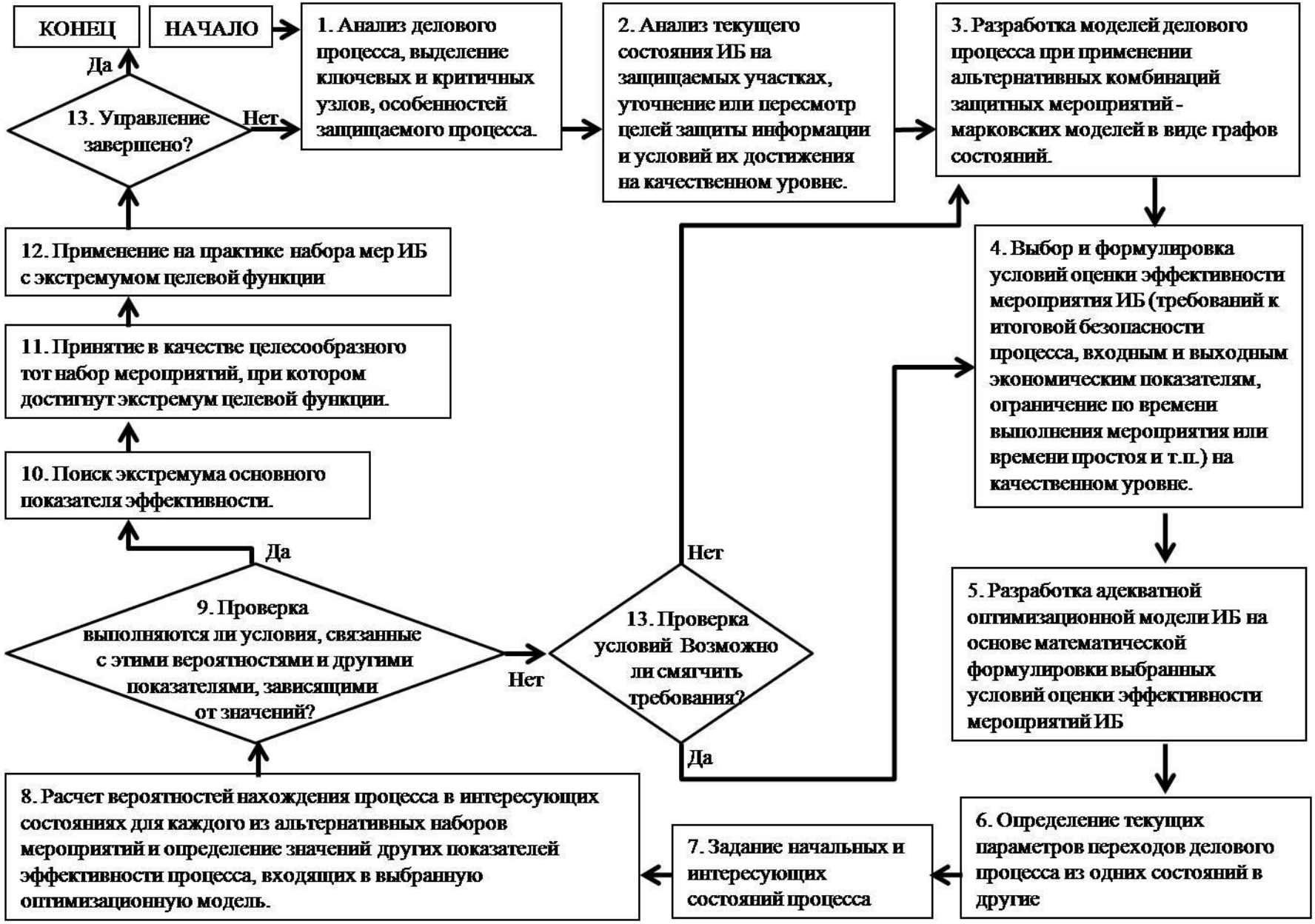


Рисунок 2 – Метод управления ИБ СВО

Кроме того, в настоящем алгоритме присутствует несколько условных операторов, смысл которых заключается в проверке выбранных альтернативных мероприятий ИБ на соответствие условиям эффективности. В случае, когда ни одно из предложенных к проверке мероприятий не удовлетворяет условиям эффективности, имеет смысл либо пересмотреть адекватность выбранных условий эффективности, либо осуществить поиск альтернативных мероприятий ИБ.

Далее рассмотрим основные рекомендации по использованию представленного метода. При разработке модели защищаемого делового процесса с учётом мероприятий ИБ в виде графа состояний следует исходить из целесообразного уровня формализации. Излишняя детализация влечёт за собой повышение затрат на разработку модели процесса и определение её параметров. Грубая формализация позволяет оперативно получать интересующие оценки, однако не обеспечивает необходимой точности результатов.

Что бы построить такой граф, в соответствии с предлагаемым алгоритмом, следует, прежде всего, определиться с уровнем масштабирования модели, интересующими результатами и изучить объект моделирования – защищаемый деловой процесс, затем выделить:

- основные этапы его выполнения;
- задействованные ресурсы;
- определить есть ли в процессе стандартные ответвления, связанные с принятием решений;
- какие могут быть ошибки, сбои в выполнении процесса;
- какие атаки на процесс актуальны, и к каким последствиям (нарушениям) на каких этапах могут привести;
- какие из нарушений связаны с защищаемыми ресурсами, какие с нарушениями требований, какие с человеческими ошибками.

На основании указанных выше данных могут быть выделены последовательности состояний, в которых может находиться процесс, и возможные переходы между ними. Следует уделить построению графа состояний наибольшее внимание, поскольку именно этим выбором будет определяться область получаемых результатов и характер возможных выходных данных.

В качестве условий оценки эффективности мероприятий ИБ могут выступать: требования к итоговой безопасности процесса, входным и выходным данным, экономическим показателям, ограничение по времени выполнения мероприятия или времени простоя и другие.

Следующим важным моментом является задание исходных данных, условий поиска и искомых/требуемых результатов (план задачи и целевая функция). Одновременно в качестве них могут выступать следующие параметры:

- наличие тех или иных связей и переходов из состояния в состояние;
- интенсивности переходов из состояния в состояние;
- вероятности нахождения в том или ином состоянии;
- начального времени (состояния);
- конечного времени;
- затраты на реализацию защиты;
- ущерб от реализации угрозы.

Интенсивности переходов из состояния в состояние и ограничение по времени ($t_{конеч.}$) могут задаваться основываясь на:

- регламенте моделируемого делового процесса;
- статистических данных;
- требуемых (заданных по техническому заданию) показателям.

Поскольку деловые процессы СВО зачастую жёстко регламентированы, в том числе по времени, то для большинства переходов значения интенсивности фиксированы и являются обязательной частью процесса. Но некоторые из интенсивностей переходов зависят от вероятностей реализации той или иной угрозы и от особенностей мероприятий ИБ (к примеру, от частоты проведения проверок). Эта неопределённость может быть исключена в ходе разработки оптимизационных моделей ИБ, поскольку эти интенсивности становятся искомыми параметрами, в другом случае, они могут быть определены путём сбора и обработки статистических данных. В ряде случаев, когда известны начальные и конечные состояния процесса на некотором интервале времени, то определение

исходных интенсивностей осуществимо также путём подбора параметров с использованием метода наименьших квадратов.

Важным моментом моделирования является распознавание состояний, в которых система может находиться на исходный момент времени и зависит от того, какой результат требуется получить, и на каком узле процесса следует сфокусировать внимание.

В случае, когда процесс, протекающий в физической системе со счётным множеством состояний и непрерывным временем, является марковским, можно описать этот процесс с помощью обыкновенных дифференциальных уравнений, в которых неизвестными функциями являются вероятности состояний. Таким образом, для расчёта вероятностей нахождения процесса в интересующих состояниях составляется система линейных дифференциальных уравнений, называемых уравнениями Колмогорова, и разрешается относительно заданных начальных и интересующих состояний.

В соответствии с этим алгоритмом выбор конкретной оптимизационной модели должен осуществляться, исходя из наибольшего соответствия её реальной ситуации с учётом возможностей и неопределённостей.

Особенность представленного метода заключена в комбинации использования циклической модели управления Шухарта-Деминга, являющегося стандартом в области обеспечения ИБ [5], математического аппарата марковских процессов, теории дифференциальных уравнений применительно к задаче управления информационной безопасностью СВО.

Представленный метод подразумевает разработку моделей защищаемых деловых процессов СВО, а также оптимизационных моделей оценки эффективности. В типовых случаях метод предлагает использовать уже готовые разработанные модели (не требуется глубоких знаний и временных затрат), что позволяет значительно повысить скорость поиска альтернативных мероприятий ИБ и скорость принятия решений.

2.2. Оптимизационные модели мероприятий информационной безопасности

В рамках предложенного метода (п. 2.1) рекомендуется находить целесообразный период пересмотра мероприятий ИБ. Учитывая особенности ИБ СВО и результаты предыдущих глав, основываясь на противоречиях между уровнем защищённости и доступности информационных ресурсов – государственных услуг, уровнем защищённости и затратами на обеспечение ИБ, затратами на обеспечение ИБ и возможным информационным ущербом со стороны несанкционированных пользователей, приведём оптимизационные модели, в соответствии с которыми предлагается осуществлять обоснование оптимального периода пересмотра мероприятий (ППМ) ИБ [128].

Модель 1. В случаях, когда требуется найти этот период Δt_o, при котором на интервале времени T достигается минимум интегральных потерь $S_o(\Delta t_o,T)$, рекомендуется решать задачу:

$$S_o(\Delta t_o, T) = \min_{k \in Q} \int_0^T L_k(\Delta t_k, t)dt, \quad (1)$$

$$L_k(\Delta t_k, t) = B_k(\Delta t_k, t) + V(t) * P_{H_k}(\Delta t_k, t), \quad (2)$$

$$P_{C_k}(\Delta t_k, T) \leq P_{\text{зад.}} \quad (3)$$

$$P_{H_k}(\Delta t_k, T) \leq P_{\text{доп.}}, \quad (4)$$

$$k = 1, 2, \ldots, K.$$

В модели (1) - (4) приняты обозначения: Q -область допустимых периодов пересмотра мероприятий по защите информации; $L_k(\Delta t_k,t)$ - суммарные потери при k-м значении периода Δt_k пересмотра мероприятий на момент времени t; $B_k(\Delta t_k,t)$ - суммарные затраты на защиту информации при k-м значении периода; $V(t)$ - ценность защищаемых информационных ресурсов; K — число возможных значений периода пересмотра мероприятий ИБ; $P_{H_k}(\Delta t_k, T)$ – вероятность реализации угрозы нарушения процесса при k-м значении периода пересмотра мероприятий ИБ на момент T; $P_{\text{доп.}}$ - допустимое значение для вероятности нарушения процесса.

Суммарные затраты на защиту информации и ценность защищаемых информационных ресурсов в (2) могут выражаться в виде функций от времени, как

$$B_k(\Delta t_k, t) = b_{0_k} + a * \frac{t}{\Delta t_k}, \quad (5)$$

$$V(t) = V_0 \cdot \exp(-\gamma \cdot t), \quad (6)$$

где a, γ, V_0 – константы; b_{0_k} – суммарные затраты на $t = 0$, в частном случае они могут не зависеть от Δt_k. В результате вместо (2) имеем:

$$L_k(\Delta t_k, t) = b_{0_k} + a * \frac{t}{\Delta t_k} + V_0 * exp(-\gamma * t) * P_{H_k}(\Delta t_k, t). \quad (7)$$

Из (5) следует, чем меньше Δt_k, тем больше затраты. Выражение (6) отражает эффект устаревания информации во времени без учёта НСД. Величину V_0 можно определить с использованием известного подхода [131]. В частном случае она равна минимуму затрат на восстановление утраченной информации, если нет других последствий. Особенность этой модели в том, что она учитывает: как затраты на реализацию мероприятий по защите информации, так и возможный информационный ущерб от нарушения информационной безопасности. Кроме этого интеграция возможных потерь осуществляется по времени.

И ещё один важный фактор – вероятный ущерб от реализации угрозы нарушения защищаемого процесса должен быть значительным, чтобы оправдывать затраты на мероприятия по защите. Тогда имеет смысл сравнить интегральные потери от реализации угрозы с суммарными затратами на её защиту. По их разнице можно судить об эффективности системы защиты.

Модель 2. Когда интерес представляет минимум суммарных потерь на конкретный момент времени T, при ограничениях на вероятность реализации угрозы и на время реакции системы защиты в чрезвычайных ситуациях, поиск Δt_o можно осуществлять с использованием модели:

$$L_o(\Delta t_o, T) = \min_{k \in Q} L_k(\Delta t_k, T), \quad (8)$$

$$P_{H_k}(\Delta t_k, T) \le P_{\text{доп.}}, \quad (9)$$

$$T_{б_k} \le T_{\text{доп.}}, \quad (10)$$

$$k = 1, 2, \ldots, K.$$

Здесь $T_{б_k}$ - время реакции системы защиты при k-м периоде пересмотра мероприятий защиты; $T_{доп.}$ - допустимое время реакции системы защиты. Другие обозначения такие же, как и в (1) - (4). Заметим, что при решении задачи (8) - (10) в частных случаях можно ограничиться только потерями в виде возможного информационного ущерба (второе слагаемое в правой части выражения (2)).

Модель 3. В ситуации, когда требуется найти Δt_o, исходя из максимума оставшейся ценности защищаемой информации на конкретный момент времени T при ограниченных суммарных затратах на её защиту, с учётом (5), (6) применима модель:

$$V_{opt}(\Delta t_0, T) = \max_{k \in Q} V_0 * exp(-\gamma * T) * (1 - P_{H_k}(\Delta t_k, T)), \quad (11)$$

$$B_k(\Delta t_k, T) = b_{0_k} + a * \frac{T}{\Delta t_k} \leq B_{\text{зад.}}. \quad (12)$$

Модель 4. Когда предоставляется возможность иметь интегральные потери, не превышающие допустимых $S_{доп..}$, а наибольший интерес представляет минимизация вероятности нарушения процесса, для определения Δt_o предлагается использовать модель:

$$P_{H_0}(\Delta t_0, T) = \min_{k \in Q} P_{H_k}(\Delta t_k, T), \quad (13)$$

$$\int_0^T L_k(\Delta t_k, t)dt \leq S_{\text{доп}}, \quad (14)$$

$$\text{k} = 1, 2, ..., \text{K}.$$

Специфика модели (13) – (14) состоит в расчёте основного показателя и в проверке условия (1414). Причём основу интегральных потерь в ней составляют, прежде всего, суммарные затраты на защиту информации (первое слагаемое в выражении (2)). Что касается второго слагаемого в $L_k(\Delta t_k, t)$, то при минимизации вероятности нарушения процесса одновременно минимизируются возможные потери ценности этих ресурсов.

Модель 5. В ситуации, когда трудно определить суммарные или частные потери, связанные с защитой информации, для поиска Δt_o можно использовать модель:

$$\Delta t_o = \max_{k \in Q} \Delta t_k, \tag{15}$$

$$P_{H_k}(\Delta t_k, T) \leq P_{\text{доп.}}, \tag{16}$$

$$k = 1, 2, \ldots, K.$$

В соответствии с (15) - (16) ищется наибольший период пересмотра мероприятий по защите информации, при котором вероятность нарушения процесса на момент T не превышает допустимого значения, $P_{доп.}$. В этой модели максимизация периода пересмотра мероприятий, в какой-то мере равносильна минимизации текущих расходов на защиту информации.

Модель 6. Вычислить Δt_o, при котором обеспечивается максимальная разница $W_0(\Delta t_k, T)$ между ущербом от реализации угрозы $V(T) * P_{H_k}(\Delta t_k, T)$ и затратами на мероприятия ИБ $B_k(\Delta t_k, T)$.

$$W_0 = (\Delta t_k, T) = max\, W_k(\Delta t_k, T), \tag{17}$$

$$W_k(\Delta t_k, T) = V(T) * P_{k_н}(\Delta t_k, T) - B_k(\Delta t_k, T), \tag{18}$$

$$P_{H_k}(\Delta t_k, T) \leq P_{\text{доп.}}, \tag{19}$$

$$k = 1, 2, \ldots, K.$$

Кроме приведённых моделей возможны также и другие варианты, учитывающие при поиске целесообразного ППМ по защите информации ограничения на время восстановления защищаемого процесса и другие условия, от которых зависят вероятность реализации угрозы и вероятный ущерб. А также все приведённые выше модели могут быть переформулированы, таким образом, чтобы оптимальность мероприятий оценивалась по экстремуму показателей зависимости от потребностей решаемых задач.

Предлагается для примера также обосновать наиболее эффективный набор прав доступа. Оптимизационная модель, в соответствии с которой предлагается осуществлять обоснование может выглядеть следующим образом:

Модель 7. Обеспечить минимальную вероятность нарушения процесса, вероятность корректного завершения процесса не ниже заданного значения и период проверки не выше допустимого на заданном интервале времени T. В

зависимости от особенностей защищаемого процесса в других случаях она может быть переформулирована.

Таким образом, оценку эффективности выданных прав доступа рекомендуется осуществлять согласно модели:

$$P_H\ (T) = \min_{k \in Q} P_{H_k}(T), \tag{20}$$

$$P_{K_k}\ (T) \geq\ P_{\text{зад.}}, \tag{21}$$

$$T_{\text{пров.}}(T)\ \leq\ T_{\text{доп.}}, \tag{22}$$

$$k=1,2, \ldots, K.$$

В модели (20) - (22) приняты обозначения: k – число сравниваемых вариантов прав доступа, $\mathrm{P_{H_k}(T)}$ – вероятность нарушения процесса при k-том варианте доступа на момент времени T, $\mathrm{P_{K_k}(T)}$ – вероятность того корректного завершения процесса; $P_{зад.}$ – заданная нижняя граница вероятности корректного завершения процесса; $T_{пров.}(T)$ – период проверки; $T_{доп..}$ – допустимый период проверки.

Кроме приведённых моделей возможны также и другие варианты, учитывающие более широкий круг условий или комбинирующие уже приведённые выше условия в необходимых сочетания для достижения максимального приближения к поставленной задаче.

Предложенный комплекс оптимизационных моделей обоснования мероприятий ИБ СВО при необходимости позволяет включать в оценку оптимальности мероприятий по ИБ такие параметры как: период проверки, период пересмотра мероприятий по защите, предполагаемый ущерб, остаточная ценность, ресурсы, затрачиваемые на восстановление, ресурсы, затрачиваемые на мероприятия по ИБ, вероятность нарушения ИБ процессов, удобство для пользователей, интегрируемость в текущую инфраструктуру, контролируемость и т.п.

Системообразующим ядром всех этих оптимизационных моделей выступают модели процесса ИБ в виде графов состояний (Гл. 3).

2.3. Метод обоснования мероприятий информационной безопасности по критерию минимума интегральных потерь на заданном интервале времени

В интересах оценки интегральных потерь при обеспечении ИБ необходимо оценивать ценность защищаемых информационных ресурсов (ЗИР) СВО в зависимости от времени. Ресурс имеет высокую ценность для СВО в случае, когда его использование позволяет получить эффект, покрывающий расходы на добывание и содержание ресурса и превышающий эффект системы без этого ресурса. Второй вариант – затраты на получение эффекта с использованием ресурса должны быть настолько малы, что вместе с расходами на добывание и содержание ресурса должны быть ниже расходов на достижение такого же эффекта без этого ресурса. В экономике оценка любых активов, в том числе и нематериальных, заключается в последовательном применении трёх стандартных подходов – доходного, затратного, сравнительного, затем на основании полученных данных аудитор выводит итоговый результат [129]. Опираясь на более ранние работы [131, 130], определим ценность ЗИР как:

$$V = W - (C_1 + C_2 + C_3), \quad (23)$$

где W – доходы (получаемый эффект), C_1 – расходы на достижение этих эффектов, C_2 – расходы на содержание ресурса, C_3 – расходы на добывание ресурса, V – чистый доход.

Следует отметить, что формула, используемая для оценки ценности ЗИР в работе [131] учитывает доходный, затратный и сравнительный подход одновременно. Эффект, получаемый организацией при наличии и отсутствии ЗИР, «чистая прибыль», которую приносят те или иные нематериальны ресурсы. Если подключить сравнительный метод и учитывать, что все показатели должны рассматриваться с учётом влияния фактора времени, поскольку он является основополагающим при определении ценности информационных ресурсов, а также учитывая то, что информация может использоваться одновременно в разных информационных системах организации для обеспечения сразу нескольких деловых процессов, то ценность ЗИР следует определить как:

$$V(t) = V_2(t) - V_1(t), \qquad (24)$$

здесь $V_2(t)$, $V_1(t)$ – конечные эффекты на момент времени *t*, пересчитанные к входу системы – санкционированного потребителя, при наличии и отсутствии указанного ЗИР соответственно. Перерасчёт конечных эффектов к входу предусматривает в нашем случае вычитание из них затраченных материальных и других ресурсов на получение интересующей информации. При этом предполагается, что потребитель использует полученную информацию оптимальным способом. Потребителем, в частном случае, может выступать сама система – обладатель ЗИР.

В соответствии с этими исходными посылками и учитывая то, что информация может использоваться одновременно для достижения разных целей, конечные эффекты $V_1(t)$, $V_2(t)$ согласно [131] могут быть представлены следующей аналитической зависимостью:

$$V_{1(2)}(t) = \max_{i(j)\in I(J)} \left\{ W_{1(2)i(j)}(t) - \sum_{r=1}^{N} a_r \cdot C_{1(2)r_{i(j)}}(t) \right\}, \qquad (25)$$

где $W_{1i}(t)$, $W_{2j}(t)$ эффекты, получаемые потребителем на момент времени *t* при достижении одних и тех же целей без интересующих ЗИР и при их наличии, соответственно; *t* – время жизни ресурса; *I*, *J* – множества всех возможных способов получения конечных эффектов в первом и втором случаях; $C_{1r_{i(j)}}(t)$, $C_{2r_{i(j)}}(t)$ - расходы *r*-го ресурса потребителя информации на достижение, соответственно, результатов $W_{1i}(t)$, $W_{2j}(t)$; a_r – коэффициент приведения расхода *r*-го ресурса потребителя к единицам измерения конечных эффектов; *N* – число видов ресурсов потребителя, которые он может расходовать на получение и использование ЗИР.

Если выделить среди всех затраченных ресурсов на достижение эффекта $V_2(t)$ ресурсы, которые израсходованы на получение и содержание использованных ЗИР (на их разработку, покупку, восстановление, добывание), тогда

$$\sum_{r=1}^{N} a_r \cdot C_{2rj}(t) = \sum_{r=1}^{N} a_r \cdot C_{2.1\,rj}(t) + \sum_{r=1}^{N} a_r \cdot C_{2.2rj}(t) + \sum_{r=1}^{N} a_r \cdot C_{2.3rj}(t)\,. \qquad (26)$$

Первое слагаемое в правой части выражения (26) соответствует затратам ресурсов на достижение эффекта $W_{2j}(t)$ при условии, что необходимые ЗИР в наличии, а второе на получение ЗИР и их дальнейшее содержание. С учётом (31), (32) ценность $V(t)$ ЗИР можно определить согласно формуле как:

$$V(t) = \max_{j \in J} \min_{i \in I} \left\{ W_{2j}(t) - W_{1i}(t) - \sum_{r=1}^{N} a_r \cdot (C_{2.1\,rj}(t) - C_{1r_i}(t)) - \right.$$
$$\left. - \sum_{r=1}^{N} a_r \cdot C_{2.2\,rj}(t) - \sum_{r=1}^{N} a_r \cdot C_{2.3\,rj}(t) \right\} . \quad (27)$$

Проанализируем это выражение. В условиях, когда разница между затратами ресурсов на достижение $W_{1i}(t)$, $W_{2j}(t)$ сводится к затратам на приобретение и содержание ЗИР, то есть:

$$\sum_{r=1}^{N} a_r \cdot \left(C_{2.1rj}(t) - C_{1ri}(t) \right) = 0. \quad (28)$$

Тогда, если содержание ЗИР ничего не стоит, их ценность относительно потребителя равна:

$$V(t) = \max_{j \in J} \min_{i \in I} \left\{ W_{2j}(t) - W_{1i}(t) - \sum_{r=1}^{N} a_r \cdot C_{2.3\,rj}(t) \right\}. \quad (29)$$

Снижение ценности $V(t)$ ЗИР для потребителя возможно, например, за счёт искажения или внедрения в них ложных данных или раскрытия конфиденциальности. В ситуации, когда можно успешно восстановить утраченные ЗИР до момента их использования, ценность ЗИР определяется как минимум затрат на их восстановление:

$$V(t) = \min_{i \in I} \sum_{r=1}^{N} a_r \cdot C_{2.3\,rj}(t). \quad (30)$$

Таким образом, в самом простом случае ценность защищаемых информационных ресурсов можно оценивать согласно (30), а при учёте отдалённых последствий – по формуле (27) или (29).

Действуя в соответствии с алгоритмом, изложенным в предыдущем параграфе, рассмотрим частный случай обоснования мероприятий ИБ СВО, в ситуации, где в качестве основного условия эффективности принимается минимум суммарных потерь после реализации набора мероприятии. Под суммарными потерями понимаются затраты на реализацию мероприятий и вероятный ущерб после их реализации.

Разработаем частную оптимизационную модель для такого обоснования. Суммарные затраты $B_k(M_k,t)$ на реализацию комплекса M_k мероприятий ИБ могут складываться из стоимости приобретаемых и устанавливаемых средств защиты, затрат на управление ими и восстановление ЗИР. Определение их может осуществляться простым суммированием затрат на реализацию отдельных мероприятий.

Вероятный ущерб можно оценить, только вычислив возможные деструктивные воздействия на защищаемые ресурсы, вероятность, силу и последствия каждого из них. Для чего на этапе анализа защищаемого процесса и текущего состояния ИБ следует воспользоваться методом синтеза потенциально возможных деструктивных программ. Алгоритм такого синтеза в интересах обоснования комплексов мероприятий ИБ предложен в работе [131]. Он учитывает результаты потенциальной осведомлённости о системе ИБ возможных злоумышленников и интересующих их результатов (целей). Для каждого анализируемого комплекса мероприятий ИБ предлагается задавать вектор исходных данных $\overline{DB}$ и вектор интересующих результатов (целей) $\overline{DW}$, такой что:

$$\overline{DB} = (\overline{DB_1}, \overline{DB_2}, \overline{DB_3}, \dots, \overline{DB_N}), \quad (31)$$

$$\overline{DW} = (\overline{DW_1}, \overline{DW_2}, \overline{DW_3}, \dots, \overline{DW_M}), \quad (32)$$

где N и M – конечное количество исходных данных и целей. А также задаются условия, связывающие исходное состояние с конечным:

$$F_{zv}(d_{zv\_e};\ e = 1, 2,.., E_z) \rightarrow d_{zv\_a}, \quad (33)$$

$$z = 1, 2,.., Z, \quad (34)$$

$$v = 1, 2,.., V_z, \quad (35)$$

В (33-35) могут входить, например, функции получения доступа к ресурсам сервера с преодолением средств защиты, открытия защищаемых файлов, копирования, изменения параметров средств защиты для облегчения последующего доступа и др. При выполнении этих функций могут участвовать как аппаратно-программные средства, так и злоумышленник. Каждой из них ставятся в соответствие временные затраты на их реализацию. Если за конечное число шагов, исходя из $\overline{DB}$ может быть достигнут конечный результат $\overline{DW}$, то такая программа называется результативной.

Синтез программ на заданном множестве условий предлагается осуществлять исходя из стремления найти программу с наибольшим числом интерпретаций исходных данных, при которых достигается положительный результат [132].

В результате такого синтеза получаем схемы программы действий нарушителей, подлежащих оцениванию. Простые примеры таких схем программ показаны на рисунке ниже, где F_{ij} - функции, которые потенциально могут реализовываться злоумышленниками при проведении той или иной атаки.

Зная структуры таких программ и принимая во внимание случайный характер подлежащих анализу процессов, вероятности деструктивных воздействий могут быть рассчитаны с применением математического аппарата полумарковских процессов [133]. Частным случаем его выступает аппарат марковских процессов.

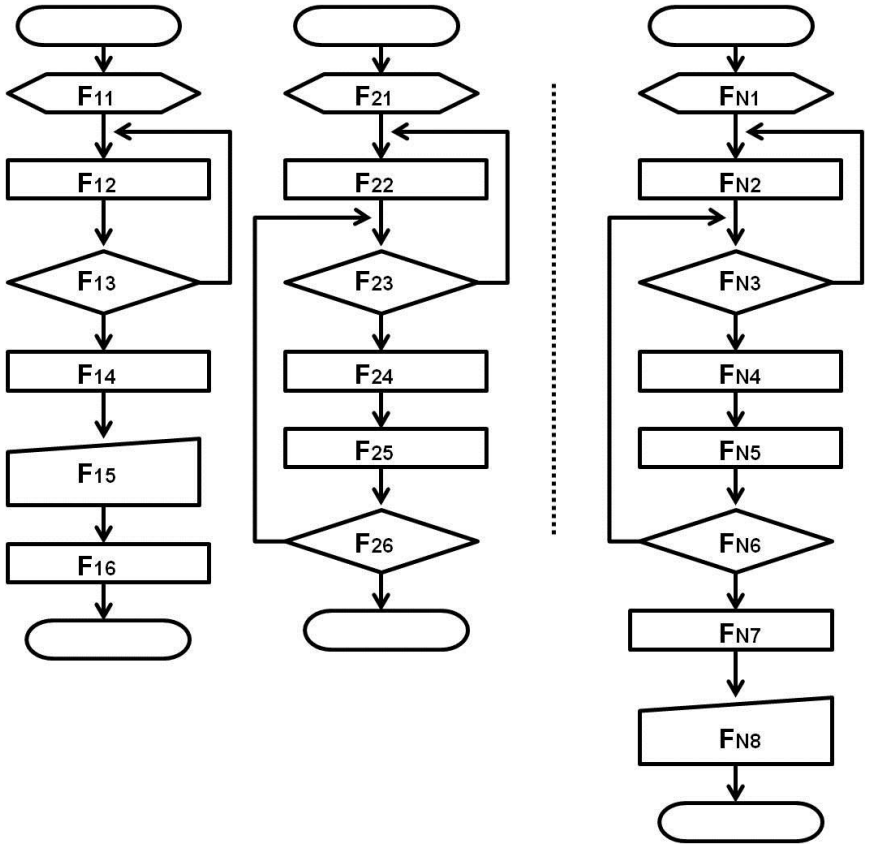


Рисунок 3 – Примеры программ действий нарушителя

Предлагается по структурам синтезированных программ автоматически составлять системы интегральных (для полумарковских процессов) или дифференциальных (для марковских процессов) уравнений и разрешать их, получать искомые вероятности $P_{kzs}(PRG_{kzs}(M_k), t)$ деструктивных воздействий на z-е информационные ресурсы по возможным s-м программам $PRG_{kzs}(M_k)$ при реализации комплекса M_k мероприятий ИБ. Технология автоматического составления таких систем уравнений известна. Методы разрешения их реализованы в ряде пакетов прикладных программ (Matlab, Mathcad). В ряде случаев могут быть использованы и другие методы оценки [134].

Особенностью такого анализа выступает необходимость учёта неопределённости по разрешению логических условий в синтезированных программах. Эта неопределённость численно характеризуется числом и длительностью циклов в соответствующих программах, которые необходимо реализовать, чтобы её преодолеть. Её также можно определять через относительные частоты анализируемых переходов. При этом возможен

автоматический синтез на знаниях не только линейных программ деструктивных воздействий, но и программ с циклами и их оценка.

По условию, все показатели должны рассчитываться с учётом влияния фактора времени. С течением времени исходные данные, защищаемые ресурсы, возможные мероприятия ИБ и условия (33-35) могут изменяться, поэтому обоснование мероприятий ИБ должно осуществляться для предварительно заданного интервала времени T, а период повторения $\Delta t << T$ такого обоснования и реализации найденных решений должен выбираться в зависимости от интенсивности угроз. В этом заключается одно из основных отличий предлагаемого подхода от всех существующих.

Итак, оптимизационная модель обоснования мероприятий ИБ можно сформулировать в следующем виде. Требуется найти комплекс M_o целесообразных мероприятий ИБ, при котором на момент времени t достигается минимум суммарных потерь $L_o(M_o, t)$:

$$L_0(M_0, t) = \min_{k \in Q} \left\{ B_k(M_k, t) + \sum_{z=1}^{Z} V_z(t) \times \right.$$
$$\left. \times \left(1 - \prod_{s=1}^{S_{kz}} (1 - P_{kzs}(PRG_{kzs}(M_k), t)) \right) \right\} \quad , \qquad (36)$$

и выполняются условия:

$$P_{kzs}(PRG_{kzs}(M_k), t) \geq P_E \, , \qquad (37)$$

$$PRG_{kzs}(M_k) \in \mathrm{R}, \qquad (38)$$

$$\mathrm{k} = 1, 2,.., \mathrm{K}; \; \mathrm{z} = 1, 2,.., \mathrm{Z}; \; \mathrm{s} = 1, 2,.., \mathrm{S_z} \, .$$

В (36)-(38) приняты обозначения: Q – область допустимых мероприятий ИБ; $B_k(M_k, t)$ – суммарные затраты на реализацию комплекса M_k мероприятий ИБ; $V_z(t)$ – текущая ценность z-го защищаемого информационного ресурса (ЗИР); K – число мероприятий ИБ; Z – число защищаемых информационных ресурсов (ЗИР); $P_{kzs}(PRG_{kzs}(M_k), t)$ – вероятность деструктивного воздействия на z-й ресурс по возможной s-й программе $PRG_{kzs}(M_k)$ при реализации комплекса M_k мероприятий

ИБ; S_{kz} – число возможных альтернативных программ деструктивных воздействий на z-й ресурс при комплексе M_k мероприятий ИБ; P_E – вероятность, при превышении которой угроза принимается во внимание; R – область допустимых результативных программ деструктивного воздействия на ЗИР.

В правой части выражения (36) второе слагаемое – это ожидаемые потери ценности ЗИР (риски). Потеря ценности z-го ресурса имеет место, если он подвергся деструктивному воздействию, хотя бы по одной из s-х программ. Согласно (37) принимаются во внимание только деструктивные программы с эффектом не ниже заданного. В соответствии с (38) анализируются только результативные программы, приводящие к нарушениям ИБ за конечное число шагов.

Оригинальность метода заключена, прежде всего, в комбинации нескольких известных подходов к оценке рисков, оценке ценности информационных ресурсов, комбинаторики, теории формальной логики и теории марковских процессов. Математический аппарат марковских процессов использовался для расчёта вероятностей деструктивного воздействия на защищаемые ресурсы по синтезированным программам. При оценке ценности информационных ресурсов в ситуации, когда можно успешно восстановить утраченные ЗИР до момента их использования, предлагается применять выражение (30), которое определяет ценность ЗИР как минимум затрат на их восстановление.

Поскольку обоснование мероприятий ИБ предлагается осуществлять, исходя из минимума общих потерь, среди которых ключевое место занимают потери из-за снижения ценности ЗИР, используемая модель оценки ценности этих ресурсов была доработана из ныне существующих и уточнена для конкретной ситуации, что позволило упросить расчёты и исключило наличие многих неизвестных, ранее получаемых статистическим путём или методом экспертного опроса, что, в свою очередь, имело сильное влияние на точность и объективность оценки при расчёте этого показателя. Подробно вывод этой формулы будет представлен в следующей главе, при описании математических моделей систем – потребителей конкретной информации.

Новизна предлагаемого метода состоит в новой совокупности условий, при которой предлагается обосновывать мероприятия ИБ. В целом особенностью предлагаемого метода выступает его ориентированность на широкий круг возможных ситуаций обеспечения ИБ, учёт ценности ЗИР и потенциальной информированности злоумышленников на текущий момент времени. Отдельные положения метода могут быть применимы также при решении частных задач ИБ. В целом предлагаемый метод расширяет взгляды и возможности по обоснованию мероприятий ИБ в различных условиях.

При расчёте ущерба всегда надо помнить о «тонких» моментах, связанных с учётом последствий нарушения режима ИБ. Как правило, имеются экономические и неэкономические аспекты (например, аспекты, связанные с разглашением персональной информации или потерей репутации организации), которые следует приводить (отображать) в денежные шкалы.

Поскольку, как уже было сказано в предыдущей главе, для СВО понимание «информационной безопасности» подразумевает защиту интересов населения, т.е. обеспечение безопасности всех субъектов услуг СВО и их прав при выполнении процесса, и здесь ущерб рассчитывается не по отношению в СВО, а по отношению к его клиентам. Что сделать сложнее настолько, насколько сложнее определить ценность той или иной информации для каждого конкретного человека и обобщить этот показатель. Однако в отношении процесса Назначение и выплата пенсии эту оценку сделать немного проще. Ценность остановки этого процесса для любого гражданина, имеющего право на пенсию, будет укладываться как минимум в сумму неполученной выплаты, а как максимум будет включать в себя моральный ущерб, который может быть причинён как нарушением непрерывности процесса и не точности оценки пенсионных прав, так и нарушением конфиденциальности персональных данных. Для СВО нарушение этого процесса повлечёт ряд штрафных санкций, наложенных государством в ответ на понесённые им репутационные риски, размер которых ограничен законодательством.

Необходимо разработать комплекс моделей, включающий возможные варианты реализации атаки на представленные защищаемые процессы, учитывая

объективные закономерности реального процесса, что и будет сделано в следующей главе.

Выводы по второй главе

Предложен метод управления ИБ СВО на основе комплекса разработанных оптимизационных моделей и усовершенствованный метод обоснования мероприятий ИБ по критерию минимума интегральных потерь на заданном интервале времени.

Согласно первому методу в качестве объекта защиты может рассматриваться не только информационная система, но и вся организация в целом. Учитывается необходимость защиты не только информационных ресурсов, но и процессов. Может учитываться широкий спектр интересов заинтересованных лиц. Возможно включение в оценку оптимальности мероприятий по ИБ таких параметров как: удобство для пользователей, интегрируемость в текущую инфраструктуру, контролируемость и т.п. Этот метод позволяет не только давать рекомендации и управлять системой защиты, выстраивать политики высокого уровня и стратегию обеспечения ИБ, но и давать рекомендации по эффективному выстраиванию основных деловых процессов СВО и построению самих объектов защиты. Выстраиваемая таким образом СОИБ обладает всеми требуемыми свойствами: системность, интегрируемость, комплексность, прозрачность, адекватность, оптимальность и подконтрольность.

Предложенные в рамках первого метода оптимизационные модели охватывают широкий круг условий и задач, которыми специалист по ИБ может руководствоваться при поиске оптимальных мероприятий ИБ. Особенность их построения заключается в способности задавать комбинации любых необходимых условий оценки оптимальности мероприятий ИБ, поэтому на их основе могут быть выработаны наиболее адекватные поставленной задаче рекомендации.

Согласно второму методу обоснование мероприятий ИБ предлагается осуществлять, исходя из минимума общих потерь, среди которых ключевое место

занимают потери из-за снижения ценности защищаемых информационных ресурсов.

В интересах этого метода также предложено несколько моделей оценки ценности информации, которые учитывают то, что информация может использоваться одновременно в разных информационных системах организации для обеспечения сразу нескольких деловых процессов, а все показатели рассматриваются с учётом влияния фактора времени, поскольку он является основополагающим при определении ценности информационных ресурсов.

В целом особенностью предлагаемых методов выступают их ориентированность на широкий круг возможных ситуаций обеспечения ИБ, учёт ценности ЗИР и потенциальной информированности злоумышленников на текущий момент времени.

3. МОДЕЛИ ЗАЩИЩАЕМЫХ И ДЕЗОРГАНИЗУЮЩИХ ПРОЦЕССОВ ДЛЯ СОЦИАЛЬНО-ВАЖНЫХ ОБЪЕКТОВ

3.1. Модель функционирования социально-важного объекта

Структура и порядок функционирования любой организации формируется под влиянием её основных деловых процессов. Можно говорить о том, что совокупность основных деловых процессов организации фактически полностью описывают её функциональную модель. Анализ предлагается провести на примере ПФР. Поэтому для разработки модели функционирования СВО был выбран один из наиболее характерных ПФР деловой процесс «Назначение и выплата пенсии». Этот процесс в полной мере является типовым для СВО, поскольку: состоит из нескольких базовых функциональных циклов: получение данных, проверка, анализ и получение результата, проверка, ввод данных, проверка и т.д.; имеет несколько заранее известных типов существенных состояний - (не) корректно отказано в регистрации заявления; принято (не)корректное решение об отказе в удовлетворении заявления, заявление (не)корректно выполнено; выполнение каждого из шагов отмечается и закрепляется юридически; на результаты и ход выполнения процесса влияют различные факторы, в том числе наличие случайных и преднамеренных разрушающих воздействий, а также возможность совершения ошибок первого и второго рода при принятии решений (проверках).

События, возникающие в этих процессах, имеют массовый и случайный характер. И, при этом, обладают свойством статистической устойчивости, что позволяет использовать в процессе принятия решений эффективные математические методы теории случайных процессов и, в частности, одного из её разделов - теории марковских процессов.

События процесса дискретны, время выполнения непрерывно, а сам процесс может быть представлен как процесс с отсутствием последействия, т.е. он обладает свойством марковости. В итоге, например, процесс «назначения и выплаты пенсии» можно формализовать марковским процессом. Анализ таких случайных

процессов обычно проводится с помощью графов состояний и переходов. Процесс назначения и выплаты пенсии может быть представлен следующим графом (рисунок 4).

Представленный ниже граф описывает сложный деловой процесс, результатом выполнения которого могут быть следующие варианты:

– заявление правомерно возвращено без регистрации (отказано в выплате) с разъяснением причины отказа;

– выплата произведена в соответствии с законодательством (направление списков в банк и платёжных документов в казначейство);

– заявление неправомерно возвращено без регистрации (отказано в выплате);

– выплата произведена не корректно (поддельные списки направлены в банк, платёжные документы с не корректными суммами направлены в Казначейство). Первые два из них являются желательными, вторые два – являются следствиями нарушений делового процесса.

Где под цифрами понимаются следующие состояния:

1 – в клиентскую службу обратился гражданин либо поступило заявление;

2 – ожидание результата проверки достоверности и полноты представленных документов;

3 – заявление правомерно возвращено без регистрации с разъяснением причины отказа;

4 – заявление неправомерно возвращено без регистрации;

5 – заявление ошибочно зарегистрировано, документы отсканированы;

6 – заявление правомерно зарегистрировано, документы отсканированы;

7 – ожидание недостающих документов (запрошена выписка ИЛС, направлены уточняющие запросы в другие подразделения, внешние организации (истребованы недостающие документы));

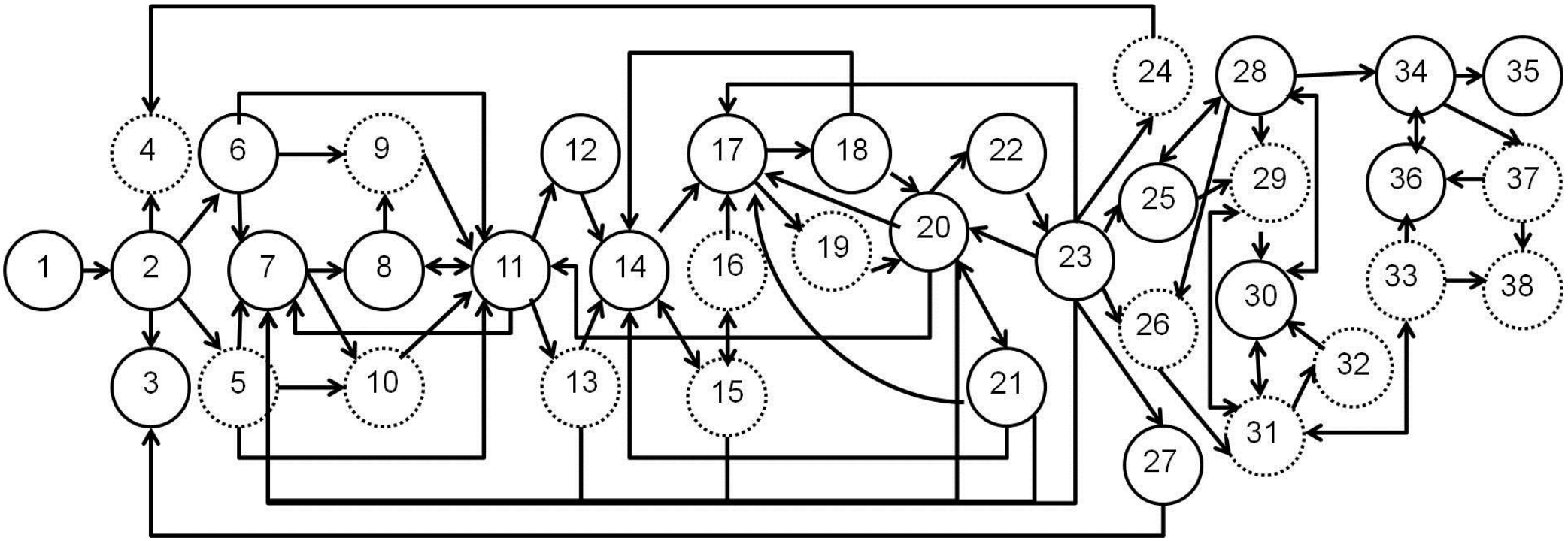


Рисунок 4 – Деловой процесс «Назначение и выплата пенсии»

8 – запрашиваемые документы поступили;

9 – внесены НС изменения в бумажное и электронное дело;

10 – потупили некорректные (поддельные) документы/данные;

11 – ожидание результата проверки соответствия копий оригиналам и полноты представленных документов руководителем клиентской службы;

12 – к назначению принято полное и правильно оформленное выплатное дело и передано на проверку руководителю назначения;

13 – к назначению принято выплатное дело с некорректными данными и передано на проверку руководителю назначения;

14 – ожидание результата проверки полноты представленных документов специалистом отдела назначения;

15 – выписка из индивидуального лицевого счета (ИЛС) не подтвердила данные в выплатном деле;

16 – внесение изменений в ПТК СПУ;

17 – выписка из ИЛС подтвердила данные в выплатном деле;

18 – данные выплатного дела заведены в ПТК НВП;

19 – в ПТК НВП заведены некорректные данные;

20 – выработан проект решения, ожидание результата проверки отделом контроля назначения;

21 – пересчитанный проект решения не совпал с предыдущим расчётом;

22 – пересчитанный проект решения совпал с предыдущим;

23 – ожидание проверки последнего рассчитанного проекта решения;

24 – принято неправомерное решение об отказе в удовлетворении заявления;

25 – принято правомерное решение об удовлетворении заявления;

26 – принято неправомерное решение об удовлетворении заявления;

27 – принято правомерное решение об отказе в удовлетворении заявления;

28 – изменения внесены в ИЛС, сформирована сумма на выплату (осуществляется в автоматизированном режиме на основании принятого решения+удержания);

29 – в данные по удержаниям либо в выплатные суммы внесены несанкционированные изменения (НСД в базу);

30 – появились новые данные (удержания, новое решение), необходима проверка сумм на выплату;

31 – сформированы некорректные суммы на выплату;

32 – произведён очередной расчёт массивов выплатной информации и реестры не сошлись;

33 – очередной расчёт массивов выплатной информации и реестры сошлись, но конкретные суммы выплаты неверны и на выплату приняты некорректные документы;

34 – произведён очередной расчёт массивов выплатной информации, реестры сошлись и выплатные документы приняты на выплату;

35 – выплата произведена в соответствии с законодательством (направление списков в банк и платёжных документов в казначейство);

36 – произведена проверка принятых на выплату документов;

37 – в выплатные документы внесены несанкционированные изменения;

38 – выплата произведена не корректно (поддельные списки направлены в банк, платёжные документы с некорректными суммами направлены в Казначейство).

В текущем виде моделируемый процесс достаточно сложен для анализа. Для многоэлементных систем с большим числом состояний аналитическое моделирование на основе теории марковских процессов становится весьма громоздким. В целях упрощения деловой процесс назначения и выплаты пенсии может быть разбит на следующие несколько подпроцессов, представленных в таблице 5.

Таблица 5. Подпроцессы назначения и выплаты пенсии

№	Название подпроцесса	Описание	Результат выполнения
1	Приём документов	Рабочий процесс клиентской службы	Правомерный либо неправомерный приём заявления, либо отказ в приёме заявления
2	Истребование дополнительных документов	Рабочий процесс клиентской службы и оценки пенсионных прав застрахованных лиц	Получение корректных и некорректных дополнительных документов
3	Принятие решения	Рабочий процесс отдела назначения пенсий и оценки пенсионных прав застрахованных лиц	Принятие правомерного либо неправомерного решения об отказе, либо об удовлетворении заявления
4	Расчёт выплат	Рабочий процесс отдела выплаты пенсии	На выплату приняты корректные либо некорректные выплатные документы
5	Выплата пенсии	Рабочий процесс отдела выплаты пенсии	Выплата произведена в соответствии с законодательством либо выплата произведена некорректно

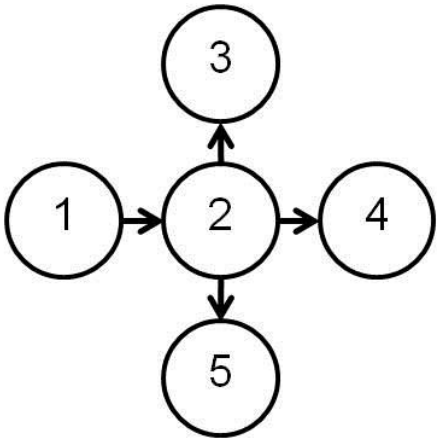
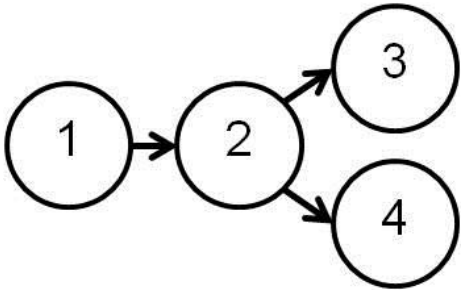
Для использования в дальнейшем и в целях получения более точной оценки необходимо разработать отдельные модели для каждого из подпроцессов делового процесса «Назначение и выплата пенсии».

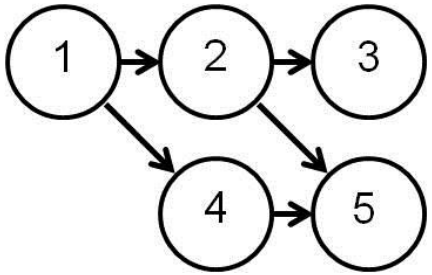
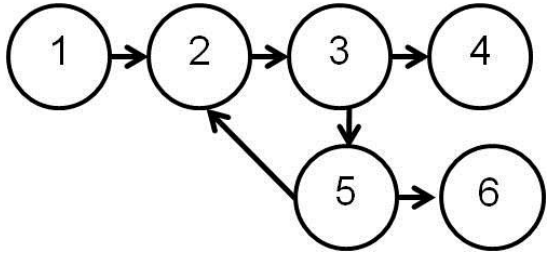
3.2. Модели защищаемых и дезорганизующих процессов применительно к информационной безопасности социально-важных объектов на примере ПФР

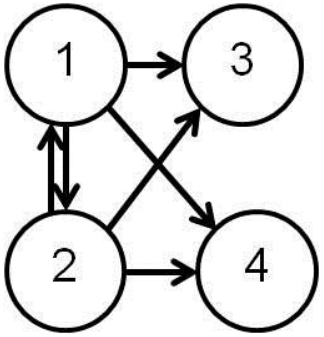
В соответствии с алгоритмом обоснования мероприятий информационной безопасности СВО, представленным в параграфе первом главы второй, составим модели подпроцессов Назначения и выплаты пенсии. Эти модели представлены в виде графов состояний и для каждой из них приведена соответствующая система дифференциальных уравнений (таблица 6).

Дальнейшее подробное рассмотрение этих и других защищаемых процессов и выделение соответствующих угроз, позволит составить более приближенную к реальности модель процесса, которая будет учитывать все возможные актуальные нарушения.

Таблица 6. Модели защищаемых деловых процессов СВО

Название модели	Граф состояний	Обозначения состояний	Система дифференциальных уравнений
Модель 1. Приём документов		1 – в клиентскую службу обратился гражданин либо поступило заявление; 2 – ожидание результата проверки достоверности и полноты представленных документов; 3 – заявление возвращено без регистрации с разъяснением причины отказа; 4 – заявление правомерно зарегистрировано; 5 – заявление ошибочно зарегистрировано.	$\frac{dP_1(t)}{dt} = -\lambda_{12}(t) * P_1(t)$; $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) - (\lambda_{23}(t) + \lambda_{24}(t) + +\lambda_{25}(t)) * P_2(t)$; $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t)$; $\frac{dP_4(t)}{dt} = \lambda_{24}(t) * P_2(t)$; $\frac{dP_5(t)}{dt} = \lambda_{25}(t) * P_2(t)$.
Модель 2. Истребование дополнительных документов		1 – заявление зарегистрировано; 2 – ожидание недостающих документов (направлены уточняющие запросы в другие подразделения, направлен запрос в другие органы (истребованы документы); 3 – запрашиваемые документы поступили; 4 – потупили некорректные (поддельные) документы/данные.	$\frac{dP_1(t)}{dt} = -\lambda_{12}(t) * P_1(t)$; $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) - (\lambda_{23}(t) + \lambda_{24}(t)) * * P_2(t)$; $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t)$; $\frac{dP_4(t)}{dt} = \lambda_{24}(t) * P_2(t)$.

Название модели	Граф состояний	Обозначения состояний	Система дифференциальных уравнений
Модель 3. Принятие выплатных дел к назначению		1 – ожидание недостающих документов (направлены уточняющие запросы в другие подразделения, направлен запрос в другие органы (истребованы документы); 2 – запрашиваемые документы поступили; 3 – к назначению принято полное и правильно оформленное выплатное дело; 4 – потупили некорректные (поддельные) документы/данные; 5 - к назначению принято выплатное дело с некорректными данными.	$\frac{dP_1(t)}{dt} = -(\lambda_{12}(t) + \lambda_{14}(t)) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) - (\lambda_{23}(t) + \lambda_{25}(t)) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t);$ $\frac{dP_4(t)}{dt} = \lambda_{14}(t) * P_1(t) - \lambda_{45}(t) * P_4(t);$ $\frac{dP_5(t)}{dt} = \lambda_{25}(t) * P_2(t) + \lambda_{45}(t) * P_4(t).$
Модель 4. Перерасчёт выплат		1 – принято решение об удовлетворении заявления; 2 – произведён расчёт сумм, полагающихся к выплате в соответствии с последним принятым решением; 3 – произведён расчёт массивов выплатной информации; 4 – на выплату приняты корректные документы; 5 – реестры сошлись, но конкретные суммы выплаты неверны (вследствие внесения несанкционированных изменений в базе данных); 6 – на выплату приняты некорректные документы.	$\frac{dP_1(t)}{dt} = -\lambda_{12}(t) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) + \lambda_{52}(t) * P_5(t) - -\lambda_{23}(t) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t) - (\lambda_{34}(t) + \lambda_{35}(t)) ** P_3(t);$ $\frac{dP_4(t)}{dt} = \lambda_{34}(t) * P_3(t);$ $\frac{dP_5(t)}{dt} = \lambda_{35}(t) * P_3(t) - (\lambda_{52}(t) + \lambda_{56}(t)) * P_5(t);$ $\frac{dP_6(t)}{dt} = \lambda_{56}(t) * P_5(t).$

Название модели	Граф состояний	Обозначения состояний	Система дифференциальных уравнений
Модель 5. Выплата пенсии		1 – выплатные документы приняты на выплату; 2 – произведена проверка принятых на выплату документов; 3 – выплата произведена в соответствии с законодательством (направление списков в банк и платёжных документов в казначейство); 4 – выплата произведена не корректно.	$\frac{dP_1(t)}{dt} = \lambda_{21}(t) * P_2(t) - (\lambda_{12}(t) + \lambda_{13}(t) + \lambda_{14}(t)) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) - (\lambda_{21}(t) + \lambda_{23}(t) + \lambda_{24}(t)) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{13}(t) * P_1(t) + \lambda_{23}(t) * P_2(t);$ $\frac{dP_4(t)}{dt} = \lambda_{14}(t) * P_1(t) + \lambda_{24}(t) * P_2(t).$

Тогда вероятность перехода в состояния нарушения конфиденциальности информации будет отражать состояние защищённости процесса и можно будет рассчитать по заданным данным любые интересующие параметры [135].

Метод получения исходных данных о процессе (включая интенсивности переходов и другие параметры), а также результаты моделирования для этих данных с применением разработанных методов и моделей будут представлены в третьей главе.

Рассмотрим актуальные для делового процесса СВО угрозы нарушения информационной безопасности. Помимо типовых и распространённых угроз, направленных на остановку или прерывание делового процесса, существует целый класс характерных именно для СВО угроз некорректного завершения делового процесса. В целом, некорректное завершение делового процесса СВО может быть спровоцировано тремя способами:

– за счёт подачи в СВО поддельных документов на протяжении всей жизни (работает по факту один человек, а стаж и зарплата, то есть пенсионный капитал числится за другим) – эффект «мёртвых душ» и нарушение аутентичности;

– подделка дополнительных документов, влияющих на определение размера выплаты (старше 80-ти лет, ордена и награды, северные, и т.п., то есть независимые от пенсионного капитала) – нарушение достоверности;

– внесение изменений непосредственно в платёжные документы – нарушение целостности.

В рамках представленного деления интерес представляет подробный анализ возможных нарушений на конкретном деловом процессе СВО. В качестве примера возьмём все тот же процесс Назначения и выплаты пенсий (далее НВП). Рассматривая основные этапы, которые процесс проходит во времени, и, учитывая схожесть и различия технической реализации атаки, следует говорить о четырёх типах атак на этот типовой процесс:

Первая – подделка документов ещё до момента их подачи в СВО для создания эффекта «мёртвых душ». В этом случае ни на одном из этапов невозможно будет обнаружить, что такого человека фактически не существует.

Данную угрозу реализует внешний нарушитель, идёт нарушение аутентичности информации (подмена личности – одного человека выдают за другого);

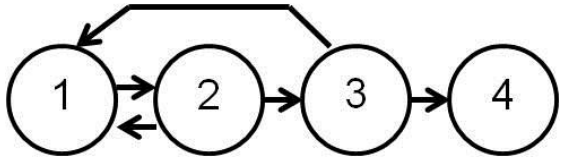
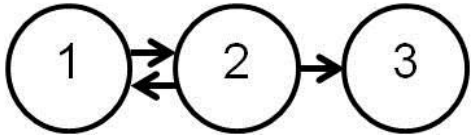
Вторая – подделка документов на этапе проверки правильности заявления и сопутствующих документов, когда оператор принимает к регистрации оформленные с нарушениями документы. Это может быть, как заявитель, так и ошибка или содействие оператора, принимающего документы;

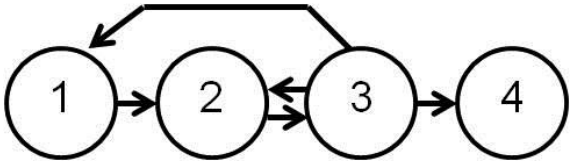
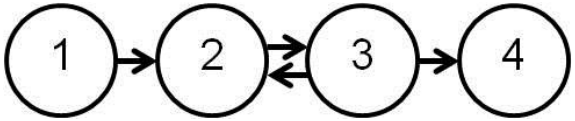
Третья – подделка документов на этапе ответа на запрос, когда в СВО приходят искажённые данные о лице, подавшем заявление, что провоцирует неверное определение прав на предоставление государственной услуги и неправомерное принятие решения об удовлетворении или отказе в услуге. Может осуществляться внутренним нарушителем ведомств, с которыми реализуется взаимодействие в рамках оказания услуги, внутренним нарушителем СВО и внешними нарушителем с помощью технического перехвата данных – атака «man in the middle»

Четвертая – неправомерная корректировка сумм выплат перед направлением списков в банки. Последняя в этом списке, но первая по количеству инцидентов атака, реализуется внутренним нарушителем. К данной категории нарушений следует отнести также подделку данных (не только сумм выплат, а любых данных) уже непосредственно при передаче в банки и в Управление Казначейства РФ с использованием атаки «man in the middle».

Каждая из представленных атак имеет собственную стратегию и представляет собой последовательный набор действий, приводящий к одному результату, за счёт нарушения работы разных звеньев делового процесса [14]. Рассуждая таким образом, можно выделить несколько типовых наборов действий нарушителя, компонуя которые можно реализовать большое количество атак, в том числе указанные выше. Эти наборы и будут представлять собой модели типовых нарушения ИБ СВО, они представлены в таблице ниже.

Таблица 7. Модели типовых нарушений ИБ СВО

Название модели	Граф состояний	Обозначения состояний	Система дифференциальных уравнений
Модель 1. Подмена источника (поставщика) данных. Атака «masquerading»		1 – злоумышленник отслеживает обращения СВО к внешнему источнику (поставщику) данных; 2 – запрос СВО к внешнему источнику данных перехвачен; 3 – злоумышленник маскируется и направляет ответ от имени источника; 4 – некорректные данные приняты (нарушение аутентичности и целостности данных)	$\frac{dP_1(t)}{dt} = \lambda_{21}(t)) * P_2(t) + \lambda_{31}(t) * P_3(t) - - \lambda_{12}(t) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) - (\lambda_{23}(t) + + \lambda_{21}(t)) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t) - (\lambda_{31}(t) + + \lambda_{34}(t)) * P_3(t);$ $\frac{dP_4(t)}{dt} = \lambda_{34}(t) * P_3(t).$
Модель 2. Перехват передаваемых данных. Атака «man in the middle» (компрометация канала связи)		1 – злоумышленник отслеживает обращения СВО к внешнему источнику (поставщику) данных; 2 – злоумышленник перехватил/вычислил/подобрал ключевую/парольную информацию; 3 – несанкционированный доступ (НСД) к защищаемым информационным ресурсам получен.	$\frac{dP_1(t)}{dt} = \lambda_{21}(t)) * P_2(t) - \lambda_{12}(t) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) - (\lambda_{23}(t) + + \lambda_{21}(t)) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t).$

Модель 3. Нарушение целостности данных		1 – злоумышленник получает доступ к данным; 2 – злоумышленник вносит изменения в данные; 3 – проверка данных; 4 – некорректные данные приняты.	$\frac{dP_1(t)}{dt} = \lambda_{31}(t) * P_3(t) - \lambda_{12}(t) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) + \lambda_{32}(t) * P_3(t) - - \lambda_{23}(t) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t) - (\lambda_{31}(t) + +\lambda_{32}(t) + \lambda_{34}(t)) * P_3(t);$ $\frac{dP_4(t)}{dt} = \lambda_{34}(t) * P_3(t).$
Модель 4. Подача поддельных данных на входе		1 – злоумышленником формируются поддельные документы; 2 – поддельные документы подаются в СВО; 3 – СВО принимает поддельные документы; 4 – деловой процесс нарушен.	$\frac{dP_1(t)}{dt} = -\lambda_{12}(t) * P_1(t);$ $\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) + \lambda_{32}(t) * P_3(t) - - \lambda_{23}(t) * P_2(t);$ $\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t) - (\lambda_{32}(t) + + \lambda_{34}(t)) * P_3(t);$ $\frac{dP_4(t)}{dt} = \lambda_{34}(t) * P_3(t).$

На первый взгляд, модели кажутся примитивными и не отличающимися оригинальностью, однако каждая из них имеет совершенно различный внутренний смысл, выявленный на основе обширного профессионального опыта, а их простая структура отражает реальную ситуацию в моделируемой области. Все модели имеют прикладной характер.

Если разбить атаки по типам нарушителей, то получим: внутренние инсайдерские угрозы (человеческий фактор – халатность или подкуп) – угрозы подделки документов служащими СВО и ведомств, с которыми реализуется взаимодействие в рамках оказания услуги и угрозы, реализованные внешними нарушителями, в основном это атаки на систему передачи информации.

Атаки «masquerading» и «man in the middle» с помощью технического перехвата данных требует высокой квалификации нарушителя, наличия специальных технических средств, возможно связей с организациями, предоставляющими транспорт, и значительных затрат в целом. Если эти обе атаки производятся на уровне бумажного документооборота, то стоимость такой атаки заметно снижается.

Подделка передаваемых документов, а также подделка данных на ходе может быть исключена при полноценном вводе системы межведомственного электронного взаимодействия, которая обеспечит выгрузку достоверных данных непосредственно из баз соответствующих ведомств и тогда остаётся только подделка документов на стороне ведомства, предоставляющего информацию для реализации государственной услуги.

Атаки с подделкой документов, подаваемых в СВО на протяжении всей жизни (эффект «мёртвых душ» и нарушение аутентичности), предупредить невозможно, однако она не очень популярна из-за своей масштабности, сложности и тяжести наказания. Это нарушение внутренними мерами СВО предупредить не может.

Общими словами – невозможно обеспечить силами СВО защиту документов, предоставляемых внешними организациями, с которыми реализуется взаимодействие в рамках оказания услуги – поскольку проверка таких сведений всегда будет подразумевать сверку с внешними информационными ресурсами, доверие к которым равняется доверию взаимодействующей организации, со всеми

вытекающими рисками. Здесь возможно только обеспечить безопасность каналов передачи и полагаться на достоверность источников.

Уязвимость процесса к внутренним нарушителям диктует и свой набор защитных мер. Улучшить положение можно за счёт обеспечения защиты баз данных СВО таким образом, чтобы невозможно было подделать информацию ни на одном из этапов бесконтрольно, поскольку именно состояния 2, 7, 11, 14, 20, 23 процесса назначения и выплаты пенсии (рисунок 4) являются слабым звеном системы за счёт лёгкости реализации угроз. Несанкционированный доступ к базам данных подразумевает необходимость классификации объектов и субъектов доступа, необходимость систематизировать, отслеживать и контролировать порядок предоставления доступа к разным типам ресурсов. Таким образом, чтобы там, где это возможно исключить пересечение прав исполнителей и контролирующих лиц, к примеру, в подсистеме выплаты пенсии угроза неправомерной корректировки сумм выплат внутренним нарушителем.

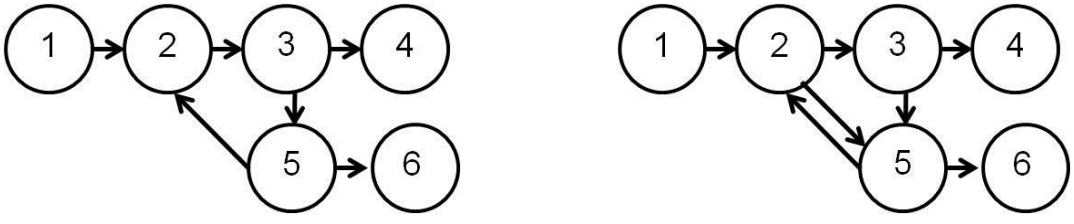
В условиях очень большого разброса в подходах к организации ИБ и свободой в принятии решений на уровне регионов используемая на сегодняшний момент структура системы предоставления доступа оставляет актуальным вопрос защиты от несанкционированного доступа. Новая система должна обладать следующими свойствами: интегрируемость, иерархичность, универсальность, гибкость, подконтрольность и простота дальнейшего отслеживания.

Общими, как для приведённой структуры, так и для других структур процесса обеспечения ИБ, являются противоречия между: уровнем защищённости и доступности информационных ресурсов; уровнем защищённости и затратами на обеспечение ИБ; затратами на обеспечение ИБ и возможным информационным ущербом со стороны несанкционированных пользователей и другие.

3.3. Модели мероприятий информационной безопасности социально-важных объектов на примере задачи обоснования набора прав доступа

Для решения поставленной задачи предлагается составить граф состояний, который бы одновременно формализовал выполнение критичной функции организации, возможных деструктивных воздействий для неё и предлагаемых мероприятий ИБ. Интенсивности переходов из состояния в состояние могут задаваться исходя из требований регламента моделируемого делового процесса и имеющейся статистики нарушений, тогда вероятность перехода в состояние нарушения делового процесса будет обратно пропорционально отражать степень его защищённости [136].

Рассмотрим в качестве примера напрямую связанный с оперированием денежными средствами подпроцесс «Перерасчёт выплат». Актуальной угрозой для этого подпроцесса является возможность корректировки данных персоналом, имеющим доступ к соответствующим записям в базе данных. Но вероятность этой угрозы, помимо изменений периода проверки назначенных сумм и выплатных документов, можно снизить дополнительными мерами, касающимися порядка организации предоставления доступа к защищаемым ресурсам. К примеру, не должны пересекаться права сотрудников, которые осуществляют ввод данных и контролируют формирование выплатных документов. Используем для указанного подпроцесса модель 4 (таблица 6) и усовершенствуем её, добавив ещё один переход. В обобщённом виде соответствующие графы состояний будут выглядеть следующим образом:



а) ***б)***

Рисунок 5 – Модель подпроцесса «Перерасчёт выплат» при условии разделения *а*) и смешения *б*) прав доступа

При этом, как уже было сказано выше, чем меньше процесс находится в состоянии 6, тем выше уровень ИБ. Также он зависит от изменения параметров переходов из состояния 3 в состояния 4 и 5, и из состояния 5 в состояния 2 и 6. Увеличение времени перехода из состояния 5 в состояние 6 связано с улучшением эффективности защитных мер. Заметим, что в случае предоставления пользователям неоптимального набора прав доступа (в данном случае права на ввод и контроль ввода выданы одному и тому же сотруднику), граф состояний будет обладать ещё одним ребром перехода из состояния 2 в состояние 5 (рисунок 5б), поскольку несанкционированные изменения могут оказаться не исправленными.

Система дифференциальных уравнений будет выглядеть следующим образом:

Таблица 8. Система дифференциальных уравнений, описывающая подпроцесс «Перерасчёт выплат»

При условии разделения прав	При условии смешения прав
$\frac{dP_1(t)}{dt} = -\lambda_{12}(t) * P_1(t);$	$\frac{dP_1(t)}{dt} = -\lambda_{12}(t) * P_1(t);$
$\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) + \lambda_{52}(t) * P_5(t) - -\lambda_{23}(t) * P_2(t);$	$\frac{dP_2(t)}{dt} = \lambda_{12}(t) * P_1(t) + \lambda_{52}(t) * P_5(t) - -(\lambda_{23}(t) + \lambda_{25}(t)) * P_2(t);$
$\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t) - (\lambda_{34}(t) + \lambda_{35}(t)) * * P_3(t);$	$\frac{dP_3(t)}{dt} = \lambda_{23}(t) * P_2(t) - (\lambda_{34}(t) + \lambda_{35}(t)) * * P_3(t);$
$\frac{dP_4(t)}{dt} = \lambda_{34}(t) * P_3(t);$	$\frac{dP_4(t)}{dt} = \lambda_{34}(t) * P_3(t);$
$\frac{dP_5(t)}{dt} = \lambda_{35}(t) * P_3(t) - (\lambda_{52}(t) + \lambda_{56}(t)) * * P_5(t);$	$\frac{dP_5(t)}{dt} = \lambda_{35}(t) * P_3(t) + \lambda_{25}(t) * P_2(t) - -(\lambda_{52}(t) + \lambda_{56}(t)) * P_5(t);$
$\frac{dP_6(t)}{dt} = \lambda_{56}(t) * P_5(t).$	$\frac{dP_6(t)}{dt} = \lambda_{56}(t) * P_5(t).$

Точно такая же ситуация с подпроцессом «Выплата пенсии» (рабочий процесс отдела выплаты). Актуальной угрозой для этого подпроцесса является возможность некорректной проверки направленных на выплату документов и отправку на выплату документов с поддельными данными. Вероятность этой

угрозы можно снизить только контролем выдачи ролей и прав доступа на ввод и проверку данных, также, как и для подпроцесса «Перерасчёт выплат». Модель выплаты пенсии представлена в таблице 6 на рисунке 5 и, учитывая возможные наборы прав доступа, она может выглядеть следующим образом:

а) *б)*

Рисунок 6 – Модель подпроцесса «Выплата пенсии»
при условии разделения *а*) и смешения прав доступа *б*)

На представленном выше рисунке использованы обозначения согласно таблице 6. Получаем что в случае, когда процесс организован по всем требованиям безопасности, невозможно что бы после проверки оставались какие-либо искажённые данные, т.е. переход из состояния 2 в состояние 4 исключён и наоборот. При этом, уровень ИБ зависит от изменения параметров переходов в состояния 3 и 4. В случае 2а) увеличение интенсивности перехода из состояния 1 в состояние 2 по отношению к 1-4 повышает уровень ИБ. При предоставлении пользователям неоптимального набора прав доступа - в случае 2б) переход в состояние 2 не гарантирует достоверность сведений, поэтому так важен показатель перехода из состояния 2 в 3 и 4, их пропорциональность и связь с переходами из 1 в 3 и 4.

Таблица 9. Система дифференциальных уравнений, описывающих подпроцесс «Выплата пенсии»

При условии разделения прав	При условии смешения прав
$\frac{d\mathrm{P}_1(\mathrm{t})}{dt} = \lambda_{21}(\mathrm{t}) * \mathrm{P}_2(\mathrm{t}) - (\lambda_{12}(\mathrm{t}) + \lambda_{13}(\mathrm{t}) + \lambda_{14}(\mathrm{t})) * \mathrm{P}_1(\mathrm{t});$ $\frac{d\mathrm{P}_2(\mathrm{t})}{dt} = \lambda_{12}(\mathrm{t}) * \mathrm{P}_1(\mathrm{t}) - (\lambda_{21}(\mathrm{t}) + \lambda_{23}(\mathrm{t})) * \mathrm{P}_2(\mathrm{t});$ $\frac{d\mathrm{P}_3(\mathrm{t})}{dt} = \lambda_{13}(\mathrm{t}) * \mathrm{P}_1(\mathrm{t}) + \lambda_{23}(\mathrm{t}) * \mathrm{P}_2(\mathrm{t});$ $\frac{d\mathrm{P}_4(\mathrm{t})}{dt} = \lambda_{14}(\mathrm{t}) * \mathrm{P}_1(\mathrm{t}).$	$\frac{d\mathrm{P}_1(\mathrm{t})}{dt} = \lambda_{21}(\mathrm{t}) * \mathrm{P}_2(\mathrm{t}) - (\lambda_{12}(\mathrm{t}) + \lambda_{13}(\mathrm{t}) + \lambda_{14}(\mathrm{t})) * \mathrm{P}_1(\mathrm{t});$ $\frac{d\mathrm{P}_2(\mathrm{t})}{dt} = \lambda_{12}(\mathrm{t}) * \mathrm{P}_1(\mathrm{t}) - (\lambda_{21}(\mathrm{t}) + \lambda_{23}(\mathrm{t}) + \lambda_{24}(\mathrm{t})) * \mathrm{P}_2(\mathrm{t});$ $\frac{d\mathrm{P}_3(\mathrm{t})}{dt} = \lambda_{13}(\mathrm{t}) * \mathrm{P}_1(\mathrm{t}) + \lambda_{23}(\mathrm{t}) * \mathrm{P}_2(\mathrm{t});$ $\frac{d\mathrm{P}_4(\mathrm{t})}{dt} = \lambda_{14}(\mathrm{t}) * \mathrm{P}_1(\mathrm{t}) + \lambda_{24}(\mathrm{t}) * \mathrm{P}_2(\mathrm{t}).$

Оценку эффективности выданных прав доступа рекомендуется осуществлять согласно оптимизационной модели (20) – **Ошибка! Источник ссылки не найден.**, где $\mathrm{P}_{\mathrm{H}_k}(\mathrm{T})$ – вероятность некорректной выплаты при *k*-то варианте доступа на момент времени *T*, $\mathrm{P}_{\mathrm{K}}(\mathrm{T})$ – вероятность того что выплаты произведены в соответствии с законодательством; $P_{зад.}$ – заданная нижняя граница вероятности выплаты в соответствии с законодательством; $T_{пров.}(T)$ – период перерасчёта сумм в выплатных документах; $T_{доп.}$ – допустимый период перерасчёта сумм в выплатных документах. Так для модели «Перерасчёт выплат»:

$$P_H(T) = P_6(T), \tag{39}$$

$$P_{K_k}(T) = P_{4_k}(T), \tag{40}$$

$$T_{\text{пров.}}(T) = T_{52_k}(\mathrm{T}). \tag{41}$$

А для модели «Выплата пенсии»:

$$P_H(T) = P_4(T), \tag{42}$$

$$P_{\mathrm{K}_k}(\mathrm{T}) = P_{3_k}(\mathrm{T}), \tag{43}$$

$$T_{\text{пров.}}(\mathrm{T}) = T_{12_k}(\mathrm{T}). \tag{44}$$

В следующем параграфе рассмотрим метод, позволяющий рассчитать распределение вероятностей состояний, в которых может находиться процесс в начальный момент времени.

3.4. Метод определения начальных состояний защищаемых процессов

Состояния, в которых на начальный момент времени могут находиться указанные выше защищаемые процессы СВО, также требуют подробного рассмотрения. При обосновании мероприятий ИБ немаловажную роль играет анализ и выделение ключевых узлов процесса, для его успешного моделирования, а также распознавание состояний, в которых система может находиться на исходный момент времени для определения показателей эффективности процесса, входящих в выбранную оптимизационную модель.

При моделировании защищаемого делового процесса необходимо учитывать, наличие возможности либо чтобы первым состоянием всегда было начальное, инициирующее запуск процесса. Могут возникать также ситуации, когда точкой отсчёта следует выбрать одно из состояний выбора, последующих инициирующему. К примеру, возьмём модель 4 таблица 6 «Модель перерасчёта выплат». Если в качестве начального состояния задать состояние 5, то можно исследовать следующие аспекты, недоступные для анализа в других случаях: как будет вести себя система после совершения атаки (в выплатные документы внесены изменения), какова вероятность возврата в защищённое состояние, а также значение периода стабилизации перед началом следующей атаки (переход из состояния 3 в состояние 5).

Также граф состояний лучше составлять, учитывая разницу в интенсивностях переходов. Если разница в интенсивностях заданных и искомых переходов различается на несколько порядков, то определение влияния искомых переходов на защищённость системы становится затруднительным. В связи с этим, при построении моделей, необходимо выбирать такие участки защищаемого процесса, которые позволят наглядно оценить вклад обосновываемого мероприятия. Иначе можно воспользоваться выбором исходных состояний, начиная с чувствительного участка системы, либо переформировать модель, отсекая нерелевантные состояния и оставить только связку чувствительных к мероприятиям по защите состояний.

Рассмотрим альтернативный метод определения начальных состояний - распознавания состояний, в которых система может находиться на исходный момент времени. Представим ниже возможные признаки состояний деловых процессов СВО (таблица 10).

Таблица 10. Признаки состояний деловых процессов СВО

№ п/п	Типовые состояния	Признаки состояний	Веса
1.	Поступление в СВО заявления от гражданина	A_{11} - Получение СВО заявления о назначении пенсии	$A_{11} = 0,8$
		A_{12} - Получение СВО любого из документов, обязательных для предоставления государственной услуги, в том числе, которые гражданин вправе представить по собственной инициативе	$A_{12} = 0,2$
2.	Приём и проверка правильности оформления представленных документов	A_{21} - Осуществлён запрос в базы данных СВО об отсутствии факта назначения и выплаты пенсии	$A_{21} = 0,3$
		A_{22} - Осуществлён запрос наличия макета пенсионного дела	$A_{22} = 0,1$
		A_{23} - Произведено снятие недостающих копий документов	$A_{23} = 0,3$
		A_{24} - Заверение копий документов своей подписью и подписью, и печатью руководителя клиентской службы СВО	$A_{24} = 0,3$
3.	Возврат заявления без регистрации и разъяснение причины отказа	A_{31} - Обнаружено нарушение в оформлении представленных документов	$A_{31} = 0,5$
		A_{32} - Обнаружено отсутствие какого-либо из необходимых документов	$A_{32} = 0,4$
		A_{33} - Не было выдано уведомление о приёме и регистрации заявления об установлении пенсии	$A_{33} = 0,05$
		A_{34} - В журнале регистрации заявлений и решений органа СВО (далее - журнал) не была произведена регистрация заявления	$A_{34} = 0,05$
4.	Регистрация заявления (ошибочно или корректно)	A_{41} - Гражданину было выдано уведомление о приёме и регистрации заявления об установлении пенсии	$A_{41} = 0,4$
		A_{42} - Произведена регистрация заявления в журнале	$A_{42} = 0,4$
		A_{43} - Были сформированы электронные образы документов, представленных на бумажных носителях, путём их сканирования	$A_{43} = 0,1$
		A_{44} - В подразделение персонифицированного учёта (ПУ) направлен запрос выписки из индивидуального лицевого счета ЗЛ (ИЛС ЗЛ)	$A_{44} = 0,1$
5.	Направление запроса в другие органы	A_{51} - Отсутствие документа о неполучении пенсии или других документов, находящихся в	$A_{51} = 0,2$

		распоряжении других государственных органов (далее – недостающих документов)	
		A_{52} - Подписание и отправка истребования недостающих документов	$A_{52} = 0,8$
6.	Поступление недостающих документов (поддельных либо нет)	A_{61} - Наличие документа о неполучении пенсии и полного пакета документов, необходимых для начисления пенсии и находящихся в распоряжении других государственных органов	$A_{61} = 0,5$
		A_{62} - Дополнение макета выплатного (пенсионного) дела (загрузка файлов в систему) недостающими документами	$A_{62} = 0,5$
7.	Принято решение	A_{71} - Заверение руководителем СВО распоряжения об удовлетворении либо об отказе в удовлетворении поданного заявления	$A_{71} = 0,25$
		A_{72} - Заверение макета выплатного (пенсионного) дела подписями ответственных лиц	$A_{72} = 0,25$
		A_{73} - Формирование и брошюровка выплатного дела на бумажных носителях	$A_{73} = 0,25$
		A_{74} - Фиксация факта принятия решения в соответствующей информационной системе СВО (далее - ИС)	$A_{74} = 0,25$
8.	Расчёт выплат	A_{81} - Формирование электронного лицевого счета (далее - ЭЛС) пенсионера в ИС	$A_{81} = 0,1$
		A_{82} - Начисление сумм пенсий выплат в ЭЛС	$A_{82} = 0,6$
		A_{83} - Изменение статуса макета выплатного дела на открытое выплатное дело	$A_{83} = 0,3$
9.	Выплатные документы сформированы	A_{91} - Формирование массива доставочных документов	$A_{91} = 0,2$
		A_{92} - Передача доставочных документов специалисту, осуществляющему контроль	$A_{92} = 0,8$
10.	Осуществление перерасчёта/проверки	$A_{10,1}$ - Наступление окончания месяца или периода инвентаризации (истечение установленного периода проверки/перерасчёта)	$A_{10,1} = 0,4$
		$A_{10,2}$ - Разнесение информации по ЭЛС	$A_{10,2} = 0,6$
11.	Выплатные документы приняты на выплату	$A_{11,1}$ - Заверение выплатных документов подписью руководителя подразделения выплаты	$A_{11,1} = 1$
12.	Выплата произведена	$A_{12,2}$ - Получение информации об итогах доставки	$A_{12,2} = 1$

Здесь каждому из состояний процесса приведены в соответствие признаки, с той или иной вероятностью сигнализирующие о том, что процесс находится именно в этом состоянии. Все работы произведены с учётом реалий деловых процессов СВО. За основу составления данной таблицы был взят внутренний административный регламент СВО по осуществлению процесса назначения и

выплаты пенсии, который затрагивает все из исследуемых подпроцессов и состояний.

Важным моментом здесь также является определение весов для каждого из признаков. Веса были определены экспертным путём. Шкала была задана от 0 до 1, но так что бы выполнялась нормировка по всем A_{ij}, согласно которой:

$$\sum_{j=1}^{N_i} A_{ij} = 1. \quad (45)$$

То есть оценка веса каждого из показателей производилась с учётом его относительного вклада в определение оцениваемого состояния. Поскольку в целом мы должны получить распределение вероятностей по состояниям, в которых на начальный момент времени может находиться моделируемый процесс, требуется чтобы выполнялась также нормировка:

$$\sum_{i=1}^{M} P_i = 1. \quad (46)$$

Таким образом, при расчётах начального распределения вероятностей состоянии мы должны учитывать количество состояний, наличие либо отсутствие каждого из признаков и вклад каждого из присутствующих признаков относительно их общего числа:

$$P_{ij} = \frac{A_{ij}X_{ij}}{\sum_{i=1}^{M}\sum_{j=1}^{N_i} A_{ij}X_{ij}}, \quad (47)$$

где X_{ij} - булева функция, принимающая значение 1, если ij-й признак реально присутствует (наблюдается), 0 - в противном случае. Тогда вероятность нахождения процесса в i-м состоянии можно определить как:

$$P_i = \frac{\sum_{j}^{N_i} A_{ij}X_{ij}}{\sum_{i=1}^{M}\sum_{j=1}^{N_i} A_{ij}X_{ij}}. \quad (48)$$

Обратим внимание на используемый алгоритм распознавания состояний, в которых система может находиться на исходный момент времени:

1. На основе анализа защищаемого процесса выделяем признаки всех состояний этого процесса;

2. Фиксируем для каждого состояния моделируемого процесса ограниченный набор признаков;

3. Присваиваем каждому признаку каждого состояния его относительный вес – определяем значения всех A_{ij};

4. На интересующий момент времени выясняем выполняемость (наличие) всех зафиксированных выше признаков – определяем значения всех X_{ij};

5. Рассчитываем начальное распределение вероятностей P_i в соответствии с формулой (49).

Знание начальных состояний нам необходимо для разрешения соответствующих систем уравнений при обосновании мероприятий по обеспечению информационной безопасности, примеры которых будут представлены в следующей главе.

Выводы по третьей главе

В рамках предложенного в Гл. 2 метода управления ИБ СВО разработана модель функционирования СВО на примере ПФР. Поскольку структура и порядок функционирования любой организации формируется под влиянием её основных деловых процессов для разработки модели функционирования СВО был выбран один из наиболее характерных ПФР деловой процесс «назначение и выплата пенсии». Этот процесс был представлен в виде графа состояний. Поскольку в представленном виде моделируемый процесс достаточно сложен для анализа, он был разбит на типовые подпроцессы, на базе которых разработан комплекс моделей основных защищаемых деловых процессов ИБ СВО. Эти модели учитывают многократность санкционированного и несанкционированного доступа к защищаемым информационным ресурсам, возможность пересмотра мероприятий защиты, а также блокирования доступа в случаях нарушения ИБ, благодаря чему повышается информативность оценки ИБ СВО.

Также приведён комплекс из четырёх моделей основных типовых дезорганизующих процессов, применительно к ИБ СВО, который описывает все возможные атаки на деловой процесс назначения и выплаты пенсии ПФР, благодаря чему обеспечивается системность вырабатываемых контрмер.

Деловые процессы ИБ СВО и процессы нарушения ИБ СВО были рассмотрены как марковские, что позволило использовать соответствующий математический аппарат: составить системы дифференциальных уравнений, описывающие анализируемый процесс, и решить их, получая искомые вероятности нахождения процесса в каждом из состояний, что в дальнейшем позволяет рассчитать по заданным данным любые интересующие параметры.

Кроме того, было расширено представление об использовании представленных моделей. На примере рассмотрено их возможное использование в рамках предложенного метода управления ИБ СВО.

Новизна предложенных в Гл. 3 моделей состоит в отражении в формализованном виде ранее не исследуемых закономерностей, свойственных процессам обеспечения ИБ СВО, в частности в ПФР.

В целях уточнения результатов моделирования, получаемых при использовании предложенного в Гл. 2 метода управления ИБ СВО разработан метод определения начальных состояний, позволяющий распознавать состояния, в которых система может находиться на исходный момент времени.

4. РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ И ПРЕДЛОЖЕНИЯ ПО ПОВЫШЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО-ВАЖНЫХ ОБЪЕКТОВ

4.1. Исходные данные и результаты моделирования

Как уже было сказано выше, согласно представленному методу управления ИБ на основе комплекса оптимизационных моделей (рисунок 2) первым этапом обоснования мероприятии ИБ является разработка марковской модели соответствующего процесса и в том числе задание входных данных и условий поиска, а также интересующих результатов. В качестве этих данных могут одновременно выступать следующие параметры:

– наличие тех или иных связей и переходов из состояния в состояние (пример – обоснование набора прав доступа);

– интенсивности переходов из состояния в состояние (пример - обоснование оптимального периода пересмотра мероприятий по защите);

– вероятности нахождения в том или ином состоянии (пример – оценка уровня защищённости процесса);

– начальный и конечный моменты времени;

– затраты на реализацию защиты;

– ущерб от реализации угрозы (пример последних двух - обоснование мероприятий ИБ СВО по критерию минимума интегральных потерь на заданном интервале времени).

Следует уделить построению графа состояний и заданию исходных параметров наибольшее внимание, поскольку именно этим выбором будет определяться область получаемых результатов и характер возможных выходных данных.

Для представленных в предыдущей главе моделей защищаемых деловых процессов и типовых нарушений (таблица 6, таблица 7) в качестве входных данных

интенсивности переходов из состояния в состояние и ограничение по времени ($t_{конеч.}$) могут задаваться основываясь на:

– регламенте моделируемого делового процесса;

– статистических данных;

– требуемых (заданных по техническому заданию) показателях.

Поскольку деловые процессы СВО зачастую жёстко регламентированы, в том числе по времени, то для большинства переходов значения интенсивности фиксированы и являются обязательной частью процесса. Но некоторые из интенсивностей переходов определены вероятностью реализации той или иной угрозы или зависят от особенностей мероприятий ИБ (к примеру, от частоты проведения проверок). Эта неопределённость может быть исключена в ходе разработки оптимизационных моделей ИБ, поскольку эти интенсивности становятся искомыми параметрами.

Например, при определении наиболее оптимального периода пересмотра мероприятий по защите можно столкнуться со следующими сложностями. Хотя период проведения проверки зафиксирован в нормативных документах, мы можем рассчитать период обеспечения определённого уровня безопасности, т.е. на какой период времени в текущих условиях может гарантироваться определённая вероятность нахождения процесса в состоянии 4 для модели 1 и 4 (таблица 6) в состоянии 3 для моделей 2, 3 и 5 (таблица 6), а также оценить безопасность системы с любым заданным периодом проверки и многое другое.

В другом случае, интенсивности переходов могут быть определены путём сбора и обработки статистических данных. В ряде случаев, когда известны начальные и конечные состояния процесса на некотором интервале времени, то определение исходных интенсивностей осуществимо также путём подбора параметров с использованием метода наименьших квадратов, также, как и распознавание исходных состояний системы.

Рассмотрим результаты распознавания состояний процесса на основе параграфа 3.4. предыдущей главы. В качестве примера возьмём модель подпроцесса «Приём заявлений» (модель 1, таблица 6) и рассчитаем для неё

начальное распределение вероятностей по формуле (49). Пример результатов такого расчёта приведён в таблице 11.

Таблица 11. Определение начальных состояний для модели «Приём заявления»

Состояние	A_{ij}	X_{ij}	P_{ij}	P_i
1.В клиентскую службу обратился гражданин либо поступило заявление	$A_{11} = 0,8$	1	0,47058824	0,588235
	$A_{12} = 0,2$	1	0,11764706	
2.Ожидание результата проверки достоверности и полноты представленных документов	$A_{21} = 0,3$	1	0,17647059	0,411765
	$A_{22} = 0,1$	1	0,05882353	
	$A_{23} = 0,3$	1	0,17647059	
	$A_{24} = 0,3$	0	0	
3. Заявление возвращено без регистрации с разъяснением причины отказа	$A_{31} = 0,5$	0	0	0
	$A_{32} = 0,4$	0	0	
	$A_{33} = 0,05$	0	0	
	$A_{34} = 0,05$	0	0	
4.Заявление правомерно зарегистрировано	$A_{41} = 0,4$	0	0	0
	$A_{42} = 0,4$	0	0	
	$A_{43} = 0,1$	0	0	
	$A_{44} = 0,1$	0	0	
5.Заявление ошибочно зарегистрировано	$A_{51} = 0,4$	0	0	0
	$A_{52} = 0,4$	0	0	
	$A_{53} = 0,1$	0	0	
	$A_{54} = 0,1$	0	0	

И таким образом мы получаем следующее начальное распределение [0,6; 0,4; 0; 0; 0] для модели «Приём документов» при наличии заданного набора наблюдаемых признаков.

Теперь рассмотрим вклад, который вносят такие исходные данные, как определение начальных состояний, в расчёт интересующих неизвестных.

Пример 1. *Определим ценность истребуемых документов, находящихся в ведомстве других организации, для подпроцесса «Принятия выплатного дела (ВД) к назначению» (таблица 6, модель 3).* Актуальной угрозой для этого подпроцесса

является возможность получения некорректных документов из других организаций, что повлечёт к принятию ВД с некорректными данными, а значит к произведению выплат с нарушением законодательства. Предлагается, согласно алгоритму обоснования мероприятий по защите информации, составить системы дифференциальных уравнений, описывающие анализируемый процесс, и решить их, получая искомые вероятности нахождения процесса каждом из состояний.

Согласно модели защищаемого процесса (таблица 6, модель 3), если процесс на заданный момент времени достигает состояния 3 с вероятностью выше заданной, то процесс можно считать защищённым, а значит тем выше уровень информационной безопасности СВО. Если периоды переходов укладываются в заданные (Административным регламентом) максимальные значения, то мы можем назвать процесс непрерывным. Если процесс находится в состоянии 4 с вероятностью менее заданной, мы можем гарантировать защищённость процесса к угрозе получения поддельных документов из других ведомств на заданном уровне. Если процесс находится в состоянии 5 с вероятностью менее заданной, мы можем гарантировать безопасность процесса к угрозе принятия неверного решения на заданном уровне.

Если по результатам направления запроса в другие органы (истребование документов) в орган СВО не поступило документов или поступили недостоверные документы, решение о принятии ВД к назначению будет априори принято не верно. В качестве ЗИР здесь выступают дополнительные документы и данные, находящиеся в ведомстве других организации, поскольку они играют немаловажную роль при принятии решений о назначении пенсии. Что бы достоверно определить важность и ценность этих документов для подпроцесса «Принятия выплатного дела (ВД) к назначению» воспользуемся подходом к оценке ценности ЗИР, изложенным в параграфе 2.3 настоящей работы.

Принимая в качестве получаемого эффекта уровень защищённости процесса, рассчитаем вероятность нахождения процесса в третьем состоянии $P_3(t)$ на конечный момент времени $t_{конеч.}$ при наличии ЗИР W_2 и их отсутствии W_1. Тогда разница между ними даст нам искомый эффект $\Delta W = P_{3ЗИР}(t) - P_{3безЗИР}(t)$.

В случае, когда периоды перехода из состояния в состояние равны T_{xy}, то $\lambda_{xy}=1/T_{xy}$. Периоды переходов задаются на основе регламента моделируемого производственного процесса и приведены в таблице 12.

Таблица 12. Исходные данные для модели «Принятие ВД к назначению»

Переход	1→2	2→3	2→5	1→4	4→5
$\lambda_{ЗИР}$	0,066667	0,2	0,005	0,02	0,2
$\lambda_{безЗИР}$	0,066667	0,2	0,005	0,2	0,2

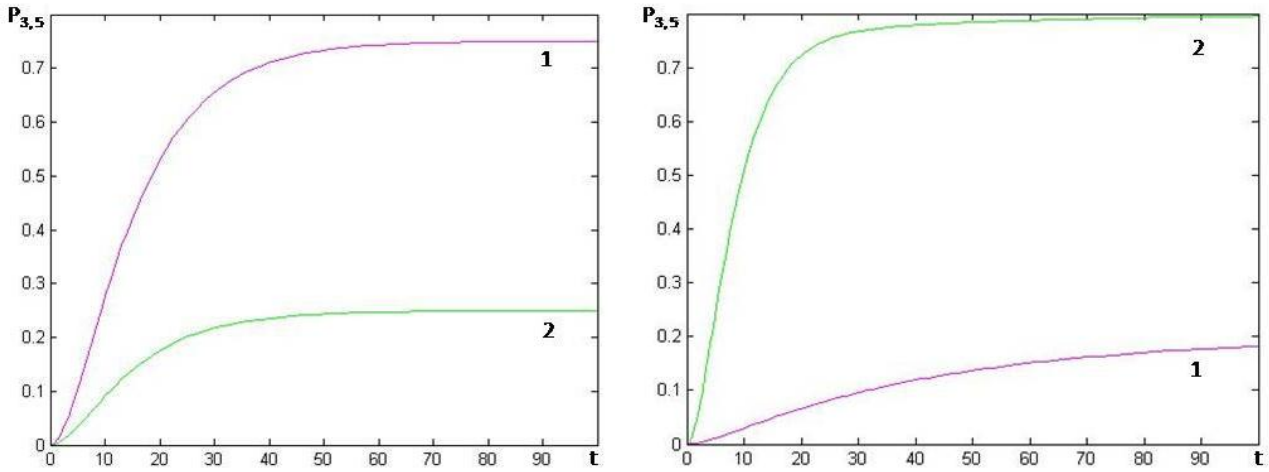
Здесь выше заданы периоды переходов из состояния 1 в состояния 4 и 2 в зависимости от получаемых достоверных и недостоверных данных. Изменение интенсивностей соответствующих переходов приведут к снижению вероятности принятия верного решения, которое и необходимо вычислить.

Моделирование производится следующим образом, при всех заданных λ мы можем вычислить любое $P_x(t)$, для любого t на выбранном отрезке. К примеру, для указанных выше T и $t_{конеч.}=20$, при условии распределения начальных состояний [1,0,0,0,0], согласно нотации, принятой в пакете MatLab, система дифференциальных уравнений имеет вид, приведённый в таблице 13.

Таблица 13. Системы дифференциальных уравнений для модели «Принятие ВД к назначению»

При наличии ЗИР	При отсутствии ЗИР
*F= [– 0.06667*y(1) – 0.02*y(1);* *0.06667*y(1) – 0.2*y(2) – 0.005*y(2);* *0.2*y(2);* *0.02*y(1) – 0.2*y(4);* *0.005*y(2) + 0.2*y(4)]*	*F= [– 0.06667*y(1) – 0.2*y(1);* *0.06667*y(1) – 0.02*y(2) – 0.005*y(2);* *0.2*y(2);* *0.2*y(1) – 0.2*y(4);* *0.005*y(2) + 0.2*y(4)]*

Вероятность принятия корректного ВД $P_3(t)$ и некорректного ВД $P_5(t)$ по условиям задачи неизвестны. Требуется оценить $P_3(t)$ при разных условиях. Все расчёты были осуществлены в программном комплексе MatLab, куда были подставлены соответствующие системы дифференциальных уравнений. Для наглядности представим следующую зависимость.



а) *б)*

Рисунок 7 – Зависимость вероятности принятия корректного (кривая 1) и некорректного (кривая 2) ВД от времени при наличии *а)* и при отсутствии *б)* ЗИР

Сравнивая рисунки, представленные выше, наблюдаем прямо пропорциональную картину изменения вероятностей принятия к назначению корректного и некорректного ВД в зависимости от наличия и отсутствия ЗИР. Эти графики наиболее наглядно показывают насколько важна роль ЗИР, верных входных данных, документов, необходимых для подпроцесса «Принятия выплатного дела (ВД) к назначению».

На рисунке 8 приведены также зависимости вероятности корректного принятия выплатного дела от времени для других условий.

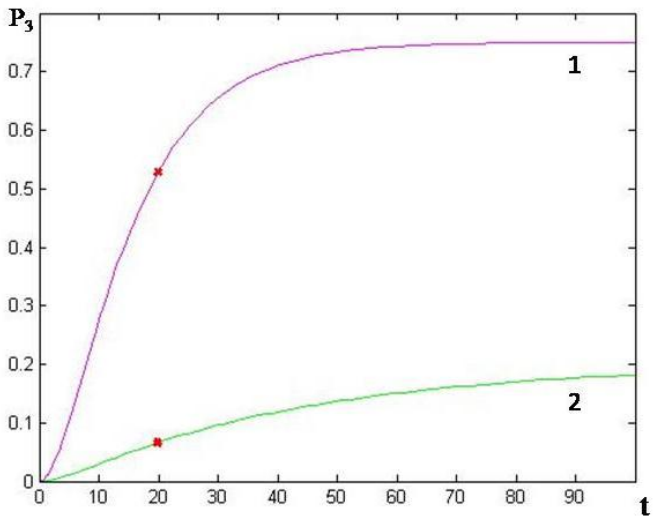


Рисунок 8 – Зависимость вероятности принятия корректного ВД от времени при наличии (кривая 1) и при отсутствии ЗИР (кривая 2)

На момент времени $t = 20$ вероятность принятия к назначению корректного ВД равна 0,5282 и 0,06561 соответственно. Таким образом, можно говорить о том, что правильно полученные документы, которые находятся в ведомстве других организаций, имеют вклад, оказываемый на правильность принятого решения, равный 46%. Интересно также наблюдать характер роста вероятности принятия ВД в обоих вариантах. В первом случае рост экспоненциальный первые 30 минут, последующие пол часа рост продолжается, но значительно медленнее, пока вовсе не останавливается на отметке в 0,7479 при $t = 60$. Далее рост наблюдается практически незаметный и на наблюдаемом отрезке времени не превышает 0,8. Во втором случае вероятность принятия к назначению корректного ВД возрастает постоянно с практически неизменной скоростью и в итоге на наблюдаемом промежутке не превышает 0,2.

Результаты расчётов показали следующее:

$$P_{ЗЗИР}(t=20) = 0,5285,$$

$$P_{ЗбезЗИР}(t=20) = 0,06561.$$

А ΔW:

$$\Delta W = 0,5285 - 0,0656 = 0,46289.$$

Для другого t:

$$P_{ЗЗИР}(t=60) = 0,7435,$$

$$P_{ЗбезЗИР}(t=60) = 0,1519.$$

В этом случае ΔW:

$$\Delta W = 0,7435 - 0,1519 = 0,5916.$$

То есть, при $t = 60$ с течением времени ценность ЗИР повышается и вероятность принятия к назначению корректного ВД равна практически 60%.

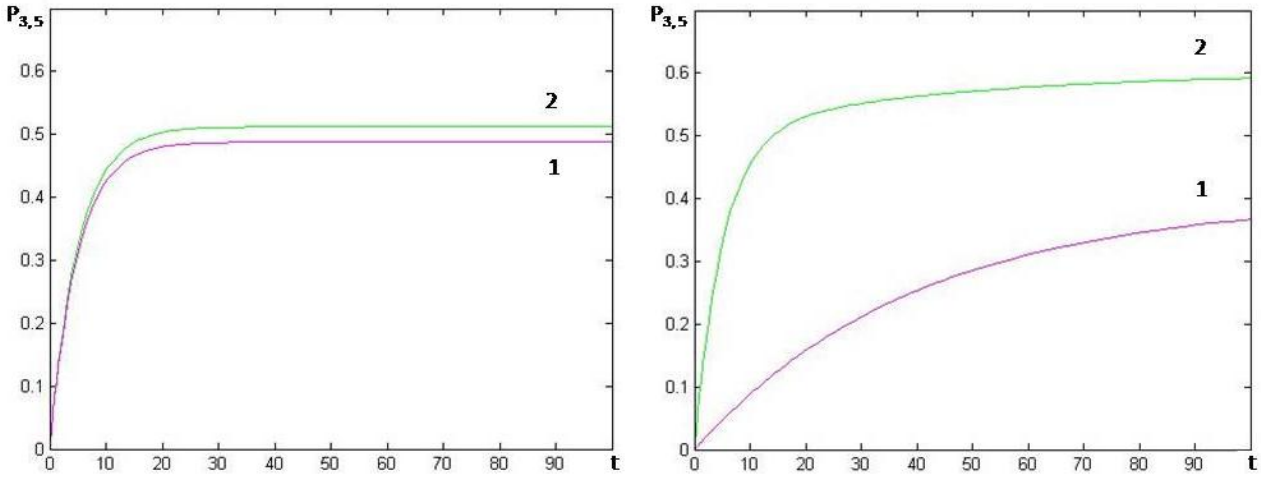
Пример 2. *Произведём те же самые вычисления с предварительной оценкой начальных состояний, где набор наблюдаемых признаков соответствует* X_{ij}, *указанным в таблице ниже.*

Таблица 14. Определение начальных состояний для модели подпроцесса «Принятие ВД к назначению»

Состояние	A_{ij}	X_{ij}	P_{ij}	P_i
1. Направление запроса в другие органы (истребование документов)	$A_{11} = 0,2$	0	0	0
	$A_{12} = 0,8$	0	0	
2. Поступление необходимых документов	$A_{21} = 0,5$	1	0,25	0,5
	$A_{22} = 0,5$	1	0,25	
3. Принято корректное решение об удовлетворении заявления/отказе в приёме заявления	$A_{31} = 0,3$	0	0	0
	$A_{32} = 0,3$	0	0	
	$A_{33} = 0,3$	0	0	
	$A_{34} = 0,1$	0	0	
4. Документы не получены/получены поддельные документы	$A_{41} = 0,5$	1	0,25	0,5
	$A_{42} = 0,5$	1	0,25	
5. Решение принято неверно	$A_{51} = 0,3$	0	0	0
	$A_{52} = 0,3$	0	0	
	$A_{53} = 0,3$	0	0	
	$A_{54} = 0,1$	0	0	

В итоге получим следующее распределение начальных состояний [0; 0,5; 0; 0,5; 0]. При таком начальном раскладе рассчитаем вероятность принятия корректного ВД к назначению при наличии и отсутствии ЗИР и вычислим в итоге ценность ЗИР согласно системам дифференциальных уравнений (таблица 13). Все

расчёты были также осуществлены в программном комплексе MatLab. Результаты моделирования представлены на рисунках 9, 10.



а) ***б)***

Рисунок 9 – Зависимость вероятности корректного (кривая 1) и некорректного (кривая 2) принятия решений от времени при наличии *а)* и при отсутствии *б)* ЗИР при заданных начальных состояниях

На этих рисунках наблюдается совершенно иная зависимость: в обоих случаях вероятность принятия корректного ВД всегда ниже вероятности некорректного. На рисунке 9а функции имеют одинаковую динамику и вероятности практически сравниваются по значению. То есть при начальном распределении вероятностей получения корректных и некорректных документов 50 на 50 и при условии наличия ЗИР мы получаем точно такое же распределение вероятностей на выходе. Не смотря на неизменно высокую вероятность принятия некорректного ВД, влияние ЗИР все же играет свою роль – при их отсутствии вероятность принятия корректного ВД сильно снижается. Разберём ценность ЗИР подробнее.

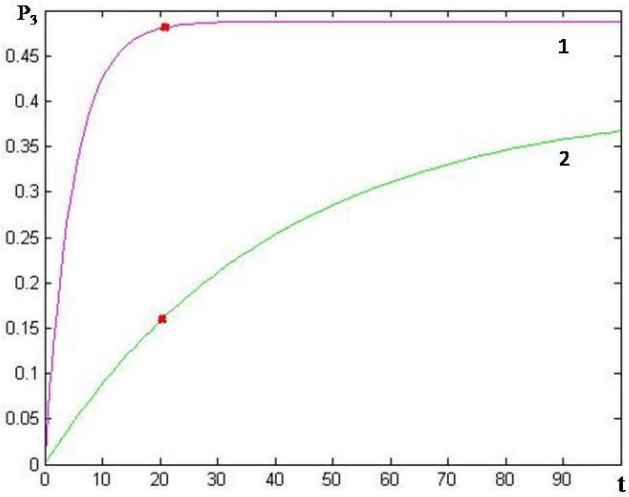


Рисунок 10 – Зависимость вероятности принятия корректного ВД от времени при наличии (кривая 1) и при отсутствии ЗИР (кривая 2) при заданных начальных состояниях

Как можно заметить, при таком раскладе:

$$P_{3ЗИР}(t=20) = 0,48,$$

$$P_{3безЗИР}(t=20) = 0,16.$$

Тогда

$$\Delta W = 0,48-0,16 = 0,32.$$

Ценность ЗИР значительно снижается и уже не оказывает такого внушительного влияния на вероятность принятия корректного ВД, однако она всё ещё составляет одну треть - 32% от общей доли показателей, влияющих на правильность принятия решения. Здесь можно сделать ещё один важный вывод – в случае, когда относительно первоначального момента времени мы не уверены в каком состоянии находится исследуемый процесс, необходимо прибегать к методу поиска первоначальных вероятностей, изложенному в параграфе 3.4, поскольку первоначальное распределение играет очень важную роль. В итоге, при наличии равных начальных вероятностей получения правильных и поддельных документов ценность ЗИР снижается, поскольку мы изначально предполагаем, что с вероятностью 50% мы получим необходимые документы. В данном случае такое первоначальное распределение вероятностей позволяет рассчитать ценность ЗИР, когда невозможно определить корректность полученных документов.

Здесь характер роста функций следующий: при наличии ЗИР наблюдается резкий рост вероятности первые 10 минут, где $P_З=0,42$ затем рост замедляется и, в итоге, начиная с $t=45$ не превышает 0,4878. Тогда как в отсутствии ЗИР вероятность принятия корректного ВД к назначению хоть и не превышает $P_З= 0,4$, однако и достигает этого значения только при $t=360$, через 45 минут равна 0,27, а через 60 минут равна 0,30.

Результаты расчётов показали следующее:

$$P_{ЗЗИР}(t=45) = 0,4878;$$

$$P_{ЗбезЗИР}(t=45) = 0,27;$$

$$\Delta W =0,4878-0,27= 0,2178.$$

Для другого t:

$$P_{ЗЗИР}(t=60) = 0,4878;$$

$$P_{ЗбезЗИР}(t=60) = 0,30;$$

$$\Delta W = 0,4878 - 0,30 = 0,1878.$$

Пример 3. *Рассмотрим результаты обоснования прав доступа для подпроцесса «Перерасчёт выплат»* согласно изложениям, представленным в параграфе 3.4 настоящей работы. Ниже представлены исходные данные для моделирования. Модель соответствующего защищаемого процесса представлена в параграфе 3.2 и 3.3 и различается в случаях, когда права пользователей разделены в соответствии с внутренним регламентом назначения и выплаты пенсии, а также когда предоставленные права доступа превышают необходимы минимум для выполнения той или иной роли.

Таблица 15. Исходные данные для модели «Перерасчёт выплат»

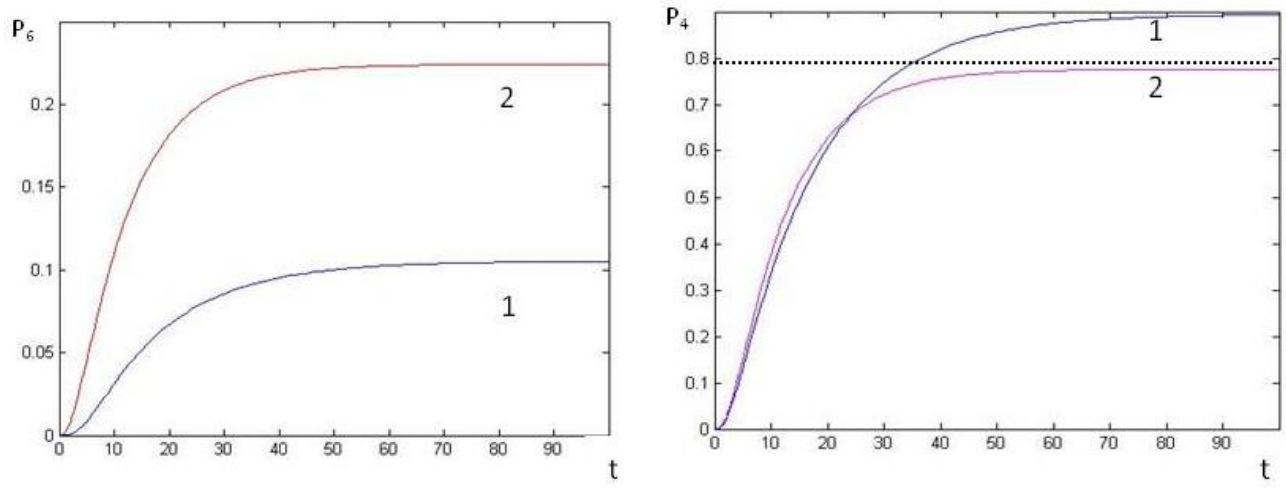
Переход	**1→2**	**2→3**	**2→5**	**3→4**	**3→5**	**5→2**	**5→6**
при разделении прав λ	0,066667	1	-	0,5	0,033333	0,5	0,5
при смешении прав λ	0,066667	1	0,033333	0,5	0,033333	0,5	0,5

Следует заметить, что в случае разделения прав доступа переход 2→5 отсутствует. Соответственно системы дифференциальных уравнений в этом случае будут выглядеть следующим образом:

Таблица 16. Система дифференциальных уравнений для модели «Перерасчёт выплат» с данными

При условии разделения прав	При условии смешения прав
*F= [– 0.06667*y(1);* *0.06667*y(1) + 0.06667*y(5) – y(2);* *y(2) – 0.5*y(3) – 0.06667*y(3);* *0.5*y(3);* *0.06667*y(3) – 0.06667*y(5) – 0.5* y(5);* *P_6(t)= 0.5*y(5)]*	*F= [– 0.06667*y(1);* *0.06667*y(1) + 0.06667*y(5) – 0.2*y(2) – y(2);* *y(2) – 0.5*y(3) – 0.06667*y(3);* *0.5*y(3);* *0.2*y(2) + 0.06667*y(3) – 0.06667*y(5) –* *– 0.5* y(5);* *0.5*y(5)]*

После соответствующих расчётов с применение программного комплекса MatLab, при условии, что процесс на момент времени t=0 находился в состоянии 1, получаем следующие графики (рисунок 11):



а) ***б)***

Рисунок 11 – Зависимость вероятности некорректной (*а*) и корректной (*б*) выплаты от времени для набора с разделением прав (кривая 1) и для набора со смешением прав (кривая 2) процесса перерасчёта выплат

Достаточным для анализа было выбрано $t_{конеч.} = 100$, поскольку в дальнейшем функция никаким образом не меняет своего поведения. Оценку эффективности выданных прав доступа для подпроцесса «Перерасчёт выплат» рекомендуется осуществлять согласно принятой оптимизационной модели (20 - 22), при $P_{зад.} = 0{,}8$ и $T_{доп.} = 15$. Обозначения используются согласно (40 - 42). На рисунке 11 б) видно, что условие $P_{4_k}(T) \geq P_{\text{зад.}}$ в первом случае выполняется начиная с T = 33, а во втором не выполняется вовсе. Следует заметить, что если бы были выбраны другие значения для $P_{зад.}$ и $T_{доп.}$, то результаты могли бы получиться иными. При $P_{зад.} = 0{,}95$ и $t_{конеч.} = 100$ ни для одного из наборов прав заданные выше условия не были бы выполнены, а значит ни один из них не подойдёт для реализации поставленных задач и необходимо осуществить поиск других вариантов.

Интересным представляется поведение функции $P_4(T)$ на промежутке времени [10,40], где сначала превалирует вероятность корректной выплаты для набора со смешением прав, а после T = 25 для набора с разделением прав. Это можно объяснить тем, что при смешении прав скорость прохождения проверок в целом возрастает, но со временем количество ошибок (случаев некорректного расчёта выплат) накапливается и вероятность корректной выплаты $P_{4_2}(T)$ замирает на показателе 0,78. Тогда как в случае разделения прав доступа при рассмотрении работы процесса на более продолжительном промежутке времени вероятность корректных выплат $P_{4_1}(T)$ возрастает до 0,9.

С вероятностью некорректной выплаты такого поведения не наблюдается – в обоих случаях она резко возрастает первые 20 минут, следующие 20 её рост замедляется, пока вовсе не останавливается на отметке 0,101 и 0,22 соответственно, вплоть до момента времени T = 100. Таким образом, мы наблюдаем ситуацию, где со временем процесс может находиться в одном из двух состояний – корректной, либо не корректной выплаты. Поэтому мы получаем два сбалансированных случая со следующим распределением вероятностей: при смешении прав с вероятностью 22% была получена некорректная и 78% – корректная выплата; при разделении прав с вероятностью 10% – некорректная и 90% – корректная выплата. Тогда

минимальная вероятность некорректной выплаты наблюдается в случае разделения прав доступа:

$$P_{б_1}(T) \leq P_{б_2}(T).$$

Анализ выходных данных показал, что предпочтение следует отдать первому варианту набора прав доступа, который при заданных условиях обеспечивает минимальную вероятность нарушения делового процесса.

В подтверждение того, что первый набор прав более предпочтителен в данной ситуации, можно привести тот факт, что СВО в своей деятельности действительно постепенно подходит к реализации ролевой модели доступа не только на уровне ПТК, но и на административно-управленческом уровне.

Таким образом, разработанные методы позволяют оперативно получать оценки, на основе которых однозначно можно выбирать наилучшие варианты обеспечения ИБ, оценить и снизить затраты ресурсов, эффективно управлять системой обеспечения ИБ.

Перейдём к рассмотрению процесса применения выработанных рекомендаций, решений и их реализация на практике. В следующем параграфе рассмотрим существующие на сегодняшний день средства, позволяющие специалисту по ИБ принимать решения, осуществлять оценку ситуации, обосновывать мероприятия ИБ и т.д., а также их применимость для СВО, их функционал, соответствие существующим требованиям и место в СОИБ.

4.2. Архитектура комплекса программных средств обоснования мероприятий информационной безопасности социально-важных объектов

Задача создания универсального средства управления ИТ и ИБ инфраструктурой стоит перед специалистами уже давно. Можно выделить четыре основных этапа процесса управления: сбор данных, их обработка (оценка), принятие решения и воплощение этого решения в жизнь на конкретной инструментальной базе. Существующие средства управления ИБ ориентированы на решение узких задач, что не позволяет в полной мере говорить об автоматизации

всех этапов процесса управления. Следует отметить, что поиск и обоснование мероприятий ИБ является ядром системы управления, поэтому эти задачи стоят вплотную друг к другу. При правильном применении такая система обеспечит планомерность и стратегический подход при обосновании мероприятий ИБ, что повысит их оптимальность до максимально возможного уровня. Рассмотрим: какой функционал должен быть заложен в этот комплекс, какой функционал уже реализован и какими существующими на сегодняшний день инструментами.

Этап сбора данных. Давно известны программные средства, которые собирают исходные данные о защищаемом объекте, его критичных процессах, ресурсах, инцидентах и уже существующих мероприятиях по обеспечению информационной безопасности. Во-первых, к ним следует отнести все модули прикладного, системного ПО и те модули средств защиты информации (СЗИ), которые осуществляют журналирование и собирают статистику работы. Во-вторых, системы-автоматические аудиторы – системы мониторинга, сканеры, основной задачей и целью которых является именно контроль и отслеживание состояний системы. Сюда относятся системы обнаружения вторжений (англ. Intrusion Detection System, IDS): IBM RealSecure, MaxPatrol, Cisco, Dragon, Symantec NetProwler, BlackICE Agent и т.д., системы предотвращения утечек и их разновидности (анг. Data Leak Prevention, DLP; Information Protection and Control, IPC и др.): InfoWatch, Инфосистемы Джет, Zecurion, Websense, Symantec, Трафика, Falcongaze, McAfee, GTB Technologies, Iteranet, МФИ Софт, SearchInform, DeviceLock. Отдельно можно выделить системы-опросники оценки соответствия требованиям стандартов - для получения недостающих данных экспертным путем. А также нормативно – методическая, организационно – распорядительная и отчетная (сюда относятся результаты аудитов) документация, описывающая состояние основных бизнес-процессов и состояние организации в целом.

Затем в этот пакет должны быть включены средства, которые соответствующим образом обрабатывают эти исходные данные, консолидируют и представляют их в таком виде, что бы специалист мог на их основе прогнозировать дальнейшее поведение системы, её реакцию на те или иные изменения и

раздражители. Этот функционал выполняют системы сбора и корреляции событий (анг. Security Information and Event Management, SIEM) [137,138]: IBM Q1 Radar, HP ArcSight, Tibco Loglogic, McAfee Nitro, Symantec, SkyBox, RSA Envision, Splunk, Security Vision и т.д.

В работах [139, 140] предложен вариант использования Business Intelligence (BI) платформ для упомянутых выше задач информационной безопасности. BI платформы предназначены для исследования и анализа работы бизнеса и включают в себя: информационно-аналитическую систему, модуль агрегации и консолидации данных, визуализации результатов, формирования отчётов и публикации статистики. Основное их отличие и преимущество заключается в том, что они позволяют работать в режиме реального времени с большими объёмами информации (Big Data), что включает в себя:

– смешанную обработку потоковых и пакетных данных;

– многоуровневое распараллеливание вычислений с обеспечением высокой локальности данных;

– распределённое хранение данных, параметров и результатов расчётов, значений показателей и метаданных;

– выявление отклонений и нестандартного поведения анализируемых показателей;

– выявление форматов, структуры и взаимосвязей с исходных данных.

Такие платформы вполне могут быть использованы для агрегированных данных о событиях безопасности, выгода от их использования возрастает в случае, если эти продукты уже внедрены для решения основных функциональных задач организации.

При обеспечении безопасности сложных, комплексных систем важно иметь инструменты, позволяющие не только получить аналитическую информацию, упорядоченные и систематизированные знания о системе и её компонентах, но и системы, предлагающие конкретные решения, осуществляющие оценку текущего состояния и помогающие специалисту принять решение о дальнейших действиях - системы поддержки принятия решений (СППР).

Эти системы позволят осуществлять моделирование защищаемых процессов, ресурсов и возможных действий нарушителя, сценариев атак, а также мероприятий и поведение системы ИБ. В качестве результатов моделирования специалист должен получать ответы на заданные им вопросы: Как поведёт себя система при отсутствии доступности такого-то узла на такой промежуток времени? Насколько снизится вероятность нарушения защищаемого процесса при вводе в действие такого-то защитного мероприятия? Какова ценность такого-то ресурса для этого процесса? Для организации в целом? С какой периодичностью следует проводить такие-то мероприятия по защите? Какой набор мероприятий будет наиболее эффективным в заданных условиях?

Следует заметить, что методы и модели, предлагаемые в настоящей работе, позволяют ответить на эти вопросы. Из всех перечисленных выше систем самое непосредственное отношение к обоснованию мероприятий ИБ имеют СППР. В настоящий момент среди перечисленных выше сегментов этот сегмент программного обеспечения наиболее остро нуждается в совершенствовании и является перспективным для разработки. Существующие на сегодняшний день СППР не в состоянии обеспечить полную автоматизацию управления ИБ, не отвечают на все поставленные выше вопросы, результаты вычислений не обеспечивают достаточного уровня точности.

Плавно перейдём к рассмотрению процесса применения выработанных рекомендаций, решений и их реализация на практике. Здесь важна не только разработка документации и организационная работа, но также адаптация выработанных политик высокого уровня к конкретным прикладным инструментам ИТ-инфраструктуры и к парку существующих средств и систем защиты информации. Межсетевые экраны, VPN, СЗИ от НСД, системы идентификации и аутентификации (AAA, IAM, SSO, SAM, IdM), антивирусные системы, антиспамы, системы разграничения доступа, системы защиты от утечек, системы обнаружения атак — все они служат одной цели и должны реализовывать выстроенную комплексную стратегию безопасности организации. Однако, разнообразие подходов, интерфейсов, протоколов и синтаксисов значительно усложняет

управление СЗИ — теряется системность применения политик безопасности, прозрачность внесения изменений, увеличивается время отклика и обнаружения ошибок, повышается требуемый уровень квалификации персонала. Таким образом, существует потребность в сервисах, позволяющих преобразовать заданную стратегию безопасности в конкретные математические функции и, используя синтаксис конкретного оборудования, сформировать готовую конфигурацию настроек, системно увязанных между собой, которая затем будет импортирована и применена на всех существующих в организации СЗИ.

Либо эти сервисы, исходя из конкретных показателей системы, после одобрения администратора безопасности, должны автоматически исправлять, либо генерировать новые политики и конфигурационные файлы для СЗИ (правила фильтрации межсетевых экранов и прокси, таблицы маршрутизации и виртуальные частные сети для маршрутизаторов, антивирусные политики, политики домена/локальные политики ОС, политики других СЗИ) и распространять их на соответствующие СЗИ.

Также эти системы могут сравнить настройки всех устройств одного или нескольких заданных классов, проверить их системность и безопасность, а также составить наглядную карту маршрутов, либо архитектуру системы. При чем, уровень визуализации должен позволять вносить изменения в графическое представление архитектуры и автоматически конвертировать эти изменения в настройки программного и аппаратного обеспечения, таким образом, система автоматически перестраивается. Это позволит исключить человеческий фактор при настройке СЗИ, исключить другие ошибки, наложение правил безопасности, появление колец в сети, превышение полномочий, пересечение прав доступа и так далее.

Таким образом, комплекс программных средств специалиста по ИБ должен включать сегмент сервисов, автоматизирующих и унифицирующих управление средствами защиты информации. Процесс управления средствами защиты информации не менее сложный, трудоёмкий и также требует автоматизации. Подобные системы уже реализованы на практике. В качестве примера таких

средств можно привести продукты компаний Tufin, Algosec, Firemon, SkyBox. Их подробный анализ представлен в работе [141].

И, наконец, средства визуализации, которые будут обеспечивать взаимодействие комплекса со специалистом на всех этапах управления системой ИБ и принятия решений. Поскольку реализуемый этим модулем функционал не самодостаточен, то этот сегмент по большей части представлен не отдельными продуктами, а реализуется в составе систем анализа рисков, управления техническими конфигурациями, контроля изменений или управления инцидентами. Примерами систем, обладающих хорошо разработанным сегментом визуализации можно назвать упомянутые выше: HP ArcSight, Security Vision, SkyBox, IBM Q1 Radar.

Здесь, в качестве дополнения, можно упомянуть модули, разработанные в составе Business Intelligence платформ, которые предназначены для бизнес-анализа и выполняющие вполне тривиальные бизнес-задачи, которые непременно включают в себя качественную визуализацию. К примеру — Contour BI и BI QlikView.

Поскольку визуализация данных — это функционал, используемый для решения очень широкого круга задач, необходимо упомянуть также о средствах визуализации как таковых, поскольку после некоторой доработки они могут быть использованы для задач обеспечения защиты информации. К такому классу программ можно отнести в частности: Gephi, Datawrapper, Datascape.

Рассмотрев существующие на сегодняшний день инструменты управления ИБ и их функционал, представим их в комплексной системе управления ИТ и ИБ инфраструктурой. Архитектура такого комплекса может выглядеть следующим образом – рисунок 12.

Представленная архитектура вполне известна специалистам, хотя, мало где реализована на практике в силу своей сложности и высокой стоимости внедрения. Такая ситуация сложилась, по большей части, из-за отсутствия модулей, позволяющих объединить уже внедрённые и благополучно работающие инструменты первого, второго и четвёртого этапа управления (сбор, обработка

данных и исполнение принятых решений), а также вследствие сложности автоматизации высокоинтеллектуальных модулей моделирования, анализа и принятия решений.

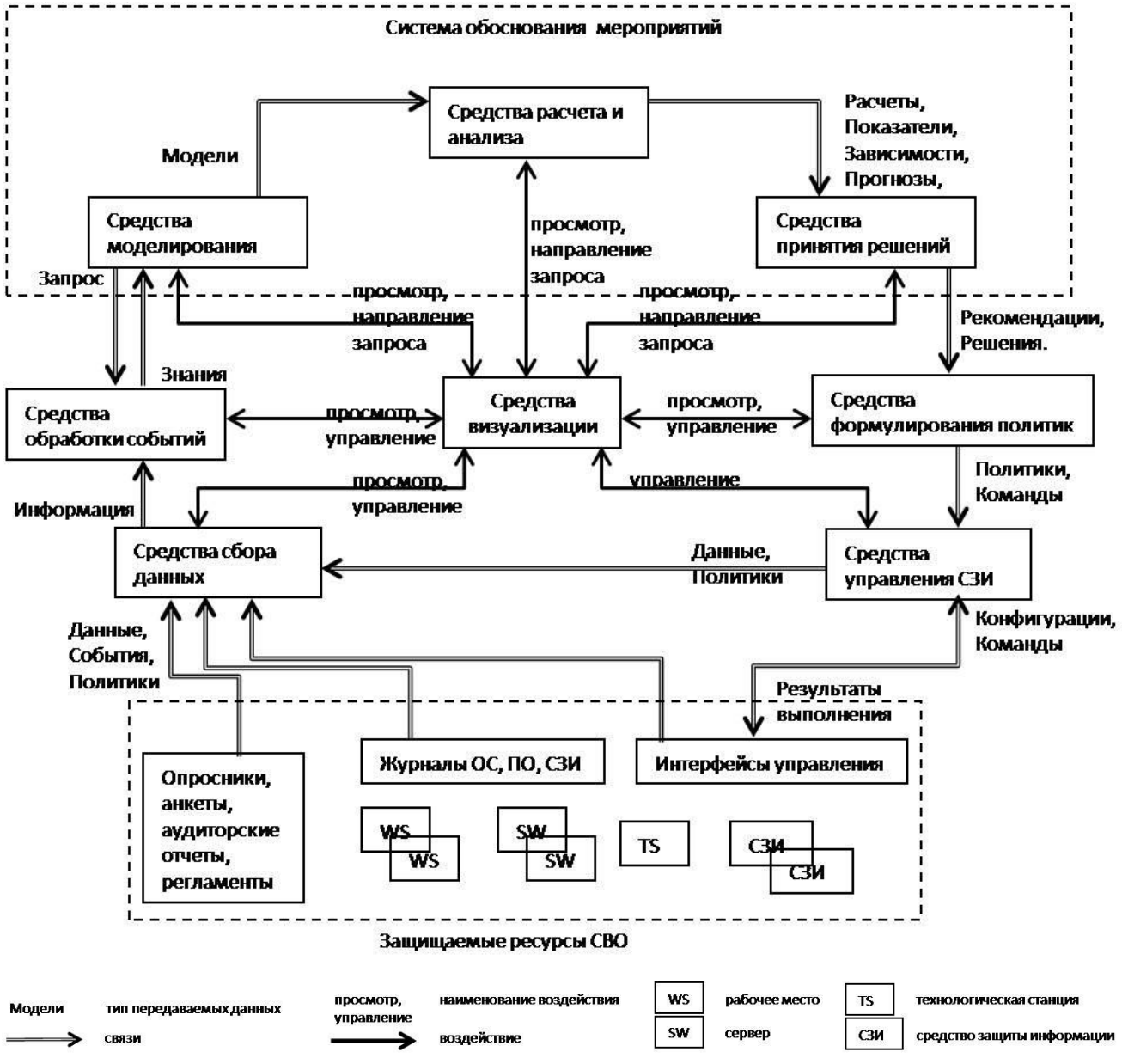


Рисунок 12 – Архитектура комплекса инструментов управления ИБ

На момент написания этой работы какие-либо комплексные системы, агрегировавшие все четыре этапа управления информационной безопасностью: сбор данных, их обработка (оценка), принятие решения и воплощение этого решения в жизнь на конкретной инструментальной базе отсутствовали. Однако упоминание их необходимости и прогнозы появления таких систем появляются во

многих работах [142, 143, 144, 145, 146]. В одной из них даже предлагается проект решения, поддерживаемого несколькими грантами [147]. В целом, об этой и подобных системах можно сказать, что они удовлетворяют всем перечисленным выше требованиям, за исключением некоторых моментов.

Во-первых, недостаточно подробно проработаны модули поддержки принятия решений. Существующие системы в целом нуждаются в разработке математически корректных алгоритмов и методов анализа данных [139]. Во-вторых, не решён вопрос «человеческого фактора» при нарушении ИБ: существующие системы не позволяют фиксировать нарушения организационных мер защиты (хранение токена, разглашение, халатность, вынос бумажных дел и документов и так далее) также оперативно и достоверно как нарушение технических мер. В-третьих, стоит отметить, что существующие системы позволяют реализовать управление только технической защитой информации. В то время как предложенный метод позволяет не только давать рекомендации и управлять организационными мероприятиями по защите, выстраивать политики высокого уровня и стратегию обеспечения ИБ, но и давать рекомендации по эффективному выстраиванию защищаемых деловых процессов и построению самих объектов защиты. Таким образом, предложенные методы и модели могут быть использованы в комплексах и системах перечисленных выше типов, однако на их основе могут быть разработаны не только средства управления СЗИ, но СОИБ. Делая выводы о недостатках в разработке класса систем, осуществляющих оценку текущего состояния и помогающих специалисту принять решение о дальнейших действиях, предлагается задание на реализацию СППР-системы обеспечения ИБ СВО, удовлетворяющей всем требованиям практикующего специалиста (таблица 17). Это задание представляет собой систему тестов, состоящих из входных данных, условий выполнения и требуемого результата их выполнения. Рабочая СППР-СОИБ СВО должна выдавать требуемый результат при вводе указанных исходных данных.

Таблица 17. Задание на реализацию СППР для СОИБ СВО

№ п/п	Типовая задача	Формулировка тестового задания	Входные данные (Дано)	Условие	Искомые данные (Найти)	Как должен быть сформулирован результат
1	Поиск оптимальной организации делового процесса с учётом требований по безопасности (Поиск оптимального периода пересмотра мероприятий по защите).	Расчёт минимального времени, необходимого для приёма и проверки документов одного клиента, при котором правомерная регистрация заявления гарантируется с максимальной вероятностью, но не менее чем 75%.	Состояния, в которых может находиться защищаемый процесс и возможные переходы; Интенсивности переходов, кроме интенсивности проверки t_x; Период времени оценки.	Вероятность правомерной регистрации заявления не менее чем 75% Минимальное время проверки t_x	Интенсивность $t = min(t_x)$	Оптимальным периодом пересмотра мероприятий будет t_x, равное Т часам. При таком периоде обеспечивается: Вероятность правомерной регистрации заявления равное Х % Минимальное время t_x равное Х мин.
2	Обеспечение безопасности процесса с вероятностью не менее заданной при минимуме ресурсов на защиту.	Вычислить набор мероприятий, при котором будет обеспечиваться минимум затрат на мероприятия по защите информации при гарантии безопасности ПТК не менее 70% в первые три недели.	Набор деструктивных программ (вектор исходных данных $\overline{DB}$, вектор интересующих результатов (целей) $\overline{DW}$, условия). Состояния, в которых может находиться защищаемый процесс и возможные переходы; Интенсивности переходов.	Вероятность нарушения делового не более 30% в течении 3-х недель. Минимум затрат на реализацию мероприятий.	Комплекс целесообразных мероприятий ИБ	Для делового процесса Х наиболее экономически эффективным будет реализация следующего комплекса мероприятий M_0. Состоящего из: мероприятие 1, мероприятие 2… При нем обеспечивается минимум потерь на заданном промежутке времени, и они могут достигать N рублей.
3	Оценка защищённости. В каких областях необходимы мероприятия по ИБ?	Оценить защищённость системы передачи данных к существующим атакам	Набор деструктивных программ (вектор исходных данных $\overline{DB}$, вектор интересующих результатов (целей) $\overline{DW}$, условия) Период времени.	Условия перехода от одной точки вектора к другой	Вероятность реализации каждой из синтезированных атак	В указанный период времени для Системы Х вероятность реализации Атаки 1 равна Х%; вероятность реализации Атаки 2 равна Х%; вероятность реализации Атаки 3 равна Х%.
4	Оценка ценности ЗИР.	Необходимо произвести оценку ценности ресурса для подпроцесса принятия решения.	Состояния, в которых может находиться процесс принятия решений и возможные переходы; интенсивности переходов. Коэффициент приведения расхода ресурса к единицам измерения конечных эффектов. Период времени, на котором расчёт должен оставаться верным.	_____	Ценность ресурса	Для процесса Х ценность ресурса У равна N рублей.

5	Максимальная безопасность при ограничении на ресурсы.	Вычислить набор мероприятий, при котором будет обеспечиваться максимальная вероятность безопасности системы в следующие 12 месяцев при затратах на защиту информации не более заданной суммы.	Набор деструктивных программ (вектор исходных данных $\overline{DB}$, вектор интересующих результатов (целей) $\overline{DW}$, условия) Состояния, в которых может находиться защищаемый процесс и возможные переходы; Интенсивности переходов.	Максимальная гарантия безопасности процесса в течении 12-ти месяцев. Затраты на защиту не более X рублей.	Комплекс целесообразных мероприятий ИБ	Для Системы X наиболее оптимальным будет реализация следующего комплекса мероприятий M_0. Состоящего из: мероприятие 1, мероприятие 2… При нем обеспечивается максимальная вероятность корректного завершения делового процесса X на заданном промежутке времени и она равна N%. Затраты на этот набор мероприятий достигают N рублей, что не превосходит X рублей.
6	Оценка эффективности мероприятий, либо закупленных СЗИ.	Вычислить экономическую эффективность заданного набора мероприятий, закупленного СЗИ.	Средство защиты. Набор деструктивных программ (вектор исходных данных $\overline{DB}$, вектор интересующих результатов (целей) $\overline{DW}$, условия) Состояния, в которых может находиться защищаемый этим СЗИ процесс и возможные переходы; интенсивности переходов. Коэффициент приведения расхода ресурса к единицам измерения конечных эффектов. Период времени, на котором расчёт должен оставаться верным.	Вероятность корректного завершения процесса Максимальная разница между затратами на защиту (закупка, поддержание СЗИ) и возможным ущербом. Минимально и максимально возможный ущерб.		Представленное СЗИ обеспечивает следующие показатели: Разница между затратами на защиту и вероятным ущербом равна X рублям. Максимально возможный ущерб = У руб. Минимально возможный ущерб = Z руб. Вероятность корректного заверения процесса = X% Согласно полученным графикам, первые X часов/дней наблюдается ситуация, когда.., следующие X часов/дней …., однако в долгосрочной перспективе … и т.п.

Если система не может выдать требуемый ответ, значит она не реализует необходимый для ИБ СВО функционал, не удовлетворяет заданию и не может быть использована. В таблице 17 представлены тесты, которые должна выполнять правильно настроенная СППР.

Представленный выше тест описывает результаты работы такой СППР, которая на сегодняшний день необходима специалисту ИБ СВО для принятия адекватных и наиболее оптимальных решений, при обосновании мероприятий ИБ.

В следующем параграфе будет рассмотрено каким образом представленный в работе метод обоснования мероприятий ИБ может быть использован для усовершенствования комплекса существующих программных средств, примерный порядок действий специалиста по ИБ, в случае, если он использует представленные методы и модели вручную, а также какие методы и модели задействуются при решении типовых задач обеспечения ИБ СВО.

4.3. Методические рекомендации к применению предложенных методов и моделей в программных средствах

В этом параграфе рассмотрим существующие задачи, которые стоят перед специалистом ИБ СВО, какие методы и модели задействуются при решении поставленных задач, каким образом представленный в работе метод обоснования мероприятий (рисунок 2) позволит решать специалисту конкретные практические задачи. И во второй части параграфа будут представлены методические рекомендации к разработке интеллектуальной системы обоснования мероприятий ИБ СВО и её возможная структура в рамках комплекса уже существующих средств.

В целом, можно сказать, что все многообразие задач, решаемое специалистами по ИБ, сводится к следующим трём: вычислить набор мероприятий при заданных условиях, вычислить показатели системы при заданном наборе, вычислить показатели заданного набора. В дальнейшем будет показано, что метод управления ИБ на основе комплекса оптимизационных моделей позволяет решать все эти задачи.

Рассмотрим наиболее типичные ситуации, возникающие в повседневной практике специалиста ИБ СВО. На их примере покажем каким образом

представленные в настоящей работе методы и модели могут быть использованы для решения этих задач (таблица 18).

Согласно таблице 18, для решения этих и подобных задач предлагается прибегнуть к методу управления ИБ СВО на основе комплекса оптимизационных моделей (рисунок 2). В рамках первого и второго шага этого алгоритма предусматривается сбор недостающих данных, за что отвечают системы мониторинга, контроля и журналирования событий. Следующий шаг – моделирование защищаемого процесса при различных условиях. Следует заметить, что в рамках каждого из указанных выше случаев необходимо использовать метод определения начальных состояний, поскольку он обеспечивает точность и адекватность получаемых результатов. Причём для всех случаев, кроме пятого, в настоящей работе были приведены работающие модели соответствующих защищаемых процессов СВО. Четвёртый шаг подразумевает под собой формулировку поискового запроса, и эта формулировка приведена для каждого из случаев. Затем все исходные данные приводятся в необходимый математический вид, осуществляются все расчёты, сравниваются и анализируются полученные результаты.

Рассмотрим вариант автоматизации действий специалиста по ИБ с использованием предложенных методов и моделей в рамках комплекса существующих программных средств. В принципе, математическую часть, включая расчёты и представление результатов расчётов в той или иной форме можно осуществить в тех же программных комплексах, что использовались в настоящей работе, таких как MatLab, Matematica и подобных, путём встраивания их модулей в СППР.

Таблица 18. Применение разработанных методов и моделей для решения типовых задач ИБ СВО

№ пп	Типовая задача	Ситуация (Пример)	Формулировка поискового запроса	Общий порядок действий	Задействованные методы
1	Поиск оптимальной организации делового процесса с учётом требований по безопасности (Поиск оптимального периода пересмотра мероприятий по защите).	Необходимо составить Регламент работы клиентской службы, в котором должны быть заданы формальные параметры качества работы, например – время приёма одного клиента. При этом ограничение времени приёма может повлечь за собой снижение качества принимаемых решений. Кроме того, известно, что если в СВО будет поступать более 75% неправильно оформленных документов это повлечёт такие затраты на последующих этапах, которые невозможно будет возместить сокращением времени приёма.	Расчёт минимального времени, необходимого для приёма и проверки документов одного клиента, при котором правомерная регистрация заявления гарантируется с максимальной вероятностью, но не менее чем 75%.	Использовать в качестве графа состояний и систем диф. уравнений данные для Модели приёма документов (таб.6 п.1); Рассчитать начальное распределение вероятностей, используя метод определения начальных состояний; Для дальнейших вычислений использовать оптимизационную модель 5, только искать t_{min}: Вычислить вероятность правомерной регистрации заявления при разных tx; Подобрать минимальную интенсивность tx, при которой вероятность правомерной регистрации заявления не менее чем 75%.	Метод управления ИБ СВО на основе комплекса оптимизационных моделей (п.2.3). Оптимизационная модель 5 периода пересмотра мероприятий (п.2.2), только ищется t_{min}. Модель защищаемого процесса СВО – Модель приема документов (таб.5 п.1). Метод определения начальных состояний (п.3.4)
2	Обеспечение безопасности процесса с вероятностью не менее заданной при минимуме ресурсов на защиту.	Руководство поставило перед отделом ЗИ задачу – для обеспечения сжатых сроков ввода в эксплуатацию нового ПТК (к примеру - модуля ПТК НВП, осуществляющего подпроцесс перерасчёта выплат), снизить объем мероприятий по защите информации, не снижая уровня безопасности делового процесса более чем на 10%. Вероятность, с которой можно гарантировать безопасность делового процесса в настоящий момент равна 80%. Окончание ввода в эксплуатацию планируется через три недели.	Вычислить набор мероприятий, при котором будет обеспечиваться минимум затрат на мероприятия по защите информации при гарантии безопасности ПТК не менее 70% в первые три недели.	Осуществить синтез программ на заданном множестве условий, используя алгоритм, изложенный в Методе обоснования мероприятия по критерию минимума; Составить граф состояний защищаемого процесса и системы диф. или интегральных уравнений для каждого из них – в качестве основания использовать Модель перерасчёта выплат (таб.6 п.4); Рассчитать начальное распределение вероятностей; Для дальнейших вычислений использовать оптимизационную модель 2: Вычислить вероятности того что выплатные документы приняты на выплату; Используя формулу рассчитать для каждого набора затраты на мероприятия по защите. Подобрать такой набор мероприятий, при которой выполняются заданные условия.	Метод управления ИБ СВО на основе комплекса оптимизационных моделей (п.2.1). Метод обоснования мероприятий ИБ СВО по критерию минимума интегральных потерь на заданном интервале времени (п.2.3). Оптимизационная модель 2 периода пересмотра мероприятий (п.2.2). Модель защищаемого процесса СВО – Модель перерасчёта выплат (таб.6 п.4). Метод определения начальных состояний (п.2.4)
3	Оценка защищённости. В каких областях необходимы мероприятия ИБ?	Необходимо привести систему защиты в соответствие. Согласно аудиту, проводившемуся в прошлом квартале были обнаружены крупные нарушения в приёме документов от других организации.	Оценить защищённость системы передачи данных к существующим атакам	Осуществить синтез программ на заданном множестве условий. В качестве базовых использовать Модели типовых нарушений (таб.2); Рассчитать начальное распределение вероятностей, используя соответствующий метод;	Метод управления ИБ СВО на основе комплекса оптимизационных моделей (п.2.1). Метод обоснования мероприятий ИБ СВО по критерию минимума

				Для дальнейших вычислений использовать оптимизационную модель 5: Рассчитать вероятности реализации каждого из видов атак.	интегральных потерь на заданном интервале времени (п.2.3). Модели типовых нарушений (таб.7). Метод определения начальных состояний (п.2.4)
4	Оценка ценности ЗИР.	Необходимо произвести оценку ценности передаваемого в руки СВО информационного ресурса. Эта информация используется в процессе назначения пенсии при принятии решения	Необходимо произвести оценку ценности ресурса для подпроцесса принятия решения.	Использовать в качестве графа состояний и систем диф. уравнений данные для Модели принятия решения (таб.6 п.3); Рассчитать начальное распределение вероятностей; Для дальнейших вычислений использовать Модель оценки ценности защищаемого ресурса (36), (33) или (35). Вычислить вероятность принятия корректного решения для обоих случаев; Вычислить коэффициент приведения расхода ресурса к единицам измерения конечных эффектов. Рассчитать разницу.	Метод управления ИБ СВО на основе комплекса оптимизационных моделей (п.2.1). Модель оценки ценности защищаемого ресурса (36), (33) или (35). Модель защищаемого процесса СВО – Модель принятия решения (таб.6 п.3). Метод определения начальных состояний (п.2.4)
5	Максимальная безопасность при ограничении на ресурсы.	Необходимо составить план мероприятий и план по закупке СЗИ на следующий год. Для отдела по защите выделен ограниченный набор ресурсов. Необходимо так максимально эффективно ими распорядиться, чтобы обеспечить максимально возможный уровень безопасности, ограничиваясь только выделенными ресурсами.	Вычислить набор мероприятий, при котором будет обеспечиваться максимальная вероятность безопасности системы в следующие 12 месяцев при затратах на защиту информации не более заданной суммы.	Осуществить синтез программ на заданном множестве условий; Составить граф состояний защищаемой системы для каждого из них; Составить системы диф. или интегральных уравнений; Рассчитать начальное распределение вероятностей; Вычислить вероятности положительного исхода процесса либо вероятности деструктивных процессов; Используя формулу рассчитать для каждого набора затраты на мероприятия по защите. Подобрать такой набор мероприятий, при которой выполняются заданные условия.	Метод управления ИБ СВО на основе комплекса оптимизационных моделей (п.2.1). Метод обоснования мероприятий ИБ СВО по критерию минимума интегральных потерь на заданном интервале времени (п.2.3). Оптимизационная модель 4 периода пересмотра мероприятий (п.2.2). Метод определения начальных состояний (п.2.4)
6	Оценка эффективности мероприятий, либо закупленных СЗИ.	Обосновать необходимость мероприятий по защите их эффективностью. Где под эффективностью понимают минимум интегральных потерь. Т.е. минимум затрат на сами мероприятия и минимум затрат на восстановление системы. Таким образом принятые мероприятия по защите должны обеспечивать состояние безопасности с вероятностью не менее 80%.	Вычислить для заданного набора мероприятий максим.разницу между затратами на защиту и возможным ущербом. Отдельно высчитать минимально и максимально возможный ущерб.	Составить граф состояний защищаемого процесса для заданного набора мероприятий и системы диф. уравнений; в качестве базовых использовать Модель выплаты пенсии (таб.6, п. 5); Рассчитать начальное распределение вероятностей; Для дальнейших вычислений использовать оптимизационную модель 6. Вычислить вероятности деструктивных процессов; Используя формулу рассчитать затраты на мероприятия по защите и возможный ущерб. Рассчитать разницу.	Метод управления ИБ СВО на основе комплекса оптимизационных моделей (п.2.1). Оптимизационная модель 6 периода пересмотра мероприятий (п.2.2). Модель защищаемого процесса СВО – Модель выплаты пенсии (таб.6 п.5). Метод определения начальных состояний (п.2.4)

Однако автоматизации одних только расчётов, как было замечено в предыдущем параграфе, недостаточно для практикующего специалиста. Для его удобства, в частности, можно автоматизировать следующие процессы:

– моделирование защищаемого процесса на основе входных данных (составление графа состояний);

– составление системы дифференциальных уравнений на основе графа;

– решение системы дифференциальных уравнений исходя из заданных для поиска параметров;

– вычисление попутно других интересующих данных;

– на основе полученных расчётов выработка соответствующих рекомендаций.

Кроме того, для полной автоматизации процесса (которая возможна при полноценном внедрении и успешной работе сопутствующего комплекса программных средств) может быть реализованы следующие функции:

– определение области действия запроса;

– выделение ключевых и критичных узлов и особенностей области моделирования;

– определение дополнительных данных, которые могут быть полезны для формирования рекомендаций;

– оценка полноты полученных данных;

– определение набора недостающих входных данных;

– оценивает адекватность имеющихся данных и поставленной задачи.

Как было замечено, этот функционал должен быть интегрирован в существующий комплекс программных средств управления ИБ СВО. Можно сделать следующие заключения о связи метода управления ИБ на основе комплекса оптимизационных моделей (рисунок 2) с представленной архитектурой комплекса инструментов управления ИБ (рисунок 12):

– средства сбора и обработки данных – 1, 2 этапы алгоритма;

– средства моделирования реализуют этапы 3, 6, 7 алгоритма;

– средства расчёта и анализа, используя выработанные модели, анализируют работу системы и прогнозируют как она будет развиваться в будущем. Эти средства реализуют 4, 5, 8 этапы алгоритма;

– средства принятия решений реализуют 9-11 и 13 этапы алгоритма;

– средства формулировки политик и средства управления СЗИ – 12 шаг алгоритма.

Очевидно, что средства визуализации, осуществляющие взаимодействие со специалистом, выходят за рамки метода.

Следует отметить, что автоматизация таких этапов метода как: сбор данных и применение на практике набора защитных мер (первый, второй и последний шаги) может быть осуществлена на должном уровне уже существующими на сегодняшний день инструментами и потому не будет рассматриваться в дальнейшем.

Как было замечено в предыдущем параграфе, из всех модулей комплекса инструментов управления ИБ выделяются средства моделирования, анализа и принятия решений. Этот класс средств в настоящий момент наиболее остро нуждается в усовершенствовании научно-теоретической базы. Предлагается модифицировать три блока из представленной выше архитектуры с использованием метода управления ИБ на основе комплекса оптимизационных моделей.

Рассмотрим предлагаемый вариант модификации модулей моделирования, расчёта, анализа и принятия решений с использованием метода управления ИБ на основе комплекса оптимизационных моделей. В совокупности они будут представлять собой систему обоснования мероприятий, схема реализации которой представлена на рисунке 13.

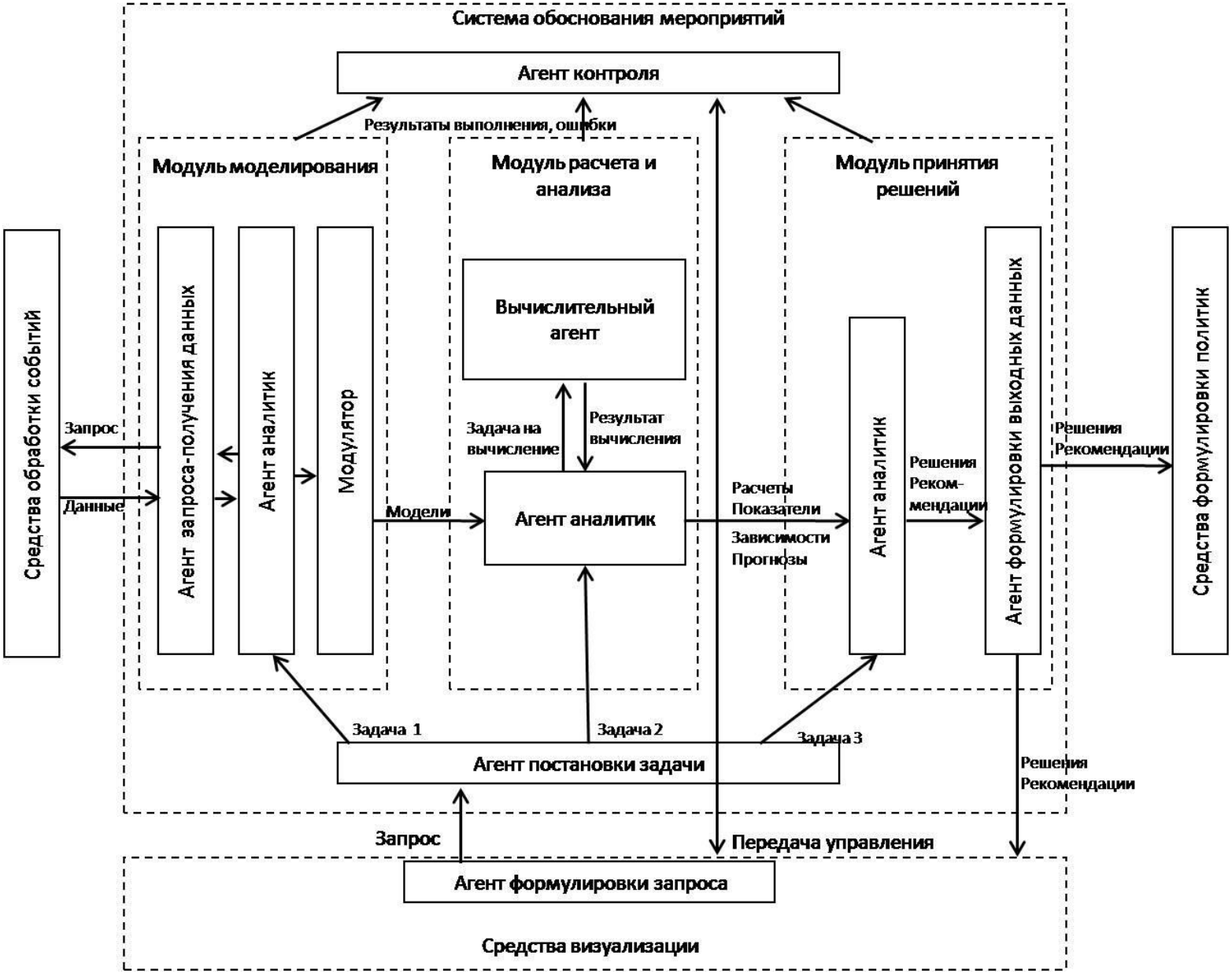


Рисунок 13 – Схема реализации системы обоснования мероприятий ИБ

Система должна состоять из нескольких модулей и агентов, каждый из которых выполняет свой функционал и нацелен на автоматизацию определённых моментов в работе специалиста ИБ.

Агент формулировки поискового запроса осуществляет взаимодействие со специалистом, желающим получить ответ на интересующий вопрос. Этот агент должен вычленить из поискового запроса все условия и ограничения, заданные специалистом, формализовать заданные ограничения поиска и условия оптимальности, осуществить их перевод в математический вид и передать в таком виде запрос Агенту постановки задачи. Поскольку поисковой запрос содержит лишь условия и ограничения, интересующие специалиста, для формулировки поисковой задачи не хватает исходных данных, на которых этот запрос следует выполнить.

Агент постановки задачи анализирует поисковый запрос, определяет область действия запроса, определяет: какие дополнительные данные могут быть полезны для формирования рекомендаций, формулирует задачу в развёрнутом виде, разделяет её на несколько отдельных подзадач для каждого из модулей и направляет им.

Агент-аналитик модуля моделирования принимает задачу, определяет набор недостающих входных данных и при необходимости направляет его агенту запроса-получения данных, а также оценивает полноту полученных этим агентом данных и отличия от уже имеющихся и при необходимости передаёт результаты Агенту контроля, выделяет ключевые и критичные узлы, особенности области моделирования, передаёт в Модулятор модифицированную задачу и исходные данные.

Модуль запроса-получения данных осуществляет взаимодействие со средствами обработки событий – направляет соответствующие запросы, принимает ответы и передаёт их аналитику.

Модулятор – собирает на основе исходных данных и поставленной задачи все необходимые для решения задачи модели и их альтернативные комбинации в

виде графов состояний, готовые модели передаёт Агенту-аналитику модуля расчёта и анализа.

Агент-аналитик модуля расчёта и анализа принимает задачу от Агента постановки задачи и готовые модели от Модулятора, оценивает адекватность имеющихся данных и поставленной задачи, при необходимости передаёт результаты Агенту контроля, разбивает общую задачу на модули задач на вычисление и ставит их по очереди перед Вычислительным агентом, получает результаты вычислений, анализирует на адекватность, при необходимости переформулирует задачи на вычисление, преобразует результаты вычислений и передаёт их Агенту аналитику модуля принятия решений.

Вычислительный агент осуществляет необходимые расчёты в полном соответствии с поставленной задачей и передаёт Агенту-аналитику результаты вычислений, а также промежуточные и дополнительные данные, указанные Агентом формулировки задачи.

Агент-аналитик модуля принятия решений должен обработать все полученные данные - осуществить поиск и сравнение экстремума основного показателя эффективности (целевой функции) для каждого из альтернативных наборов мероприятий, удовлетворяющего всем условиям задачи и ответить на поставленный вопрос, а также по возможности предоставить дополнительные рекомендации. Выходными данными могу быть как конкретное решение, возможные варианты решений, в том числе сформулированные вербально, рекомендации либо уточнения по реализации тот или иного мероприятия, а также интересующие показатели, цифры и графики, в зависимости от поставленного вопроса. При необходимости передаёт результаты Агенту контроля.

Агент формулировки выходных данных – принятые решения и рекомендации формулируются вербально и математически для передачи специалисту при помощи средств визуализации, а также формулируются в соответствии с заданными форматами для средств формулировки политик.

Агент контроля - осуществляет общее руководство и контроль выполнения поискового запроса, отслеживает этапы прохождения процесса, возникающие

ошибки и при необходимости передаёт управление процессом специалисту при помощи средств визуализации.

Таким образом, представленный в работе метод обоснования мероприятий ИБ может быть использован для усовершенствования комплекса существующих программных средств.

Требования к такой модификации и возможная структура системы обоснования мероприятий ИБ СВО в рамках комплекса уже существующих средств может быть использована специалистами при автоматизации работы специалиста ИБ СВО, при создании технических заданий и при разработке подобных комплексов и систем.

4.4. Предложения по совершенствованию организации информационной безопасности социально-важных объектов

В целом анализ предыдущих глав позволяет сформулировать следующие предложения по совершенствованию организации ИБ СВО. *Что касается развития нормативно-правовой базы* обеспечения ИБ СВО – в настоящее время она представляет собой слияние и наследие принципов и способов ИБ, используемых при обеспечении государственной безопасности. В текущей методической базе необходим баланс между организационными и техническими мерами. Зачастую хорошо проработана техническая часть при отсутствии поддерживающих, дублирующих и компенсирующих организационно-правовых мер. Поставленные задачи ИБ СВО не работают на опережение, необходима разработка мер превентивного предотвращения угроз безопасности, а также этап пересмотра существующих и обоснование новых мероприятий. Главный недостаток текущего положения – это отсутствие комплексного подхода, что может приводит к появлению «дыр» в системе защиты, утечкам защищаемой информации и к нарушению непрерывности (останову) основных производственных процессов. Необходимо составить общее представление, о том, какой должна быть эта система.

В целях повышения осведомлённости в вопросах информационной безопасности для рядовых сотрудников органов ПФР были разработаны Лекционные материалы по теме: «Информационная безопасность в АИС ПФР – 2 Пенсионного фонда Российской Федерации» [148], которые могут быть использованы как для свободного ознакомления, так и для проведения лекций специалистами подразделения по защите информации. Основной целью учебных материалов является ознакомление слушателей с системой информационной безопасности в Пенсионном фонде Российской Федерации. Эти материалы могут быть также использованы на курсах повышения квалификации, а также для обучения студентов и аспирантов по УГНС 10.00.00 - Информационная безопасность.

Разработка отраслевого стандарта также значительно продвинула бы развитие ИБ СВО и этот вопрос по вышеуказанным причинам требует активного участия со стороны государства и поддержки профессионального сообщества.

Рекомендации в области оценки рисков ИБ СВО. В каких случаях ресурс имеет высокую ценность для СВО? Либо его использование позволяет получить эффект, покрывающий расходы на добывание и содержание ресурса и при этом превышающий эффект, полученный без использования этого ресурса. И второй вариант – затраты на получение эффекта с использованием ресурса должны быть настолько малы, что вместе с расходами на добывание и содержание ресурса должны быть ниже расходов на добывание такого же эффекта без этого ресурса. Ну и всегда надо помнить о «тонких» моментах, связанных с учётом последствий нарушения режима ИБ. Как правило, имеются экономические и неэкономические аспекты (например, аспекты, связанные с разглашением персональной информации или потерей репутации организации), которые следует приводить (отображать) в денежные шкалы.

Поскольку, как уже было сказано в первой главе, для СВО понимание «информационной безопасности» подразумевает защиту интересов населения, т.е. обеспечение безопасности всех субъектов услуг СВО и их прав при выполнении процесса, и здесь ущерб рассчитывается не по отношению в СВО, а по отношению

к его клиентам. Таким образом, для типового делового процесса «Назначение и выплата пенсии» ущерб от останова для любого гражданина, имеющего право на пенсию, будет укладываться как минимум в сумму неполученной выплаты, а как максимум будет включать в себя моральный ущерб, который может быть причинён как нарушением непрерывности процесса и не точностью оценки пенсионных прав, так и нарушением конфиденциальности персональных данных. Плюс для СВО нарушение этого процесса повлечёт ряд штрафных санкций, наложенных государством в ответ на понесённые им репутационные риски, размер которых ограничен КоАП.

В интересах практической реализации этих рекомендаций был выработан следующий документ – Методические рекомендации по оценке безопасности в территориальных органах ПФР Республики Коми [149]. Эти рекомендации предназначены для специалистов подразделений по защите информации и информационной безопасности Отделений ПФР и могут быть также использованы на курсах повышения квалификации, обучения студентов и аспирантов по УГНС 10.00.00 - Информационная безопасность.

В этом документе сформулирован подход ОПФР по Республике Коми (далее - Отделения) к обоснованию мероприятий по обеспечению ИБ. Подход основан на результатах исследования деятельности Отделения и существующей системы ИБ ПФР и содержат общие рекомендации к обоснованию мероприятий ИБ, алгоритм действий специалиста, готовые модели защищаемых деловых процессов Отделения, а также набор оптимизационных моделей, которые можно использовать в целях поиска и обоснования мероприятий ИБ Отделения.

Рекомендации по предотвращению типовых нарушений ИБ СВО. Атаки с подделкой документов, подаваемых в СВО на протяжении всей жизни (эффект «мёртвых душ» и нарушение аутентичности), предупредить невозможно, однако она не очень популярна из-за своей масштабности, сложности и тяжести наказания. Это нарушение внутренними мерами СВО предупредить не может.

Подделка передаваемых документов, а также подделка данных на ходе может быть исключена при полноценном вводе системы межведомственного

электронного взаимодействия, которая обеспечит выгрузку достоверных данных непосредственно из баз соответствующих ведомств и тогда остаётся только подделка документов на стороне ведомства, предоставляющего информацию для реализации государственной услуги.

Согласно расчетам при разных условиях изыскиваемые документы, находящиеся в ведомстве других организации, имеют очень большую ценность для процесса назначения пенсии. В некоторых условиях разница между вероятностями принятия к назначению корректного ВД при наличии корректных документов и в их отсутствии достигает 60% - такую решающую роль играют эти документы. Поэтому максимальное внимание предлагается уделять безопасности каналов передачи, например, на базе технологии виртуальных частных сетей, и заключать с контрагентами (поставщиками информации) соглашения о взаимном доверии, где очень подробно прописать ответственность за предоставление недостоверных сведений, таким образом, разделяя ответственность за возможные нарушения деловых процессов СВО.

Уязвимость процесса к внутренним нарушителям диктует и свой набор защитных мер. Улучшить положение можно за счёт обеспечения защиты баз данных СВО таким образом, чтобы невозможно было подделать информацию ни на одном из этапов бесконтрольно, поскольку именно состояния 2, 7, 11, 14, 20, 23 процесса назначения и выплаты пенсии (рисунок 4) являются слабым звеном системы за счёт лёгкости реализации угроз.

Несанкционированный доступ к базам данных подразумевает необходимость классификации объектов и субъектов доступа, необходимость систематизировать, отслеживать и контролировать порядок предоставления доступа к разным типам ресурсов. Таким образом, необходимо исключить пересечение прав исполнителей и контролирующих лиц, к примеру, в подсистеме выплаты пенсии угроза неправомерной корректировки сумм выплат внутренним нарушителем. Это подтверждают результаты расчетов. На заданных условиях, при сравнении наборов прав, когда права пользователей разделены в соответствии с внутренним регламентом «Назначения и выплаты пенсии» и когда предоставленные права

доступа превышают необходимы минимум для выполнения той или иной роли, минимальная вероятность некорректной выплаты наблюдается в случае разделения прав доступа с использованием ролевой модели и равна 10%.

Интересно также следующее наблюдение - при смешении прав доступа скорость прохождения проверок (корректности расчётов) в целом возрастает, но со временем количество ошибок (случаев некорректного расчёта выплат) накапливается и вероятность корректной выплаты замирает на показателе 78%. Тогда как в случае разделения прав оператора и проверяющего на более продолжительном промежутке времени вероятность корректных выплат возрастает до 90%.

В условиях очень большого разброса в подходах к организации ИБ и свободой в принятии решений на уровне регионов используемая на сегодняшний момент структура системы предоставления доступа должна обладать следующими свойствами: интегрируемость, иерархичность, универсальность, гибкость, подконтрольность и простота дальнейшего отслеживания. Более всего этим требованиям удовлетворяет иерархическая ролевая система разграничения доступа.

Управление ИБ СВО. Система ИБ СВО в настоящий момент занимается только решением постоянно возникающих проблем в оперативном режиме, чем занимает значительную часть рабочего времени специалиста по ИБ. Такая зацикленность на низкоуровневом управлении инцидентами влечёт за собой принятие беспорядочных компенсационных мер, что в дальнейшем усложняет и снижает прозрачность СОИБ, ведёт к росту неоптимальных нагрузок, снижению эффективности ИБ и, в конце концов, увеличению числа инцидентов.

К поиску и принятию мероприятий по ИБ необходим системный, стратегический подход, а значит необходим контроль эффективности и принятия мер по устранению причин отклонений от запланированного результата, анализ и внесение соответствующих изменений в планировании и распределении ресурсов ИБ. Поэтому в ближайшее время актуальнейшим вопросом станет необходимость разработки и внедрения системы управления информационной безопасностью

СВО, а значит и поиск подходящих для СВО инструментов оценки и обоснования управляющих решений по обеспечению ИБ.

В комплекс программных средств специалиста по ИБ должны быть включены:

– вариант усовершенствования систем мониторинга и журналирования, где информация не просто консолидируются и визуализируются, а предоставляет аналитическую информацию, упорядоченные и систематизированные знания о системе и её компонентах;

– класс систем, позволяющих осуществлять моделирование защищаемых процессов, ресурсов и возможных действий нарушителя, сценариев атак, а также мероприятий и системы безопасности и принятия решений;

– средства поддержки принятия решений;

– сегмент сервисов, автоматизирующих и унифицирующих управление средствами, непосредственно осуществляющих защиту информации.

Существующие на сегодняшний день СППР не в состоянии обеспечить полную автоматизацию управления ИБ, не отвечают на все интересующие специалиста вопросы, используемые ими методы моделирования и анализа ИБ устарели и не обеспечивают необходимый уровень адекватности и точности. Именно этот сегмент отвечает за обоснование мероприятий ИБ СВО и, вследствие указанных выше причин, являются наиболее перспективным для разработки. Таким образом, представленный в работе метод обоснования мероприятий ИБ может быть использован для усовершенствования таких СППР. В работе представлена архитектура такого комплекса, а также техническое задание на реализацию СППР для СОИБ СВО.

При правильном применении такая система обеспечит планомерность и стратегический подход при обосновании мероприятий ИБ, что повысит их оптимальность до максимально возможного уровня. Эти и другие представленные в работе требования к такой модификации и возможная структура системы обоснования мероприятий ИБ СВО в рамках комплекса уже существующих средств может быть использована специалистами при автоматизации работы

специалиста ИБ СВО, при создании технических заданий и при разработке подобных комплексов и систем.

В целом, существующие разработки направлены на управление системой технической защиты, в то время как предложенный метод (рисунок 2) позволяет не только давать рекомендации и управлять организационными мероприятиями по защите, выстраивать политики высокого уровня и стратегию обеспечения ИБ, но и давать рекомендации по эффективному выстраиванию защищаемых деловых процессов и построению самих объектов защиты. Таким образом, предложенные методы и модели могут быть использованы в комплексах и системах перечисленных выше типов, однако на их основе могут быть разработаны не только средства управления СЗИ, но СОИБ.

Выводы по четвертой главе

Осуществлено моделирование процессов ИБ СВО с применением предложенных методов и моделей применительно к структурам ПФР. Полученные результаты показывают, что предложенные методы и модели позволяют оперативно получать оценки, на основе которых однозначно можно выбирать наилучшие варианты обеспечения ИБ, снижать затраты ресурсов, эффективно управлять системой обеспечения ИБ.

Предложена архитектура комплекса программных средств обоснования мероприятий ИБ СВО, которая позволяет не только давать рекомендации и управлять организационными мероприятиями по защите, выстраивать политики высокого уровня и стратегию обеспечения ИБ, но и давать рекомендации по эффективному выстраиванию защищаемых деловых процессов и построению самих объектов защиты.

Разработано задание на реализацию СППР для СОИБ СВО, представляющее собой систему тестовых заданий, состоящих из входных и выходных данных. Если система пройдёт представленные тесты, можно говорить о том, что СППР настроена правильно и будет обеспечить необходимы уровень автоматизации управления ИБ СВО.

Выработаны методические рекомендации по использованию предложенных методов и моделей: представлен примерный порядок действий специалиста по ИБ, в случае, если он использует представленные методы и модели вручную; определено какие методы и модели задействуются при решении типовых задач обеспечения ИБ СВО; представлены методические рекомендации по разработке перспективной системы обоснования мероприятий ИБ СВО, и её возможная структура в рамках комплекса уже существующих средств. В интересах практической реализации этих рекомендаций предложен новый документ – Методические рекомендации по оценке безопасности в территориальных органах ПФР Республики Коми [149]

Сформулированы предложения по совершенствованию организации ИБ СВО в части развития нормативно-правовой базы, оценки рисков, предотвращения

типовых нарушений и в области управления СОИБ СВО. В их рамках разработаны лекционные материалы по теме: «Информационная безопасность в АИС ПФР – 2 Пенсионного фонда Российской Федерации» [148].

Помимо поиска баланса и повышения общего уровня безопасности ИБ СВО предложенные модели и методы могут найти применение для усовершенствования существующих и проектирования новых информационных структур ПФР, а также при разработке интеллектуальных систем управления информационной безопасностью.

ЗАКЛЮЧЕНИЕ

В результате выполненного диссертационного исследования были разработаны:

1. Метод управления ИБ СВО на основе комплекса оптимизационных моделей. Этот метод позволяет рассматривать в качестве объекта защиты не только информационную систему, а всю организацию в целом. Учитывается необходимость защиты не только информационных ресурсов, но и процессов. В рамках этого метода предложен новый комплекс оптимизационных моделей мероприятий ИБ СВО, учитывающий широкий спектр возможных ситуаций. В целях уточнения результатов моделирования, получаемых при использовании предложенного метода, разработаны новые правила определения начальных состояний, в которых система может находиться на исходный момент времени.

2. Метод обоснования мероприятий информационной безопасности по критерию минимума интегральных потерь, отличающийся от известных новой совокупностью условий, при которых предлагается обосновывать мероприятия ИБ СВО. В интересах упрощения расчётов и повышения точности и объективности, получаемых этим методом результатов была уточнена модель оценки ценности защищаемых информационных ресурсов. Предлагаемый метод ориентирован на широкий круг возможных ситуаций обеспечения ИБ, на учёт ценности ЗИР и потенциальной информированности злоумышленников на текущий момент времени. Отдельные положения метода могут быть применимы также при решении частных задач ИБ. В целом предлагаемый метод расширяет взгляды и возможности по обоснованию мероприятий ИБ в различных условиях.

3. Модели защищаемых и дезорганизующих процессов применительно к информационной безопасности социально-важных объектов. Предложен комплекс моделей защищаемых и комплекс дезорганизующих процессов СВО. Применительно к структурам ПФР модели защищаемых процессов описывают один из основных деловых процессов назначения и выплаты пенсии. Эти модели учитывают многократность санкционированных и несанкционированных действий, возможность пересмотра защитных мероприятий, а также обнаружения

и предотвращения нарушений ИБ. Комплекс моделей типовых процессов нарушения ИБ СВО позволяет моделировать большинство атак на ИБ СВО. Предложенные модели учитывают вероятные нарушения ИБ СВО. При использовании этих моделей для принятия решений обеспечивается системность вырабатываемых контрмер. Впервые проведён анализ и моделирование таких процессов ИБ применительно к органам ПФР. Впервые рассмотрены с точки зрения практикующего специалиста по ИБ и получили научную формализацию наиболее распространённые нарушения ИБ для структур ПФР. Каждая из моделей формализует закономерности, выявленные на основе обширного профессионального опыта. Все модели имеют прикладной характер.

4. Обоснованные рекомендации по повышению информационной безопасности социально-важных объектов. Среди них методические рекомендации по использованию предложенных методов и моделей. Предложен порядок действий специалиста по ИБ, в случае, если он использует разработанные методы и модели вручную. Определено какие методы и модели должны быть использованы при решении типовых задач обеспечения ИБ СВО. Представлены методические рекомендации к разработке перспективной системы обоснования мероприятий ИБ СВО и её возможная структура в рамках комплекса уже существующих средств. Эти рекомендации нашли своё применение в документе, утверждённом к использованию в территориальных органах ПФР Республики Коми [149]. Предложен комплекс программных средств обоснования мероприятий ИБ СВО, который может быть разработан на базе предложенных в настоящей работе моделей и методов. Этот комплекс вписан в архитектуру существующих инструментов управления информационной безопасностью. Кроме того, по результатам исследования было составлено задание на реализацию СППР для системы обеспечения ИБ СВО. Оно может служить в качестве инструмента оценки качества и адекватности настройки СППР ИБ СВО. В результате анализа особенностей ИБ СВО и апробации предложенных методов и моделей были выработаны практические рекомендации по совершенствованию организации информационной безопасности социально-важных объектов в части развития

нормативно-правовой базы, оценки рисков, предотвращения типовых нарушений и в области управления СОИБ СВО.

Можно говорить о том, что разработанные методы и модели позволяют оперативно обосновывать мероприятия ИБ, управлять организационными мероприятиями по защите, выстраивать политики высокого уровня и стратегию обеспечения ИБ, выдавать рекомендации по эффективному выстраиванию защищаемых деловых процессов СВО и построению самих объектов защиты.

Признанный эксперт в области информационной безопасности – компания Gartner Group выделяется четыре уровня зрелости компании с точки зрения обеспечения ИБ от нулевого до третьего [150], [151]. Таким образом, согласно Модели зрелости информационной безопасности (с англ. Information Security Maturity Model (ISMM) предлагаемые методы и модели позволяют постепенно развить и поддерживать ИБ СВО третьем (наивысшем) уровне.

Помимо поиска баланса и повышения общего уровня безопасности ИБ СВО, предложенные решения могут найти применение при проектировании новых информационных структур СВО и органов ПФР в частности, при разработке интеллектуальных систем управления информационной безопасностью.

Таким образом, можно утверждать, что цель диссертационного исследования достигнута, а поставленная на исследование научно-техническая задача решена.

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 52143-2013 Социальное обслуживание населения. Основные виды социальных услуг; Введ. 01.01.2015. – М.: Стандартинформ, 2013 -7с.

2. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения; Введ. 01.02.2008. – М.: Стандартинформ, 2008 -12с.

3. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения Введ. 01.10.2009. – М.: Стандартинформ, 2009

4. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.

5. ГОСТ Р 51897-2011/Руководство ИСО 73:2009. Национальный стандарт Российской Федерации. Менеджмент риска. Термины и определения; Введ. 01.12.2012 - М.:Стандартинформ, 2012 -26 с.

6. ГОСТ Р ИСО/МЭК 27001—2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. –Взамен ГОСТ Р ИСО/МЭК 17799—2005; Введ. 27.12.2006 - М, 2008 -26 с. (ISO/IEC 27001:2005 «Information technology — Security techniques — Information security management systems — Requirements»).

7. ГОСТ Р ИСО/МЭК 13335-1 – 2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий; Введ. 01.06.2007. – М.: Стандартинформ, 2006 -23с.

8. Федеральный закон Российской Федерации «О государственной социальной помощи» N 178-ФЗ от 17.07.1999.

9. Федеральный закон Российской Федерации «Об основах обязательного социального страхования» N 165-ФЗ от от 16.07.1999.

10. Федеральный закон Российской Федерации «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 17.07.2006

11. Федеральный закон Российской Федерации «О коммерческой тайне», № 98-ФЗ от 29.07.2004 г.

12. Федеральный закон Российской Федерации «О персональных данных», № 152-ФЗ от 27.07.2006.

13. Gallagher B.P. Interpreting Capability Maturity Model Integration (CMMI) for Operational Organizations // Technical Note CMU/SEI-2002-TN-006 by Carnegie Mellon University April 2002, 35 pp.

14. Носаль И.А. Особенности обеспечения информационной безопасности социально важных объектов // Перспективные информационные технологии (ПИТ 2014): Сб. научн. тр. Международной научно-практической конф.(г. Самара, 30 июня – 4 июля 2014г.). Самара: Издательство Самарского научного центра РАН, 2014. С.224-227.

15. Евдокимова А. АИС – технологическая азбука ПФР // «Я работаю в ПФР». 2012. № 10/40. С. 1-2.

16. Бондарева Н. Основная программа по администрированию // «Я работаю в ПФР». 2011. № 10/10. С. 4.

17. Фазлутдинова Э. Сплошной мониторинг // «Я работаю в ПФР». 2013. № 4/50. С. 4.

18. Бондарева Н. Владельцы ситуации // «Я работаю в ПФР». 2011. № 3/3. С. 3.

19. Губка О. Создание централизованной БД прав доступа как способ снизить риски ИБ // Защита информации. Инсайд. 2014 №4. С.56-57.

20. ГОСТ Р 52448-2005 «Обеспечение безопасности сетей электросвязи. Общие положения» Введ. 01.01.2007. – М.: Стандартинформ, 2008 -15с.

21. Носаль И.А. Потенциал нападения и типовая модель нарушителя // Информационная безопасность и защита персональных данных: Проблемы и пути их решения: материалы VI Межрегиональной научно-практической конф.(г. Брянск, 28 апреля 2014г.). Брянск: Издательство БГТУ, 2014. С.96-101.

22. Осипов В.Ю., Юсупов Р.М., Информационный вандализм, криминал и терроризм как современные угрозы обществу // Труды СПИИРАН, 2009, выпуск 8, 34–45

23. Мартин Дж. Вычислительные сети и распределённая обработка данных. Программное обеспечение, методы и архитектура / Пер. с англ. М.: Финансы и статистика, 1986

24. Managing CRAMM Reviews Using PRINCE. Central Computer & Telecommunications Agency (UK) // Publisher: Stationery Office Books, November 1993, 140 pages. - Режим доступа: - http://www.cramm.com/files/techpapers/Managing%20CRAMM%20Reviews%20Using%20Prince.pdf. (дата обращения: 12.05.2013).

25. Peltier T.R. Information Security Risk Analysis // Boca Raton, FL: Auerbach publications; 1 edition, 31.01.2001, 296 pages.

26. Alberts C., Dorofee A. Managing Information Security Risks: The OCTAVE (SM) Approach // Publisher: Addison-Wesley (E); 1 edition, Juli 2002, 470 pages.

27. Storms A. Using vulnerability assessment tools to develop an OCTAVE Risk Profile // GIAC GSEC Practical (v1.4b) December 03, 2003.

28. RiskWatch users manual // Режим доступа: - http://www.riskwatch.com. (дата обращения: 12.05.2013).

29. Александрович Г.Я., Нестеров С.А., Петренко С.А. Автоматизация оценки информационных рисков компании // Защита информации.Конфидент. 2003, № 2. С.78-81

30. Chaplin M., Creasey J. Information Security Forum. Standard of Good Practice (ISF ―SoGP) The Standart for Information Security // Published by Information Security Forum Limited, June 2011, 282 pages. – Режим доступа: http://www.securityforum.org. (дата обращения: 12.05.2013).

31. Нестеров С.А. Анализ и управление рисками в информационных системах на базе операционных систем Microsoft // Режим доступа: - http://www.intuit.ru/department/itmngt/riskanms. (дата обращения: 22.04.2014).

32. Security Risk Management Guide // Published: October 15, 2004|Updated: March 15, 2006. Режим доступа: - http://technet.microsoft.com/en-us/library/cc163143.aspx. (дата обращения: 22.04.2014).

33. Shostack A. Reinvigorate your Threat Modeling Process // MSDN Magazine, July 2008. Режим доступа: https://msdn.microsoft.com/en-us/magazine/cc700352.aspx. (дата обращения: 22.04.2014).

34. ГОСТ Р ИСО/МЭК ТО 13335-3 – 2007 Руководство по управлению безопасностью информационных технологий. Часть 3. Методы управления безопасностью информационных технологий; Введ. 01.09.2007. – М.: Стандартинформ, 2006 -49с.

35. Корт С.С. Теоретические основы защиты информации: Учебное пособие. – М.: Гелиос АРВ, 2004. – 240 с.

36. Digital Security. Алгоритм: модель анализа угроз и уязвимостей // Режим доступа: - http:www.dsec.ru (дата обращения: 22.04.2014).

37. Open Web Application Security Project, OWASP Top Ten 2010 // Режим доступа: - http://www.owasp.org/ (дата обращения: 22.04.2014).

38. Trike v.1 Methodology Document. Saitta P., Larcom B., Eddington M.; (13.07.2005) // Режим доступа: - http://www.net-security.org/dl/articles/Trike_v1_Methodology_Document-draft.pdf. (дата обращения: 22.04.2014).

39. Oladimeji E.A., Supakkul S., Chung L. Security threat modeling and analysis: a goal-oriented approach // Режим доступа: - http://citeseerx.ist.psu.edu/ viewdoc/download?doi=10.1.1.103.2997&rep=rep1&type=pdf. (дата обращения: 12.05.2013).

40. Williams L., Lippmann R., Ingols K. GARNET: A graphical attack graph and reachabiity network evaluation tool in Visualization for Computer Security (VizSEC) // ser. Lecture Notes in Computer Science, J.R. Goodall, G.J. Conti, and K.-L. Ma, Eds. - Springer, 2008. - Vol. 5210. - P. 44-59.

41. Wang L., Yao C., Singhal A., Jajodia S. Implementing interactive analysis of attack graphs using relational databases // Journal of Computer Security. 2008. N 16. P. 419–437.

42. Moore A., Ellison R., Linger R. Attack Modeling for Information Security and Survivability // Software Engineering Institute, Technical Note CMU/SEI-2001-TN-01, March 2001.

43. Бешелев С.Д. Математико-статистические методы экспертных оценок.- М.: Статистика, 1974. 159 с.

44. Трояков И.Б. Методы оценки информационной безопасности предприятия на основе процессного подхода:дис. канд. техн. наук. – Санкт-Петербург, 2010. – 134 с.

45. Ажмухамедов И.М., Ханжина Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник АГТУ. 2011. №1. С.185-190.

46. Миронов В.В., Носаль И.А. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–216.

47. Молдованин Т.В. Решение задачи выбора оптимального варианта комплексной защиты информации с помощью метода экспертного оценивания // Информационно-управляющие системы. 2007. №3. С. 39 – 44.

48. Домарев В.В. Безопасность информационных технологий. Системный подход // Киев: ООО ТИД «Диасофт», 2004. -992 с. Режим доступа: http://www.security.ukrnet.net/d-book-2/ch_06.pdf. (дата обращения: 12.05.2013).

49. Заболотский В.П., Юсупов Р.М. Применение метода индексов для оценивания эффективности защиты информации // Труды СПИИРАН. Вып.3, т.2. — СПб.: Наука, 2006.

50. Карпеев Д.О. Исследование и развитие методического обеспечения оценки и управления рисками информационных систем на основе интересо-ориентированного подхода: дис. канд. техн. наук. – Воронеж, 2009. – 171 с.

51. Корнилова А.Ю., Палей Т.Ф. Проблемы применения методов экспертных оценок в процессе экономического прогнозирования развития предприятия // Проблемы современной экономики. 2010. № 3 (35).

52. Ефимов Е.И. Возможность применения существующих средств анализа рисков в системах принятия решений с привлечением экспертов // Омский научный вестник. 2011. № 3-103. С.281-284.

53. Schneier B. Attack Trees. – Dr. Dobb`s Journal, v. 24, n. 12, Dec 1999, pp. 21-29.

54. Burgess M., Canright G., Engo-Monsen K. A graph-theoretical model of computer security // International Journal of Information Security. 2004. N 3. P. 70-85.

55. Dewri R., Ray I., Poolsappasit N., Whitley D. Optimal security hardening on attack tree models of networks: a cost-benefit analysis // International Journal of Information Security. 2012. N 11. P. 167-188.

56. Мальцев Г.Н., Теличко В.В. Оптимизация состава средств защиты информации в информационно-управляющей системе с каналами беспроводного доступа на основе графа реализации угроз // Информационно-управляющие системы. 2008. №4. С. 29 – 33.

57. Аграновский А.В., Хади Р.А., Фомченко В.Н., Мартынов А.П., Снапков В.А. Теоретико-графовый подход к анализу рисков в вычислительных сетях // Конфидент. Защита информации. 2002. № 2. С.50-53.

58. Абрамов Е.С., Кобилев М.А., Крамаров Л.С., Мордвин Д.В. Использование графа атак для автоматизированного расчета мер противодействия угрозам информационной безопасности сети // Известия ЮФУ. Технические науки. 2014. №2(151). С.92-100.

59. Аверченков В. И., Рытов М. Ю., Гайнулин Т. Р., Голембиовская О.М. Формализация выбора решения при проектировании комплексных систем защиты информации от несанкционированного доступа // Известия Волгоградского государственного технического университета.-Волгоград: ВолГТУ. 2011. №11(84). С.131-136.

60. Козленко А.В., Авраменко В.С., Саенко И.Б., Кий А.В. Метод оценки уровня защиты информации от НСД в компьютерных сетях на основе графа защищённости // Труды СПИИРАН. 2012. №21. С.41–55.

61. Кудрявцева Р.Т. Управление информационными рисками с использованием технологий когнитивного моделирования: автореф. дис. канд. техн. наук. – Уфа, 2008. – 17 с.

62. Ажмухамедов И.М. Анализ и управление комплексной безопасностью на основе когнитивного моделирования // Управление большими системами: сборник трудов. 2010. № 29. С.5-15.

63. Рытов М.Ю., Рудановский М.В. Управление безопасностью информационных технологий на основе методов когнитивного моделирования // Информационная безопасность. 2010. №4. С.579-582.

64. Чусавитин М.О. Использование метода анализа иерархий при оценке рисков информационной безопасности образовательного учреждения // Фундаментальные исследования. 2013. № 10. С.2080-2084.

65. Бикмаева Е.В., Баженов Р.И. Об оптимальном выборе системы защиты информации от несанкционированного доступа // Электронный научный журнал «APRIORI. Серия: Естественные и технические науки». 2014. №6. С. 5-16.

66. Куземко С.М., Мельничук В.М. Усовершенствованный метод анализа иерархий для выбора оптимальной системы защиты информации в компьютерных сетях // Наукові праці Вінницького національного технічного університету. 2010. № 2. Режим доступа: - http://praci.vntu.edu.ua/article/view/1253/592 (дата обращения: 10.01.2015).

67. Данилюк С.Г., Маслов В.Г. Обоснование нечёткого ситуационного подхода к созданию модели системы защиты информации с использованием ложных информационных объектов // Известия Южного федерального университета. Технические науки. 2008. № 8. т.85. С.36-41.

68. Борзенкова С.Ю., Чечуга О.В. Модель принятия решения при управлении системой защиты информации // Известия Тульского государственного университета. Технические науки. 2013. № 3. С. 471-478.

69. Круглов В.В., Дли М.И., Голунов Р.Ю. Нечёткая логика и искусственные нейронные сети. М.: Физматлит. 2001. 221с.

70. Васильев В.И., Савина И.А., Шарипова И.И. Построение нечётких когнитивных карт для анализа и управления информационными рисками вуза // Вестник УГАТУ. 2008. №2. т.10. С.199-209.

71. Sodiya A.S., Onashoga S.A., Oladunjoye B.A. Threat Modeling Using Fuzzy Logic Paradigm // Issues in Informing Science and Information Technology. 2007. Volume 4.

72. Чечулин А.А. Методика оперативного построения, модификации и анализа деревьев атак // Труды СПИИРАН. №3(26). – СПб: Наука, 2013. С.40-553.

73. Ingle M., Atique M., Dahad S.O. Risk analysis using fuzzy logic // International Journal of Advanced Engineering Technology. 2011. Vol.II, Issue III. P.96-99

74. Shang K., Hossen Z. Applying Fuzzy Logic to Risk Assessment and Decision-Making // Report of Casualty Actuarial Society, Canadian Institute of Actuaries, 2013. pp.59. Режим доступа: - http://www.cia-ica.ca/publications/publication-details/213102. (дата обращения: 20.03.2011).

75. Маслобоев А.В. Путилов В.А. Разработка и реализация механизмов управления информационной безопасностью мобильных агентов в распределённых мультиагентных информационных системах // Вестник Мурманского государственного технического университета. 2010. № 4-2, т.13. С.

76. Файзуллин Р.Р., Васильев В.И. Метод оценки защищённости сети передачи данных в системе мониторинга и управления событиями информационной безопасности на основе нечёткой логики // Вестник УГАТУ. 2013. №2 (55). С.150-156.

77. Котенко И.В., Нестерук Ф.Г., Шоров А.В. Гибридная адаптивная система защиты информации на основе биометафор «нервных» и нейронных сетей // Инновации в науке. 2013. №16-1. С.79-83.

78. Котенко И.В., Шоров А.В., Нестерук Ф.Г. Анализ биоинспирированных подходов для защиты компьютерных систем и сетей // Труды СПИИРАН. Вып.3 (18). СПб.: Наука, 2011. С. 19-73.

79. Котенко И.В., Уланов А.В. Команды агентов в кибер-пространстве, моделирование процессов защиты информации в глобальном Интернете // Труды

института системного анализа РАН. Проблемы управления кибербезопасностъю информационного общества. М: КомКнига, 2006. Т. 27. С. 108–129.

80. Sun L., Srivastava R.P., Mock T.J. An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions // Journal of Management Information Systems. Vol. 22. N 4. Spring 2006. pp.109-142.

81. Арьков П.А. Комплекс моделей для поиска оптимального проекта системы защиты информации // Известия Южного федерального университета. Технические науки. 2008. № 8. т. 85. С. 30-36.

82. Вахний Т.В., Гуц А.К. Теоретико-игровой подход к выбору оптимальных стратегий защиты информационных ресурсов // Математические структуры и моделирование. 2009. № 1 (19). С. 104-107.

83. Белый А.Ф. Компьютерные игры для выбора методов и средств защиты информации в автоматизированных системах // Известия Южного федерального университета. Технические науки. 2008 № 8. т.85. С. 172-176.

84. Шлыков Г.Н. Применение гомоморфизма в моделях защиты информации // Вестник удмуртского университета. 2011. № 4. С. 175-179.

85. Меньших В.В., Петрова Е.В. Теоретическое обоснование и синтез математической модели защищённой информационной системы ОВД как сети автоматов // Вестник Воронежского института МВД России. 2010. № 3. С.134 – 142.

86. Ерохин С.С. Голубев С.В. Оценка защищённости информационных систем с использованием скрытых Марковских процессов // Научная сессия ТУСУР 2007: Материалы докладов Всероссийской научно-технической конференции студентов, аспирантов и молодых ученных. Томск. 4-7 мая 2007 г. № 42. С.133-137.

87. Росенко А.П. Применение марковских случайных процессов с дискретным параметром для оценки уровня информационной безопасности // Известия Южного федерального университета. Технические науки. 2009. № 11. С.169-172.

88. Каштанов В.А., Зайцева О.Б. О минимаксных подходах в задачах безопасности // Труды Карельского научного центра Российской академии наук. 2013. № 1. С.55-67.

89. Иванов К.В., Тутубалин П.И. Марковские модели средств защиты автоматизированных систем специального назначения:монография. – Казань: ГБУ «Республиканский центр мониторинга качества образования», 2012. -2016 с.

90. Попов С.В., Шамкин В.Н. Определение вероятностей состояний функционирования средства контентного анализа как элемента системы мониторинга инцидентов информационной безопасности // Вестник ТГТУ. 2012. №1. С.27-37.

91. Росенко А.П. Внутренние угрозы безопасности конфиденциальной информации: Методология и теоретическое исследование:монография - М: Красанд, 2010. -160 с.

92. Осипов В.Ю., Ильин А.П., Фролов В.П., Кондратюк А.П. Радиоэлектронная борьба. Теоретические основы. Учеб. пособие для вузов. – Петродворец: ВМИРЭ, 2006. – 302 с.

93. Окрачков А.А., Фирюлин М.Е. Метод аппроксимации распределения времени реализации защитных функций системой защиты информации от несанкционированного доступа // Вестник ВИ МВД России. 2012. №4. С.123-131.

94. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации», утверждено решением председателя Гостехкомсии от 30.03.1992.

95. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа. Показатели защищённости от несанкционированного доступа к информации», утверждено решением председателя Гостехкомиссии от 30.03.1992.

96. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждена зам.директора ФСТЭК России от 14.02.2008.

97. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены руководством 8 Центра ФСБ России 21.02. 2008 № 149/54-144.

98. Приказ ФСТЭК России «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 г. N 21.

99. Приказ ФСТЭК России «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 11 февраля 2013 г. № 17.

100. Положение Центрального Банка Российской Федерации «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» от 09.06.2012 № 382-П.

101. Постановление Правительства Российской Федерации «Об утверждении Положения о защите информации в платёжной системе» от 13.06.2012 № 584.

102. Payment Card Industry Data Security Standard (PCI DSS) – PCI Security Standards Council LLC, Version 2.0. Oct. 2010. 75 p. // Режим доступа: - https://www.pcisecuritystandards.org/documents. (дата обращения: 01.07.2013).

103. Стандарт Банка России СТО БР ИББС-1.0-2010 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. – Взамен СТО БР ИББСС-1.0-2008; Введён 21.06.2010. – М.: 2010. 42 с.

104. Стандарт Банка России СТО БР ИББС-1.2-2009 Обеспечение информационной безопасности организаций банковской системы Российской

Федерации. Методика оценки соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0-2008; Введён. 01.07.2009. – М, 2009 -56 с.

105. ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement 07.12.2009, 55 page.

106. ISO/FDIS 31000:2009(E) “Risk management — Principles and guidelines”

107. IEC/FDIS 31010:2009(E) “Risk management — Risk assessment techniques”

108. An Introduction to the Business Model for Information Security by Introduction Information Systems Audit and Control Association (ISACA). Jan 2009. // Режим доступа: - http://www.isaca.org/ContentManagement/ContentDisplay.cfm?ContentID =48017. (дата обращения: 18.12.2013).

109. Control Objectives for Information and related Technology (COBIT) 5 for Information Security. Printed in the United States of America, 2015. - 208 p.

110. Aceituno V. Information security management maturity model (ISM3) v2.10/Stansfeld E. – ISM3 Consortium, 2007. Режим доступа: - http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf. (дата обращения: 18.12.2013).

111. BSI- Standard 100 - 1: Information Security Management Systems (ISMS) by Bundesamt für Sicherheit in der Informationstechnik (BSI); 2008 – 38 p.

112. BSI- Standard 100 - 3: Risk analysis based on IT – Grundschutz by Bundesamt für Sicherheit in der Informationstechnik (BSI); 2008 – 23 p.

113. National Institute of Standards and Technology Special Publication 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations // April 2013, 462 p.

114. Instruction Committee on National Security Systems revised // National Information Assurance Glossary (CNSS-4009). № 4009. June 2006. Режим доступа: - www.cnss.gov. Дата последнего доступа 12.05.2010

115. Воробьев В.И., Петров М.Ю., Шкиртиль В.И. Моделирование многомасштабных процессов на кластерных структурах // Информационно-измерительные и управляющие системы. 2013. № 9. т.11. С.43–48.

116. Синещук Ю.И., Филиппов А.Г., Терехин С.Н., Николаев Д.В., Саенко И.Б. Структурно-логический метод анализа безопасности потенциально опасных объектов // Труды СПИИРАН. №17 – СПб.: Наука, 2011. С.55–69.

117. Петренко С.А., Попов Ю.И. Оценка затрат на информационную безопасность // Конфидент. 2003. №1(49). С.68-73.

118. Обухов А.А. Диагностика необходимости инвестирования в безопасность в современном предпринимательстве и формирование на ее основе рекомендаций // Вестник Омского университета. Серия «Экономика». 2013. №3. С. 78-84.

119. Авраменко В.С., Козленко А.В. Модель для количественной оценки защищённости информации от НСД в АС по комплексному показателю // Труды СПИИРАН. № 2(13). – СПб.: Наука, 2010. С.172-181.

120. Ажмухамедов И.М., Ханжина Т.Б. Оценка экономической эффективности мер по обеспечению информационной безопасности // Вестник АГТУ. 2011. № 1 С.185-190.

121. Бирюков Д.Н., Ломако А.Г. Подход к построению системы предотвращения киберугроз // Проблемы информационной безопасности. Компьютерные системы. 2013. №2. С.13-19.

122. Крамаров Л.С., Бабенко Л.К. Обнаружение сетевых атак и выбор контрмер в облачных системах // Известия ЮФУ. Технические науки. 2013. №12(149). С.94-101.

123. McCumber J. A Structured Methodology. Assessing and Managing Security Risk in IT Systems // Publisher: Auerbach Publications; 1 edition (June 15, 2004). // Режим доступа: - https://buildsecurityin.us-cert.gov/swa/downloads/McCumber.pdf. (дата обращения: 20.03.2011).

124. Brotby K. Information security governance. A Practical Development and Implementation Approach // Hoboken: John Wiley & Sons, Inc., 2009 – 185 p.

125. Воробьев В.И., Монахова Т.В., Функциональное моделирование системы информационной защиты предприятия // Труды СПИИРАН. № 2, т.2. – СПб.: Наука, 2005. С.216–222.

126. Котенко Д.И., Котенко И.В., Саенко И.Б. Методика итерационного моделирования атак в больших компьютерных сетях // Труды СПИИРАН. №23. – СПб.: Наука, 2012. С.50–79.

127. Hentea M. Intelligent System for Information Security Management: Architecture and Design Issues // Issues in Informing Science and Information Technology. 2007. Volume 4.

128. Осипов В.Ю., Носаль И.А. Обоснование периода пересмотра мероприятий по защите информации // Информационно – управляющие системы. 2014. № 1. С. 63-69.

129. Мытарев Ф.Ю. Информационные ресурсы как предмет бизнеса // Информационные ресурсы России. 2007. № 3. С.17-19.

130. Осипов В.Ю., Кондратюк А.П. Оценка информации в интересах рефлексивного управления конкурентами // Программные продукты и системы. 2010. №2. С.64 - 68.

131. Осипов В.Ю., Носаль И.А. Обоснование мероприятий обеспечения информационной безопасности // Информационно – управляющие системы. 2013. № 2(63). С. 48-53.

132. Осипов В.Ю. Синтез результативных программ управления информационно-вычислительными ресурсами // Приборы и системы управления. 1998. № 12. С. 24 - 27.

133. Новиков И.С. Методы расчёта количественных показателей надёжности сложных программных комплексов на стадии проектирования и разработки // Труды СПИИРАН. № 6. – СПб.: Наука, 2008. – С. 86 - 111.

134. Осипов В.Ю. Оценка защищённости информационно-вычислительных ресурсов от несанкционированного доступа // Приборы и системы управления. 1996. №7. С. 16 - 19.

135. Носаль И.А. Метод обоснования мероприятий информационной безопасности социально-важных объектов // Труды СПИИРАН. № 2(39) – СПб.: Наука, 2015. – С.84-100.

136. Носаль И.А. Обоснование оптимального набора прав доступа // Комплексная защита объектов информатизации и измерительные технологии: Сб. научн. тр. Всероссийской научно-практической конф. с междунар. участ. (Санкт-Петербург, 16-18 июня 2014 г.). Санкт-Петербург:Издательство Политехнического университета, 2014. С.41-45.

137. Шелестова О. Что такое SIEM? // 2012. Режим доступа: - http://www.securitylab.ru/analytics/430777.php (дата обращения: 10.01.2015).

138. Котенко И.В., Саенко И.Б., Полубелова О.В., Чечулин А.А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Труды СПИИРАН. №20. – СПб.: Наука, 2012. С.27–56.

139. Агафонова И., Басова И., Зотова А., Петренко С. Многоцелевая BI-платформа службы безопасности // Защита информации. Инсайд. 2014. № 5. С.34-41.

140. Костина А. Нестандартное применение BI: на страже информационной безопасности // Jet Info. 2013. №2 Режим доступа: - http://www.jetinfo.ru/author/anna-kostina/nestandartnoe-primenenie-bi-na-strazhe-informatsionnoj-bezopasnosti. (дата обращения: 10.01.2015).

141. Воробьев А.В. Обзор систем по управлению устройствами обеспечения ИБ // Защита информации. Инсайд. 2014. № 6. С.64-67.

142. Климов С.М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем // Известия ЮФУ. Технические науки. 2005. №4. С.74-82.

143. Бородакий Ю.В. Интеллектуальные системы обеспечения информационной безопасности // Известия ТРТУ. 2005. № 4. С.65-69.

144. Дунин В.С., Бокова О.И., Хохлов Н.С. Алгоритм функционирования модели адаптивной системы защиты информации комплексной автоматизированной интеллектуальной системы «Безопасный город» // Вестник ВИ МВД России. 2012. №1. С.151-159.

145. Котенко И.В., Саенко И.Б. Архитектура системы интеллектуальных сервисов защиты информации в критически важных инфраструктурах // Труды СПИИРАН, 2013, выпуск 24, 21–40.

146. Бородакий Ю.В., Миронов А.Г., Добродеев А.Ю., Болдина М.Н, Бутусов И.В. Перспективные системы защиты информации должны быть интеллектуальными // Защита информации. Инсайд. 2013. № 2. С.48-51.

147. Котенко И.В., Саенко И.Б. Интеллектуальные сервисы защиты информации в компьютерных системах и сетях // Защита информации.Инсайд. 2013. № 2. С.32-41.

148. Лекционные материалы по теме: «Информационная безопасность в АИС ПФР – 2 Пенсионного фонда Российской Федерации», утверждены управляющим ОПФР по Республике Коми О.М. Колесник от 15.09.2015 г.

149. Методические рекомендации по оценке безопасности в территориальных органах ПФР Республики Коми, утверждены управляющим ОПФР по Республике Коми О.М. Колесник от 15.09.2015 г.

150. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность/Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.

151. Ed Adams The Six Best Practices of IT Security. 23.05.2007 // Режим доступа: - http://www.cioupdate.com/reports/article.php/11050_3679486_3/The-Six-Best-Practices-of-IT-Security.htm (дата обращения: 17.09.2015).