На правах рукописи

Носаль Ирина Алексеевна

ОБОСНОВАНИЕ МЕРОПРИЯТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНО-ВАЖНЫХ ОБЪЕКТОВ

Специальность 05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата технических наук

Санкт-Петербург – 2016

Работа выполнена в Федеральном государственном бюджетном учреждении науки «Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)».

Научный руководитель:	Доктор технических наук, профессор Осипов Василий Юрьевич, Санкт-Петербургский институт информатики и автоматизации Российской академии наук, заведующий лабораторией информационно-вычислительных систем и технологий программирования
Официальные оппоненты:	Доктор технических наук, профессор, Буйневич Михаил Викторович, Санкт-Петербургский государственный университет телекоммуникаций им. профессора М.А. Бонч-Бруевича, ведущий научный сотрудник управления организации научной работы и подготовки научных кадров Кандидат технических наук, доцент, Воробьев Евгений Германович, Санкт-Петербургский государственный электротехнический университет им. В.И.Ульянова (Ленина), заведующий кафедрой информационной безопасности
Ведущая организация	Санкт-Петербургский университет МВД России

Защита диссертации состоится "24" марта 2016 г. в 15.30 часов на заседании совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Д 002.199.01 при Федеральном государственном бюджетном учреждении науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук" (СПИИРАН) по адресу:
199178, Санкт-Петербург, 14-а линия В.О., 39, комн. 401.
Факс: (812) 328-44-50 тел: (812) 328-34-11.

С диссертацией и авторефератом можно ознакомиться на сайте Федерального государственного бюджетного учреждения науки "Санкт-Петербургский институт информатики и автоматизации Российской академии наук".
http://www.spiiras.nw.ru/dissovet/

Автореферат разослан "____"_____2016 г.

Ученый секретарь совета
Д 002.199.01
кандидат технических наук  Фаткиева Р.Р.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации. Для организаций, достигших определенного уровня зрелости 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, противодействующих этому. Решение этого вопроса при отсутствии соответствующих инструментов становится нетривиальной задачей. Набирающая обороты информатизация вносит свои коррективы в постановку задачи поиска целесообразных мероприятий информационной безопасности. Такие мероприятия должны быть гибкими, адаптивными и масштабируемыми, должны учитывать при этом комплексность и системность требований по защите, а также требования всех заинтересованных лиц.

Информационная безопасность для социально-важных объектов (СВО) – одно из главнейших условий надлежащего предоставления ими 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).

Под социально-важным объектом (СВО) в настоящей работе подразумевается социально-ответственный институт, не входящий в систему государственных органов власти, основной целью которого является предоставление государственных социально-экономических услуг населению и обеспечение конституционных прав граждан в области социальной защиты, государственной социальной помощи и обязательного социального страхования.

В отличие от государственной безопасности, для обеспечения информационной безопасности 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. 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 надежных методах обоснования мероприятий ИБ СВО.

Цель работы и задачи исследования. 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.

Задачи диссертационного исследования. 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 научные результаты, 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 уровня информационной безопасности социально-важных объектов.

Научная новизна полученных научных результатов заключается в следующем:

1. 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. 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.

2. Предложена новая комбинация 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.

3. Разработан новый 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.

4. Предложены новые 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. Они 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 докладывались на международной научно-практической конференции

«Перспективные информационные технологии (ПИТ 2014)» (г. Самара, 30 июня – 4 июля 2014г.), всероссийской научно-практической конференции с международным участием «Комплексная защита объектов информатизации и измерительные технологии» (Санкт-Петербург, 16-18 июня 2014 г.) и межрегиональной научно-практической конференции «Информационная безопасность и защита персональных данных: Проблемы и пути их решения» (г. Брянск, 28 апреля 2014г.).

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.).

Публикации. 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.

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.

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

СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, сформулированы цели исследования, решаемая научно-техническая задача и положения, выносимые на защиту, отражена суть и новизна основных научных результатов.

В первой главе диссертации проведен анализ целей, задач и возможностей известных систем ИБ СВО, защищаемых информационных ресурсов. Проанализированы структуры систем и мероприятий ИБ СВО. Пример информационно-организационной структуры СВО, в интересах которого необходимо обосновывать мероприятия информационной безопасности, показан на рисунке 1, где УПФР - районный уровень СВО; ОПФР - региональный уровень СВО; ПУ- персонифицированный учет 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. Выявлены критические места и направления, требующие наибольшего внимания. Определены наиболее критичные ресурсы, процессы и угрозы ИБ СВО. Сделан анализ известных методов обоснования мероприятий ИБ. Он показал, что в этих методах 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. Выстраиваемая согласно им система обеспечения ИБ не обладает требуемыми свойствами. Поставлена научно-техническая задача разработки новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, повышающих уровень их ИБ.

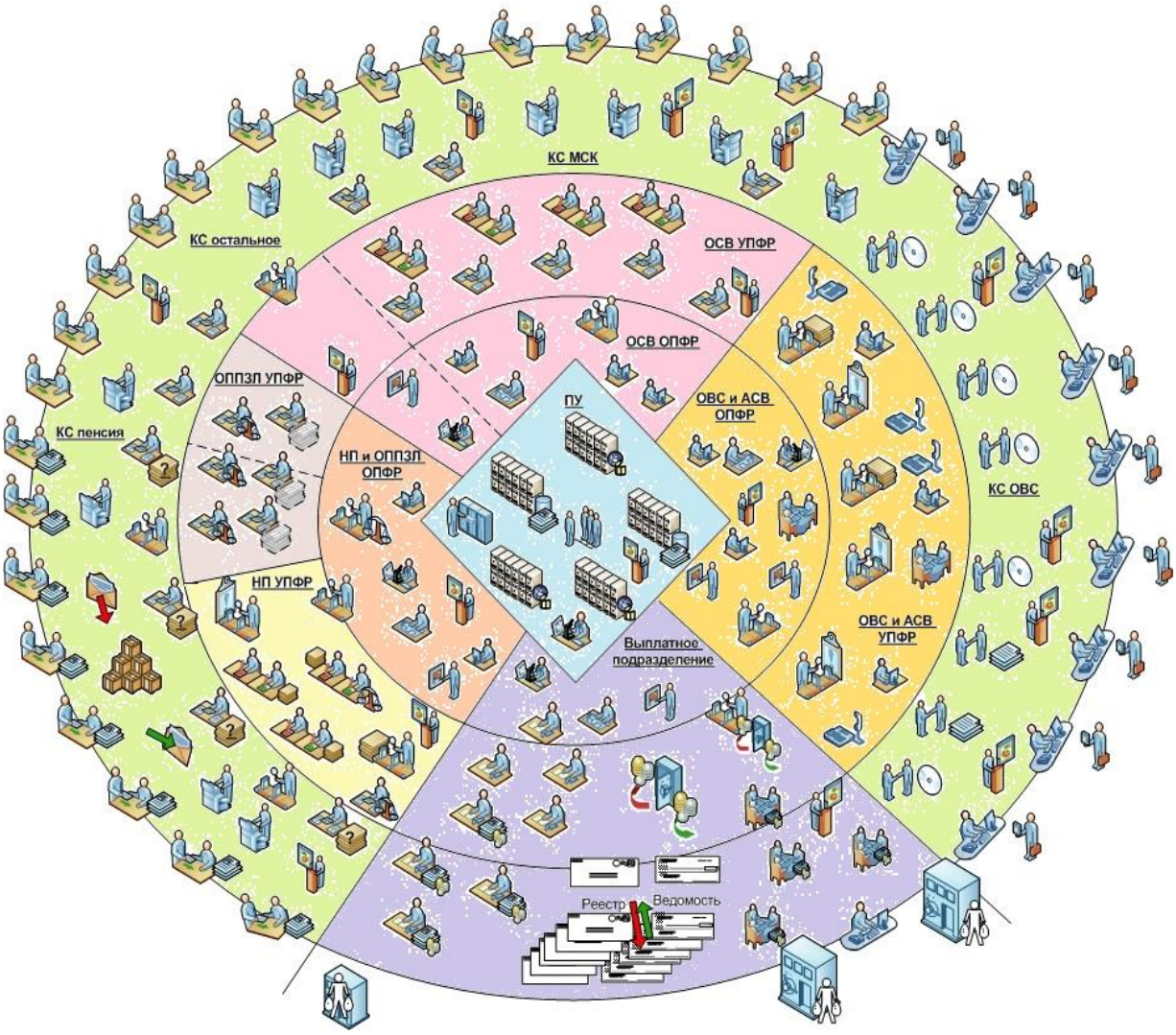


Рисунок 1 – Информационно-организационная структура СВО

Во второй главе рассматривается метод управления информационной безопасностью социально-важных объектов на основе комплекса оптимизационных моделей. Среди основных шагов метода выступают:

— разработка нескольких альтернативных моделей защищаемого процесса с учетом того или иного набора мероприятий ИБ СВО (марковских моделей в виде графов состояний);

— формулировка условий оценки эффективности мероприятия ИБ СВО (требований к итоговой безопасности процесса и к вспомогательным показателям ИБ СВО) на качественном уровне;

— разработка или выбор адекватной оптимизационной модели ИБ СВО;

— поиск экстремума основного показателя эффективности (целевой функции) при анализе альтернативных наборов мероприятий ИБ СВО, удовлетворяющего всем условиям задачи;

— принятие в качестве целесообразного тот набор мероприятий ИБ СВО, при котором достигнут экстремум целевой функции.

Для расчета вероятностей нахождения процесса в интересующих состояниях в соответствии с построенным графом составляется система дифференциальных уравнений. Затем она разрешается относительно заданных начальных и интересующих состояний.

В соответствии с этим методом выбор конкретной оптимизационной модели должен осуществляться, исходя из наибольшего соответствия ее реальной ситуации.

Предложены следующие оптимизационные модели поиска оптимального периода пересмотра мероприятий (ППМ) ИБ.

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

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

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

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

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

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

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; $P_{C_k}(\Delta t_k, T)$- вероятность санкционированного доступа к информационным ресурсам; $P_{H_k}(\Delta t_k, T)$ – 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_{0k} – суммарные затраты на $t = 0$, в частном случае они могут не зависеть от Δt_k. В результате вместо (2) имеем:

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

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:

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

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

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

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

Здесь $T_{б_k}$ - время реакции системы защиты при k-м периоде пересмотра мероприятий защиты; $T_{\text{доп.}}$ - 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:

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

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

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

Специфика модели (13) - (14) состоит в расчёте основного показателя и в проверке условия (14). 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:

$$\Delta t_o = \max_{k \in Q} \Delta t_k, \quad (15)$$

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

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

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, $P_{\text{доп.}}$. 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 $V(T)*P_{k\_н}(\Delta t_k, T)$ и затратами на мероприятия ИБ $B_k(\Delta t_k, T)$:

$$W_0 = (\Delta t_k, T) = max\, W_k(\Delta t_k, T), \quad (17)$$

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

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

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

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. Например можно обосновывать целесообразный набор прав доступа.

В развитие предложенного метода управления информационной безопасностью социально-важных объектов на основе комплекса оптимизационных моделей во второй главе также раскрыт метод обоснования мероприятий ИБ по критерию минимума интегральных потерь с учетом дополнительных условий.

Согласно ему ищется комплекс M_o целесообразных мероприятий ИБ, при котором на момент времени t достигается минимум суммарных потерь $L_o(M_o, t)$:

$$L_0(M_0,t)=\min_{k\in Q}\left\{B_k(M_k,t)+\sum_{z=1}^{Z}V_z(t)\times\right.$$
$$\left.\times\left(1-\prod_{s=1}^{S_{kz}}(1-P_{kzs}(PRG_{kzs}(M_k),t))\right)\right\}\ , \qquad (20)$$

и выполняются условия:

$$P_{kzs}(PRG_{kzs}(M_k),t)\geq P_E\ , \qquad (21)$$

$$PRG_{kzs}(M_k)\in R, \qquad (22)$$

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

В (20) - (22) 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; $P_{kzs}(PRG_{kzs}(M_k),\ t)$ – 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 (20) 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 (21) принимаются во внимание только деструктивные программы с эффектом не ниже заданного. В соответствии с (22) анализируются только результативные программы, приводящие к нарушениям ИБ за конечное число шагов. В частном случае ценность информационных ресурсов на текущий момент времени может быть определена как минимум суммарных потерь на их восстановление. В общем случае требуется учитывать также отдаленные возможные риски для СВО от потерь этих ресурсов. В соответствии с этим методом для обоснования комплекса целесообразных мероприятий ИБ предлагается синтезировать потенциальные программы деструктивных действий злоумышленников. Синтез таких программ рекомендуется осуществлять, исходя из возможной информированности злоумышленников на текущий момент времени. Особенность этого метода состоит в новой совокупности условий, при которой предлагается обосновывать мероприятия ИБ.

В третьей главе представлена модель функционирования социально-важного объекта. Можно говорить о том, что совокупность основных деловых процессов организации фактически полностью описывают её функциональную модель. Поэтому для разработки модели функционирования СВО был выбран один из наиболее характерных СВО деловой процесс «Назначение и выплата пенсии». Этот процесс формализован графом состояний, приведенным на рисунке 2. Данный граф описывает сложный деловой процесс, результатом выполнения которого могут быть различные варианты развития событий:

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

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

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

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

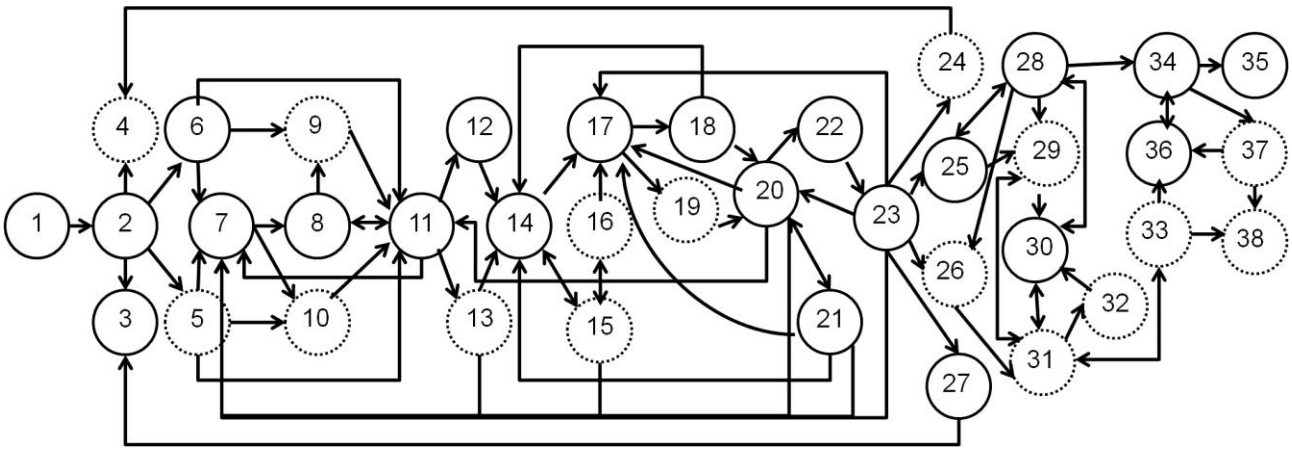
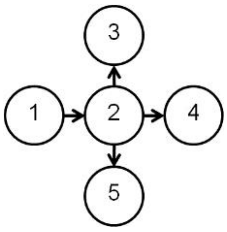
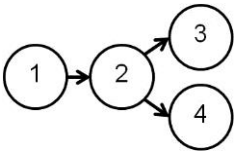
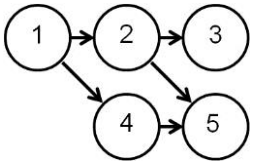
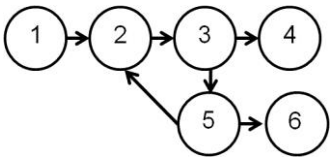
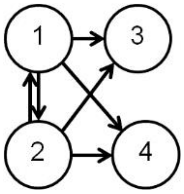


Рисунок 2 – Деловой процесс «Назначение и выплата пенсии»

Под цифрами на рисунке 2 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)); 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 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 расчетом; 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); 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 не корректные суммы на выплату; 32 – произведен очередной расчет массивов выплатной информации и реестры не сошлись; 33 – очередной расчет массивов выплатной информации и реестры сошлись, но конкретные суммы выплаты неверны и на выплату приняты некорректные документы; 34 – произведен очередной расчет массивов выплатной информации, реестры сошлись и выплатные документы приняты на выплату; 35 – выплата произведена в соответствии с законодательством (направление списков в банк и платежных 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, платежные

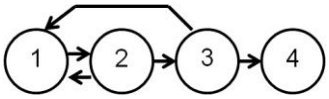
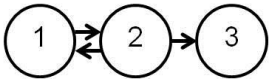
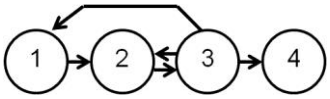
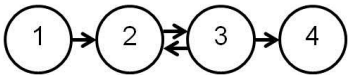
документы с не корректными суммами направлены в Казначейство). События, возникающие в таких процессах имеют массовый и случайный характер. И, при этом, обладают свойством статистической устойчивости, что позволяет использовать для их анализа математический аппарат марковских процессов. В целях упрощения такого анализа исследуемые процессы разбивались на подпроцессы, модели которых приведены в таблице 1.

Таблица 1. Модели защищаемых деловых процессов СВО

Модели	Состояния
 Модель 1. Прием документов (рабочий процесс клиентской службы - КС)	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.
 Модель 2. Истребование дополнительных документов (рабочий процесс КС и оценки пенсионных прав застрахованных лиц	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.
 Модель 3. Принятие выплатного документа (ВД) к назначению (рабочий процесс отдела назначения пенсий и оценки пенсионных прав застрахованных лиц)	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.
 Модель 4. Расчет выплат (рабочий процесс отдела выплаты)	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.
 Модель 5. Выплата пенсии (рабочий процесс отдела выплаты)	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.

В таблице 2 приведен комплекс моделей типовых нарушений ИБ СВО, который описывает возможные атаки на деловой процесс назначения и выплаты пенсии ПФР. Для каждого процесса составлялась и разрешалась своя система дифференциальных уравнений при заданных исходных данных.

Таблица 2. Модели типовых нарушений

Модели	Состояния
 Модель 1. Подмена источника (поставщика) данных Атака «masquerading»	1 – злоумышленник отслеживает обращения СВО к внешнему источнику (поставщику) данных; 2 - запрос СВО к внешнему источнику перехвачен; 3 – злоумышленник маскируется и направляет ответ от имени источника; 4 – некорректные данные приняты (нарушение аутентичности и целостности данных)
 Модель 2. Перехват передаваемых данных Атака «man in the middle»	1 – злоумышленник отслеживает обращения СВО к внешнему источнику; 2 – злоумышленник перехватил/вычислил/подобрал ключевую/парольную информацию; 3 –НСД к ЗИР получен.
 Модель 3. Нарушение целостности данных	1 – злоумышленник получает доступ к данным; 2 – злоумышленник вносит изменения в данные; 3 – проверка данных; 4 – некорректные данные приняты.
 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.

Оба комплекса моделей разработаны в рамках предложенного метода управления СОИБ СВО. Новизна этих 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 метода управления ИБ СВО, разработан также метод определения начальных состояний, позволяющий распознавать состояния, в которых система может находиться на исходный момент времени. Он предусматривает: анализ защищаемого процесса с выделением признаков всех состояний этого процесса; фиксацию для каждого состояния моделируемого процесса ограниченного набора признаков; присваивание каждому признаку каждого состояния относительного веса; определение на интересующий момент времени проявления выделенных признаков состояний; получение распределения вероятностей по состояниям процесса.

В четвертой главе приводятся результаты моделирования, подтверждающие работоспособность предложенных методов и моделей.

В качестве примера проведена оценка ценности (важности) защищаемых информационных ресурсов (ЗИР) для подпроцесса принятия выплатных документов (ВД) к назначению (таблица 1, модель 3). Если по результатам направления запроса в другие органы в СВО не поступило документов или поступили недостоверные сведения, 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. Принимая в качестве получаемого эффекта – уровень защищённости процесса, рассчитывается вероятность нахождения его в третьем состоянии $P_3(t)$ на конечный момент времени $t_{конеч.}$ при наличии ЗИР W_2 и при их отсутствии W_1. Тогда разница между ними дает искомый эффект $\Delta W = P_{3ЗИР}(t) - P_{3безЗИР}(t)$. Параметры переходов процесса из состояния в состояние задавались, исходя из регламента моделируемого производственного процесса.

В результате моделирования с применением пакета прикладных программ MatLab были получены зависимости, приведенные на рисунке 3.

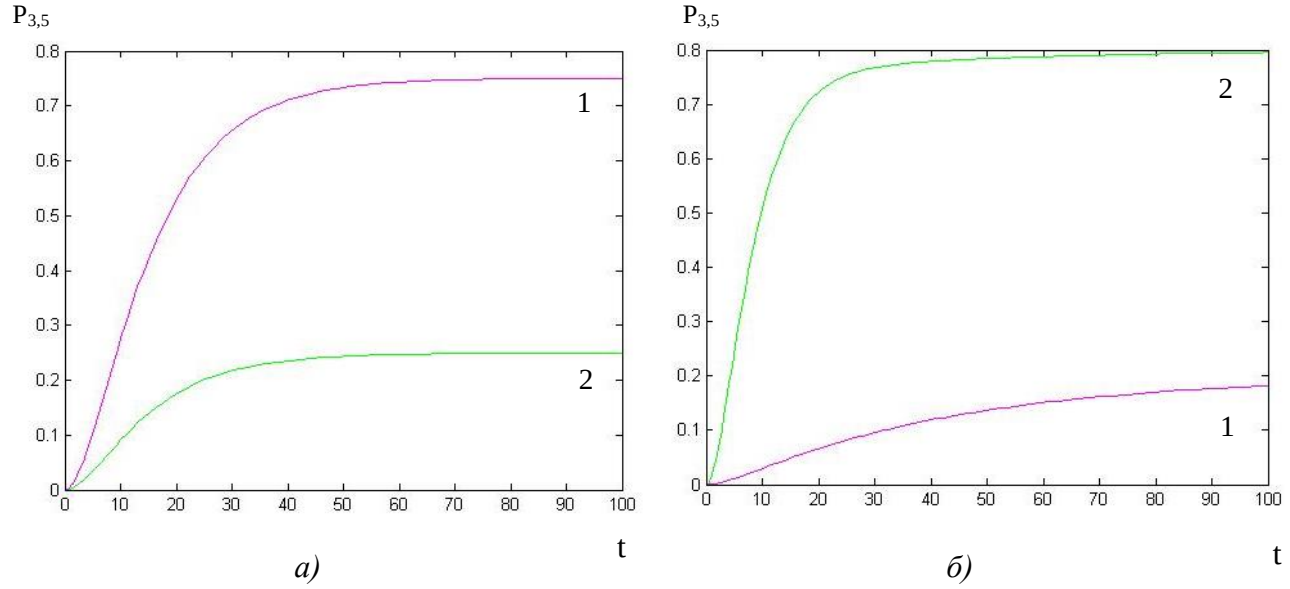


Рисунок 3 – Зависимость вероятности принятия корректного (кривая 1) и некорректного (кривая 2) ВД от времени при наличии а) и при отсутствии ЗИР б).

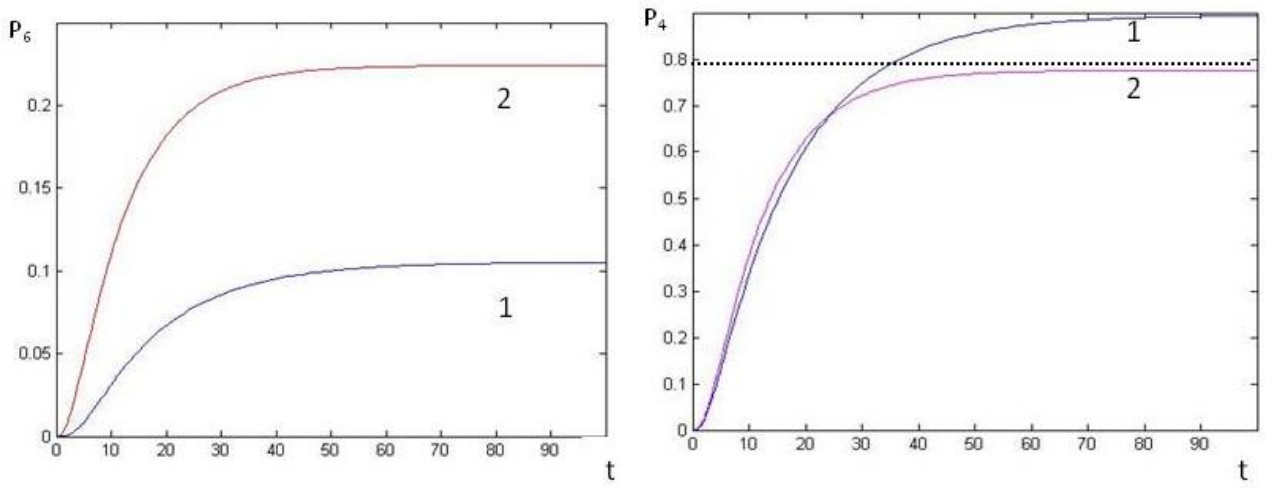
Согласно рисунку 3 на момент времени $t = 20$ вероятность принятия к назначению корректного ВД равна 0,5282 и 0,06561 соответственно. Таким образом, можно говорить о том, что правильно полученные документы, которые находятся в ведомстве других организаций, имеют вклад, оказываемый на правильность принятого решения, равный 46%.

Приведен также результат обоснования прав доступа для моделей «Перерасчет выплат» (рисунок 4).

Анализ результатов показывает, 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. Проведен количественный анализ также других деловых процессов СВО на предмет их ИБ.

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 СОИБ.

В этой же главе предложена архитектура комплекса программных средств обоснования мероприятий ИБ СВО. Она 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.



а) *б)*

Рисунок 4 – 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 «Перерасчёт выплат»

Составлено задание на реализацию системы поддержки принятия решений (СППР) для СОИБ СВО, представляющее собой систему тестовых заданий, состоящих из входных и выходных данных. Если система пройдет представленные тесты, можно говорить о том, что СППР настроена правильно и будет обеспечить необходимы уровень автоматизации управления ИБ СВО.

Предложены методические рекомендаций по использованию разработанных методов и моделей. Разработан 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 рекомендации по разработке интеллектуальной системы обоснования мероприятий ИБ СВО и её возможная структура в рамках комплекса уже существующих средств.

Сформулированы предложения по совершенствованию организации ИБ СВО в части развития нормативно-правовой базы, оценки рисков, предотвращения типовых нарушений и в области управления СОИБ СВО. Необходима разработка мер превентивного предотвращения угроз безопасности, а также включение этапа пересмотра существующих и обоснование новых мероприятий. Ставится задача о разработке отраслевого стандарта ИБ СВО.

В заключении представлены основные результаты диссертационного исследования. Сделан вывод, что поставленная научная задача разработки новых моделей и методов обоснования мероприятий информационной безопасности социально-важных объектов, повышающих уровень их ИБ, успешно решена. Цель диссертационного исследования достигнута.

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. Согласно Модели зрелости информационной безопасности Gartner Group (с англ. Information Security Maturity Model (ISMM), предлагаемые методы и модели позволяют постепенно развить и поддерживать ИБ СВО на третьем (наивысшем) уровне.

В целом предложенные решения могут найти применение при управлении ИБ СВО, создании новых информационных структур СВО и органов ПФР, их перспективных систем безопасности.

ОСНОВНЫЕ ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Публикации в журналах, входящих в перечень ВАК:

1. Носаль И. А. Обоснование периода пересмотра мероприятий по защите информации / В.Ю.Осипов, И.А.Носаль // Информационно – управляющие системы. – 2014. – № 1. – С. 63–69.
2. Носаль И.А. Обоснование мероприятий информационной безопасности / В.Ю.Осипов, И.А.Носаль // Информационно – управляющие системы. – 2013. – № 2(63). – С. 48–53.
3. Носаль И.А. Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» / В.В.Миронов, И.А.Носаль // Информация и безопасность. – 2011. – № 2. – С. 209 – 216.
4. Носаль И.А. Метод обоснования мероприятий информационной безопасности социально-важных объектов/ И.А.Носаль // Труды СПИИРАН. – СПб.: Наука, 2015. – Вып. 2(39) . – С. 84–100

Другие публикации:

5. Носаль И.А. Обоснование оптимального набора прав доступа / И.А.Носаль // 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.
6. Носаль И.А. Особенности обеспечения информационной безопасности социально важных объектов/ И.А.Носаль // 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.
7. Носаль И.А. Потенциал нападения и типовая модель нарушителя / И.А.Носаль // Информационная безопасность и защита персональных данных: Проблемы и пути их решения: материалы VI Межрегиональной научно-практической конференции. (г. Брянск, 28 апреля 2014г.). Брянск: Издательство БГТУ, 2014. – С. 96–101.