На правах рукописи

ТАРАСОВ Андрей Дмитриевич

МЕТОД И АЛГОРИТМЫ ПРОЕКТИРОВАНИЯ СИСТЕМ ФИЗИЧЕСКОЙ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА ОСНОВЕ ОБРАБОТКИ НЕЧЕТКОЙ ИНФОРМАЦИИ

Специальность:
05.13.19 – Методы и системы защиты информации, информационная безопасность (технические науки)

АВТОРЕФЕРАТ
диссертации на соискание ученой степени кандидата технических наук

Уфа – 2017

Работа выполнена на кафедре «Вычислительная техника и защита информации» в ФГБОУ ВО Уфимский государственный авиационный технический университет.

Научный руководитель: доктор технических наук, доцент
Боровский Александр Сергеевич

Официальные оппоненты: доктор технических наук, доцент
Янников Игорь Михайлович
ФГБОУ ВО «Ижевский государственный технический университет имени М.Т. Калашникова», кафедра «Техносферная безопасность», профессор

кандидат технических наук, доцент
Соколов Александр Николаевич
ФГАОУ ВО «Южно-Уральский государственный университет (национальный исследовательский университет)», кафедра «Защита информации», заведующий кафедрой

Ведущая организация: ФГБОУ ВО «Астраханский государственный технический университет», г. Астрахань

Защита диссертации состоится 15 декабря 2017 г. в 10^{00} часов на заседании диссертационного совета Д 212.288.07 на базе ФГБОУ ВО «Уфимский государственный авиационный технический университет» по адресу: 450008, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «___» _____ 2017 года.

Ученый секретарь
диссертационного совета,
д. т. н., доцент И. Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность работы. В современном мире объекты информатизации (ОИ) входят в состав большинства предприятий и организаций. Нарушение информационной безопасности ОИ может привести к разглашению конфиденциальной информации, банкротству организации, а также к нарушению функционирования предприятия. Наиболее серьезные последствия возможны, если объект информатизации является частью критически важного объекта (КВО). Такие объекты информатизации включают в себя автоматизированные системы управления производственными и технологическими процессами, выход из строя которых приводит к нарушению функционирования производства, что может повлечь за собой катастрофические последствия.

Среди всех угроз, направленных на ОИ можно выделить угрозы связанные с возможностью физического проникновения на объект с целью несанкционированного доступа к защищаемой информации и техническим средствам объекта информатизации. Средствами противодействия угрозам такого рода являются системы физической защиты (СФЗ). СФЗ представляют собой объединение сил охраны и технического оснащения – комплекса инженерно-технических средств охраны (ИТСО). Проектирование СФЗ – это сложный процесс. Если при проектировании допускаются ошибки, то полученная система, либо не сможет противодействовать угрозам, либо превысит необходимый уровень защищенности для объекта информатизации и затраты на ее создание и обслуживание будут необоснованно высоки. Поэтому физическая безопасность ОИ напрямую зависит от результатов решения задачи проектирования СФЗ.

В задаче проектирования СФЗ используется исходная информация, отражающая опыт и знания экспертов. Знания экспертов обычно являются результатами приблизительных оценок, прогнозов и предположений. Чтобы оперировать такой информацией, необходимо использовать методы обработки неточных данных.

Таким образом, **актуальность проведения исследований** заключается в необходимости информационной поддержки решения задачи проектирования систем физической защиты объектов информатизации с применением методов обработки неточной информации.

Степень разработанности темы исследования. В настоящее время идет постоянная работа по разработке нормативной документации в области обеспечения физической безопасности, в том числе по определению оптимальных структур систем физической защиты, создаются математические модели функционирования систем безопасности, математические модели объектов, математические модели нарушителей и т. п. Отечественные и зарубежные ученые, проводят многочисленные исследования, посвященные проблемам проектирования и оценки систем физической защиты: М. Гарсия, Джеймс Ф. Бродера, А.В. Бояринцев, А.Н. Бражник, А.Г. Зуев, В.В. Волхонский, В.С. Зарубин, И.М. Янников, Ю.А. Оленин, Г.Е. Шепитько, Р.Г. Магауенов, Я.Д. Вишняков, О.А. Панин, Н.Н. Радаев, В.В. Лесных, А.В. Бочков, В.А. Акимов, В.А. Герасименко, А.В. Архипов, С.Е. Сталенков, А.В. Измайлов, А.В. Ничиков, Г.Г.

Соломанидин, Н.Г. Топольский, К.И. Шестаков, Э.И. Абалмазов, А.М. Омельянчук. Описываются методы определения требований к СФЗ, способы оценки эффективности существующих и разрабатываемых систем. При этом среди исследований нет метода решения задачи проектирования СФЗ, позволяющего использовать средства информационной поддержки на этапе создания проекта СФЗ, определяющего размещение средств защиты на территории объекта. Существует отечественное и зарубежное программное обеспечение: СПРУТ, СПРУТ – ИМ, Вега – 2, ASSESS, EASI, FESEM, ISEM, SAFE, SAVI, SNAP, ALHPA, JTS и т. п., которое используется при проектировании СФЗ. Но все перечисленные программные средства применимы только на этапе тестирования готового проекта СФЗ для оценки его эффективности и не предоставляют помощи в процессе создания проекта.

Объектом исследования диссертационной работы является система физической защиты объекта информатизации.

Предметом исследования диссертационной работы является информационная поддержка решения задачи проектирования систем физической защиты объектов информатизации.

Цель диссертационной работы – разработка метода и алгоритмов для осуществления информационной поддержки решения задачи проектирования систем физической защиты объектов информатизации.

Для достижения поставленной цели необходимо решить следующие **задачи:**

1. Разработать метод создания концептуального проекта системы физической защиты объекта информатизации с определением размещения средств защиты на территории объекта.
2. Разработать алгоритмы метода создания концептуального проекта СФЗ ОИ с применением обработки неточной информации.
3. Разработать программное средство для информационной поддержки решения задачи проектирования СФЗ ОИ.
4. Провести анализ работоспособности и оценить эффективность реализованного метода и алгоритмов.

Методы исследования. Результаты исследований получены с помощью методов обработки неточной информации, таких как нечеткие переменные, генетические алгоритмы (ГА), метод ветвей и границ, многокритериальный анализ вариантов и теория графов.

Основные научные результаты, выносимые на защиту:

1. Метод создания концептуального проекта системы физической защиты объекта информатизации.
2. Алгоритмы метода создания концептуального проекта СФЗ ОИ на основе ГА с применением процедур обработки графов и нечетких чисел.
3. Алгоритм адаптивного генетического алгоритма, повышающий работоспособность программного средства информационной поддержки решения задачи проектирования СФЗ ОИ.
4. Алгоритм решения задачи проектирования СФЗ ОИ методом ветвей и границ, применяемый для анализа работоспособности ГА.

Научная новизна результатов исследования:

1. Новизна метода создания концептуального проекта СФЗ ОИ заключается в том, что его использование позволяет получить концептуальный проект в виде структурно-логической модели СФЗ, согласно которой каждый участок объекта информатизации защищается набором точек контроля (логических понятий, соответствующих частям комплекса ИТСО объекта). При рабочем проектировании точкам контроля будут сопоставляться реальные средства защиты.

2. Новизна алгоритмов метода создания концептуального проекта СФЗ ОИ заключается в проведении многокритериальной оптимизации через взвешенную сумму трех целевых функций ГА, в использовании процедуры поиска всех возможных путей перемещения нарушителя по территории объекта и процедуры отсева нерациональных путей, основанных на обработке графов и нечетких чисел.

3. Новизна алгоритма адаптивного ГА заключается в проведении анализа свойств прошедших поколений хромосом для определения необходимых изменений параметров ГА, что позволяет не выбирать значения параметров вручную. Правильно подобранные значения параметров влияют на возможности ГА по поиску решения, например, уменьшается вероятность попадания в локальный оптимум, что повышает работоспособность программного средства информационной поддержки решения задачи проектирования СФЗ ОИ.

4. Новизна алгоритма решения задачи проектирования СФЗ ОИ методом ветвей и границ заключается в использовании целевой функции ГА и способа кодирования вариантов решений аналогичного хромосомам ГА. Алгоритм позволяет найти оптимальное решение задачи размещения точек контроля для простых модельных объектов, что используется в имитационном моделировании для анализа работоспособности ГА.

Практическая ценность научной работы заключается в повышении физической безопасности объектов информатизации путем информационной поддержки решения задачи проектирования систем физической защиты в условиях неточных исходных данных.

Внедрение результатов. Результаты работы были успешно применены в проектных работах, выполняемых в организациях ФГБУ «3 ЦНИИ» МО РФ ст. Донгузская, Оренбургской обл.; ЗАО «Центр безопасности информации «ЦИНТУР» г. Оренбург; ООО «Газпром энерго» Оренбургский филиал; в учебном процессе ФГБОУ ВО Оренбургский государственный аграрный университет Институт управления рисками и комплексной безопасности; ФГБОУ ВО Оренбургский государственный университет.

Соответствие диссертации паспорту научной специальности. Представленная диссертация удовлетворяет п.6, п.9 и п.10 паспорта специальности 05.13.19 – «Методы, модели и средства защиты информации, информационная безопасность»:

п. 6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.

п. 9. Модели и методы оценки защищенности информации и информационной безопасности объекта.

п. 10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.

Достоверность результатов подтверждена результатами апробации созданного программного средства и проведением имитационного моделирования с применением метода ветвей и границ.

Апробация работы. Результаты работы докладывались и обсуждались на следующих конференциях с публикацией в сборнике трудов: XII Международная конференция «Проблемы управления и моделирования в сложных системах» 21-23 июня 2010 г., г. Самара; IV Международная научно-техническая конференция «Информационные технологии в науке, образовании и производстве» 22-23 апреля 2010 г., г. Орел; XIII Международная конференция «Проблемы управления и моделирования в сложных системах» 15-17 июня 2011 г., г. Самара; VIII Международная научно-практическая конференция «Дни науки - 2012» 27 марта - 5 апреля 2012 г. г. Прага; XV Международная конференция «Проблемы управления и моделирования в сложных системах» 25-28 июня 2013 г., г. Самара; V Международная научная конференция «Информационные Технологии и Системы» 24–28 февраля 2016 г., г. Челябинск; XIII Международная научно-техническая конференция «Новые Информационные Технологии и Системы» 23–25 ноября 2016 г., г. Пенза. Результаты диссертации использовались в работе, занявшей первое место в открытом молодежном конкурсе «Приволжье – территория безопасности», проводимого в 2013 году.

Публикации. Результаты диссертационной работы опубликованы в 21 печатном издании, в том числе в 2 монографиях, 11 статьях в изданиях из перечня ВАК, включая 2 статьи без соавторства. Получены 8 свидетельств о государственной регистрации программы для ЭВМ и одно свидетельство о регистрации электронного ресурса.

Личный вклад автора. Основные результаты и положения, выносимые на защиту, получены лично автором. Метод для определения требований к системе физической защиты объекта информатизации разработан в соавторстве с научным руководителем.

Структура и объем диссертации. Диссертационная работа состоит из введения, четырех глав основного материала, заключения, списка сокращений и списка литературы. Работа изложена на 144 страницах машинописного текста, включает 30 рисунков и 21 таблицу. Список литературы содержит 102 наименования.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы исследования, формулируется цель, задачи, объект и предмет исследования, выносимые на защиту результаты, научная новизна и практическая ценность, приведено краткое содержание работы.

В **первой главе** проводится анализ современного состояния процесса проектирования систем физической защиты объектов информатизации. Определяется понятие объекта информатизации, используется нормативная

документация по вопросу защиты объектов информатизации, рассматривается процесс проектирования системы физической защиты (ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения; Методика отнесения объектов государственной и негосударственной собственности к критически важным объектам для национальной безопасности Российской Федерации, Приказ ФСТЭК России от 14.03.2014 №31; Об утверждении рекомендаций по антитеррористической защищенности объектов промышленности и энергетики: приказ министра промышленности и энергетики РФ от 04.05.2007 № 150). Отмечается потребность в обработке экспертной информации. Проводится анализ работ, описывающих существующие методы проектирования СФЗ, методы оценки защищенности объекта и методы оценки эффективности систем защиты. Определена цель исследования: разработка метода и алгоритмов для осуществления информационной поддержки решения задачи проектирования систем физической защиты. Приводится краткое описание ранее разработанного метода определения требований к системе физической защиты объекта информатизации.

Общая последовательность действий для создания любой системы защиты выглядит следующим образом: 1) определение требований к системе защиты (формирование списка угроз: определение категорий нарушителей, определение потенциальных целей нарушителей и их приоритетность, возможная тактика их действия, их технические возможности и опыт, количественные характеристики угроз: вероятность угрозы, значимость угрозы, время до ближайшей угрозы и т.д.); 2) создание проекта системы защиты; 3) оценка проекта системы защиты. Первый и третий этап подробно описываются в таких документах как приказ министра промышленности и энергетики РФ от 04.05.2007 № 150. Второй этап сводится к разработке общих рекомендаций по созданию (совершенствованию) СФЗ объекта.

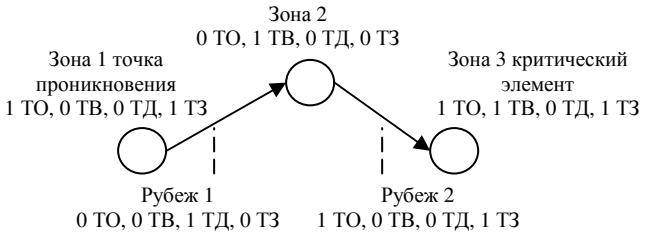
Рассмотрены результаты исследований, отраженные в монографиях, книгах, статьях отечественных и зарубежных ученых, диссертационные работы и существующие программные средства, в которых предлагаются решения задач данной предметной области. Ни один из предлагаемых способов решения задачи определения необходимого состава системы защиты не позволяет получить концептуальный проект СФЗ, определяющий расстановку элементов СФЗ на участках объекта. Использование существующих программных средств также возможно только при оценке уже созданного проекта СФЗ.

Рассматривается метод определения требований к системе физической защиты объекта информатизации. В алгоритмах метода используются следующие математические модели и понятия, необходимые для разработки метода создания проекта СФЗ: 1) Точка контроля (ТК) – это часть комплекса ИТСО объекта, влияющая на защищенность критических элементов (КЭ). Физически каждая ТК может включать в себя несколько средств комплекса ИТСО, выполняющих одну общую функцию: точка обнаружения (ТО), точка доступа (ТД), точка видеонаблюдения (ТВ), точка задержки (ТЗ). 2) Структурная защищенность КЭ – это защищенность наиболее уязвимого пути от точки проникновения на объект до КЭ. Мера структурной защищенности $\beta_{стр} = P_{обн} \cdot P_{зад}$ показывает вероятность

обнаружения и задержки нарушителя при попытке пройти по самому уязвимому пути к КЭ. $P_{обн}$ – вероятность обнаружения нарушителя на всем пути; $P_{зад}$ – вероятность задержки нарушителя на всем пути. 3) Для описания размещения элементов СФЗ на территории объекта информатизации применяется модель, которая описывает структуру объекта в виде графа, где вершины представляют зоны объекта, а ребра – рубежи. Зона – это часть территории объекта, представляющая собой ограниченное замкнутое пространство, имеющее физические границы или потенциальная цель нарушителя. Рубеж определяет способ или возможность перемещения из одной зоны в другую. Система физической защиты представляет собой совокупность средств комплекса ИТСО расположенных на объекте информатизации. Структурно-логическая модель СФЗ – совокупность точек контроля расставленных по графу ОИ [2].

Метод позволяет определить требования к СФЗ в виде необходимых значений параметров, по которым должна быть построена структурно-логическая модель СФЗ. Это наборы ТК, требуемые для защиты каждого КЭ, и структурная защищенность КЭ. Результаты работы метода будут использованы в качестве исходной информации для создания проекта СФЗ ОИ.

Во **второй главе** описывается метод создания проекта системы физической защиты объекта информатизации. Искомый концептуальный проект СФЗ представлен в виде структурно-логической модели СФЗ, определяющей на каком участке объекта должно быть установлено каждое средство защиты. Задача создания концептуального проекта СФЗ формулируется следующим образом: требуется определить оптимальное размещение ТК на территории объекта с несколькими КЭ и несколькими возможными точками проникновения нарушителей. При этом нужно соблюдать условие: защищенность всех КЭ соответствует требуемой защищенности или превышает ее при минимальных затратах на приобретение, установку и обслуживание элементов СФЗ. Пример оценки защищенности показан на рисунке 1. Рассматривается вопрос защищенности КЭ в зависимости от выбранного нарушителем пути перемещения по объекту, определяется процедура поиска всех путей и отсева нерациональных путей.



Сумма ТК на данном пути: 3 ТО, 2 ТВ, 1 ТД, 3 ТЗ
Требуемая защищенность КЭ:
набор точек контроля
2 ТО, 2 ТВ, 2 ТД, 2 ТЗ – не хватает 1 ТД
Вывод: при выборе нарушителем данного пути перемещения по территории объекта, защищенность КЭ не соответствует требуемой защищенности

Рисунок 1 – Пример оценки защищенности критического элемента при решении задачи оптимального размещения точек контроля

Алгоритм определения оптимального размещения точек контроля разработан на основе генетического алгоритма с применением процедур обработки графов и нечетких чисел. Обработка нечетких чисел проводится с помощью α-уровневого принципа обобщения. Используется поиск всех возможных путей на основе алгоритма поиска в глубину.

Хромосомы содержат в себе варианты решения задачи: размещение точек контроля в каждом участке объекта. Все участки объекта – зоны и рубежи получают сквозную нумерацию, для последовательного размещения информации по хромосоме. Для каждого участка записывается по четыре числа: $X_О^1$, $X_Д^1$, $X_В^1$, $X_З^1$ – количество точек контроля разных типов. Хромосомы представлены как двумерные массивы.

Экспертами задаются следующие исходные данные:
1) Структурно-логическая модель объекта в виде графа. 2) Необходимая защищенность каждого критического элемента объекта в виде требуемых наборов точек контроля. Например, $U_О^1$=2, $U_Д^1$=0, $U_В^1$=3, $U_З^1$=1, означает, что для защиты КЭ №1 требуется 2 ТО, 0 ТД, 3 ТВ, 1 ТЗ. 3) Ограничения на ТК в каждой зоне и в каждом рубеже объекта. Количество и состав ТК в одной зоне или рубеже должно соответствовать заданным ограничениям в виде минимума и максимума для каждого типа ТК. Например, для участка №3 – $X_О^3 \in [X_О^3{}_{min}, X_О^3{}_{max}]$, $X_Д^3 \in [X_Д^3{}_{min}, X_Д^3{}_{max}]$, $X_В^3 \in [X_В^3{}_{min}, X_В^3{}_{max}]$, $X_З^3 \in [X_З^3{}_{min}, X_З^3{}_{max}]$. 4) Вероятность обнаружения $P_{обн}$ и вероятность задержки $P_{зад}$ на каждом участке объекта, задаваемые в нечеткой форме, для отсева нерациональных путей.

Общая целевая функция строится в виде взвешенной суммы трех целевых функций, для которых используется принцип минимизации. Первая функция – F_1 отвечает за соответствие хромосом следующему правилу: каждый из путей, ведущий к каждому критическому элементу, должен содержать набор точек контроля соответствующий или превышающий (по количеству ТК каждого типа) необходимую защищенность КЭ. Функция принимает значение равное сумме недостающих точек контроля всех типов на всех путях. Например, необходимая защищенность КЭ с номером один: $U_О^1$, $U_Д^1$, $U_В^1$, $U_З^1$ сравнивается с набором ТК на первом пути до первого КЭ: $V_{О1}^1$, $V_{Д1}^1$, $V_{В1}^1$, $V_{З1}^1$. Результат сравнения для первого пути – $Path_1^1$ рассчитывается по формуле: $Path_1^1 = No_1^1 + Nд_1^1 + Nв_1^1 + Nз_1^1$, где

$$No_1^1 = \begin{cases} 0, \text{если } U_О^1 \le V_{О1}^1 \\ (U_О^1 - V_{О1}^1), \text{если } U_О^1 > V_{О1}^1 \end{cases},$$

$$Nд_1^1 = \begin{cases} 0, \text{если } U_Д^1 \le V_{Д1}^1 \\ (U_Д^1 - V_{Д1}^1), \text{если } U_Д^1 > V_{Д1}^1 \end{cases},$$

$$Nв_1^1 = \begin{cases} 0, \text{если } U_В^1 \le V_{В1}^1 \\ (U_В^1 - V_{В1}^1), \text{если } U_В^1 > V_{В1}^1 \end{cases},$$

$$Nз_1^1 = \begin{cases} 0, \text{если } U_З^1 \le V_{З1}^1 \\ (U_З^1 - V_{З1}^1), \text{если } U_З^1 > V_{З1}^1 \end{cases}.$$

Проводятся сравнения для всех путей до всех КЭ. Полученные результаты складываются: $F_1(h_1) = \sum_{i-1}^{nk} \sum_{j=1}^{np_i} Path_i^j$, где nk – количество КЭ на объекте, np_i – количество путей до i-го КЭ.

Вторая целевая функция – F_2 отвечает за то, чтобы общее число всех ТК объекта было минимально. Значение функции рассчитывается как сумма:
$F_2\,(h_1) = X_{\text{О}}{}^1 + X_{\text{Д}}{}^1 + X_{\text{В}}{}^1 + X_{\text{З}}{}^1 + X_{\text{О}}{}^2 + X_{\text{Д}}{}^2 + X_{\text{В}}{}^2 + X_{\text{З}}{}^2 + X_{\text{О}}{}^3 + \ldots$

Третья целевая функция – F_3 отвечает за то, чтобы средства обнаружения и видеонаблюдения располагались как можно ближе к точкам проникновения, т. е. находились в начале каждого пути. Такое расположение средств защиты необходимо чтобы обнаружить нарушителя как можно раньше во время проникновения на объект, а не в момент, когда нарушитель уже достиг критического элемента. Для каждого участка пути, например №1 – $X_{\text{О}}{}^1$, $X_{\text{Д}}{}^1$, $X_{\text{В}}{}^1$, $X_{\text{З}}{}^1$ соответственно наличию или отсутствию ТК разных типов создается набор логических значений: О_1, Д_1, В_1, З_1 (наличие ТК соответствует истине). Расчет значения функции F_3 для одного пути проводится следующим образом: $F_3{}^1\,(h_1) = Kp_1{}^1 + Kp_2{}^1 + Kp_3{}^1 + Kp_4{}^1 + \ldots$, где $Kp_1{}^1$ характеризует первый участок первого пути:

$$Kp_1^1 = \begin{cases} 0, \text{если } \text{О}_1, \text{Д}_1, \text{В}_1, \text{З}_1 \text{ - соответствует наличию средств обнаружения и видеонаблюдения} \\ (Lp_1\text{-}Dp_1^1), \text{если } \text{О}_1, \text{Д}_1, \text{В}_1, \text{З}_1 \text{ - наличие только средств обнаружения} \\ (Lp_1\text{-}Dp_1^1)\cdot 2, \text{если } \text{О}_1, \text{Д}_1, \text{В}_1, \text{З}_1 \text{ - наличие только средств видеонаблюдения} \\ (Lp_1\text{-}Dp_1^1)\cdot 4, \text{если } \text{О}_1, \text{Д}_1, \text{В}_1, \text{З}_1 \text{ - отсутствие средств обнаружения и видеонаблюдения} \end{cases},$$

где Lp_1 – длина пути, измеряемая в количестве участков пути, $Dp_1{}^1$ – расстояние от точки проникновения до участка пути измеряемое в количестве участков пути. Коэффициенты, на которые умножается значение разности $Lp_1 - Dp_1{}^1$, дополнительно увеличивают влияние на значение целевой функции для нежелательных вариантов (отсутствие средств обнаружения или видеонаблюдения) и уменьшают для желательных вариантов.

В итоге общая целевая функция для хромосомы h_1 рассчитывается по формуле: $F(h_1) = w_1 \cdot F_1(h_1) + w_2 \cdot F_2(h_1) + w_3 \cdot F_3(h_1)$, где w_1, w_2, w_3 – веса целевых функций, $w_1 + w_2 + w_3 = 1$. Рассмотрена проблема выбора значений w_1, w_2, w_3. Необходимо корректно задавать веса функций т. к. приспособляемость получаемых хромосом, а значит и возможность найти оптимальное решение, зависит от значений весов.

В **третьей главе** описывается реализация метода определения требований к СФЗ ОИ и метода создания проекта СФЗ ОИ в виде программного средства для информационной поддержки. Программные модули созданы на языках *Delphi* и *Visual Basic*. Проводится имитационное моделирование с использованием программного средства. Набор исходных данных для тестирования программы, включает граф модельного объекта (рисунок 2) – нефтеперерабатывающего завода. Оценка качества размещения точек контроля проводилась с помощью программы *EASI*, которая определяет вероятность прерывания действий нарушителей на выбранном пути проникновения на объект (рисунок 3). Для проверки близости получаемых программным средством решений к оптимальному, были найдены оптимальные решения задачи размещения точек контроля для объектов с простой структурно-логической моделью. Использовалась одна из схем неявного перебора – метод ветвей и границ. Были проведены эксперименты, в которых генерируемые ГА решения сравнивались с

оптимальными. Была доказана возможность получения программным средством оптимальных решений.

Показано преимущество генетического алгоритма перед методами полного и неявного перебора. Из-за большого количества вариантов решения любой метод перебора потребует очень больших вычислительных мощностей и не имеет практической осуществимости на обычном персональном компьютере. Генетический алгоритм может получить близкое к оптимальному решение задачи за приемлемое время.

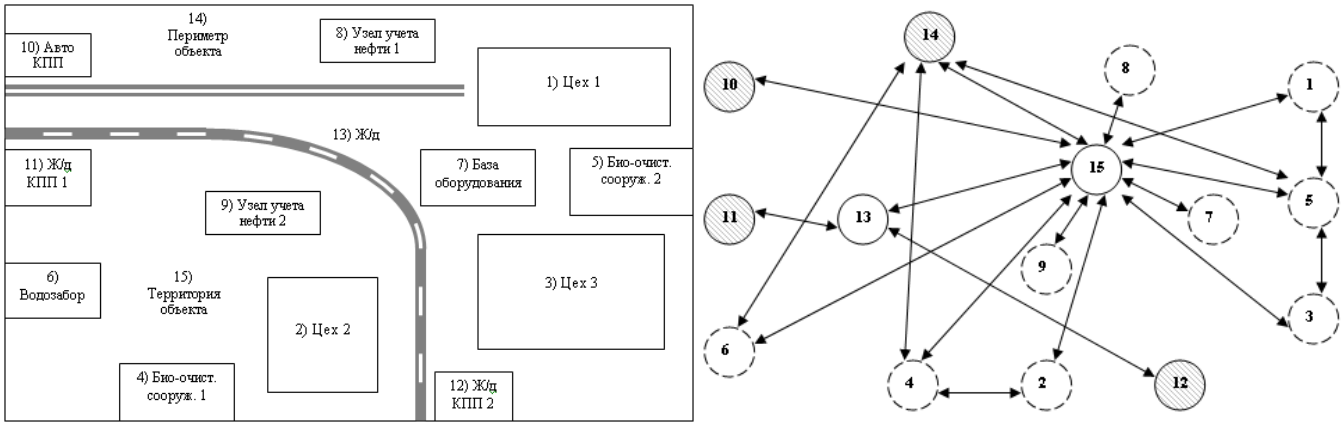


Рисунок 2 – Схема модельного объекта «нефтеперерабатывающий завод»

	Оценка прерывания последовательности действий нарушителя	Вероятность извещения охраны		Время реакции охраны, с	
				Среднее значение	Стандартное отклонение
		0,95		90	30
№	Описание	P(D)	Местоположение	Средняя задержка, с	Стандартное отклонение
1	Пройти внешние ворота	0	В	3	1
2	Преодолеть шлагбаум	0,5	В	6	2
3	Выйти на территорию объекта	0	В	10	3
4	Пройти сейсмические датчики	0,9	В	60	20
5	Обойти зону видимости камер	0,5	В	30	10
6	Пройти инфракрасные датчики	0,9	В	10	3
7	Преодолеть турникет	0,5	В	6	2
8	Преодолеть пост охраны	0,9	В	3	1
9	Вывести КЭ из строя	0	В	120	40

Рисунок 3 – Оценка качества размещения точек контроля, проводимая с помощью программы EASI

В **четвертой главе** формулируется и доказывается необходимость использования адаптивного генетического алгоритма в программном средстве. Для задачи оптимального размещения точек контроля выделены параметры ГА, значения которых сильно влияют на работоспособность алгоритма, описаны эксперименты, доказывающие необходимость определения значений этих параметров с помощью адаптивного ГА. Приведены необходимые модификации ГА и экспериментально доказывается, что работоспособность алгоритма

повышается. Адаптивный ГА был разработан и реализован в модифицированном программном модуле оптимального размещения точек контроля. Для определения необходимых изменений параметров ГА в программе проводится анализ свойств нескольких прошедших поколений хромосом.

Экспериментально доказано, что определение значений двух параметров ГА: соотношения весов целевых функций и вероятности мутации хромосом с помощью адаптивного ГА значительно ускоряет поиск оптимального решения и уменьшает вероятность попадания ГА в локальный оптимум. Среднее число итераций ГА, необходимое для нахождения оптимального решения в экспериментах с адаптацией весов целевых функций оказалось примерно в 2 раза меньше чем без адаптации. Среднее число итераций в экспериментах с адаптацией вероятности мутации хромосом в 3,5 раза меньше чем без адаптации.

Для проведения оценки эффективности разработанных метода и алгоритмов сравнивалась эффективность работы проектировщика СФЗ ОИ без помощи и с помощью программного средства. Использовался метод нечеткого многокритериального анализа вариантов. Были определены критерии с наибольшим влиянием на эффективность процесса создания концептуальной модели СФЗ ОИ. Коэффициенты относительной важности критериев определялись методом парных сравнений Саати. Вычислены значения эффективности для оцениваемых процессов. Сделан вывод, что процесс создания концептуальной модели СФЗ ОИ с использованием программного средства более чем в 1,5 раза эффективнее, чем процесс создания модели без использования программного средства.

В **заключении** подводятся итоги диссертационной работы, приводятся основные результаты и направление дальнейших исследований.

ОСНОВНЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ РАБОТЫ

1. Разработан метод создания концептуального проекта системы физической защиты объекта информатизации в виде структурно-логической модели, согласно которой каждый участок объекта информатизации защищается набором точек контроля (частей комплекса ИТСО объекта). При рабочем проектировании точкам контроля будут сопоставляться реальные средства защиты. Таким образом, в концептуальном проекте указывается размещение средств защиты на территории объекта.

2. Разработаны алгоритмы метода создания концептуального проекта системы физической защиты объекта информатизации. Алгоритмы включают в себя ГА с многокритериальной оптимизацией через взвешенную сумму трех целевых функций, процедуру поиска всех возможных путей перемещения нарушителя по территории объекта и процедуру отсева нерациональных путей, в которых используется обработка графов и нечетких чисел. Разработан адаптивный генетический алгоритм, повышающий работоспособность программного средства.

3. Разработано программное средство для информационной поддержки решения задачи проектирования систем физической защиты объектов информатизации. Программное средство объединяет шесть программных

модулей сгруппированных в две подсистемы: подсистема определения требований к системе физической защиты и подсистема создания концептуального проекта системы физической защиты.

4. Проведено имитационное моделирование, которое показало работоспособность генетического алгоритма в задаче проектирования СФЗ ОИ. Для проверки близости получаемых программным средством решений к оптимальному, методом ветвей и границ было найдено оптимальное решение задачи размещения точек контроля для модельного объекта. Показано преимущество генетического алгоритма перед методами полного и неявного перебора. Проведена оценка эффективности разработанных метода и алгоритмов с помощью нечеткого многокритериального анализа вариантов.

Перспективы дальнейшей разработки темы. Дальнейшие исследования позволят разработать и реализовать программные модули для выбора программных и программно-технических средств информационной безопасности и создать единый пакет программ для решения задачи проектирования системы информационной безопасности.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Монографии

1. Боровский, А.С. Автоматизированное проектирование и оценка систем физической защиты потенциально-опасных (структурно-сложных) объектов. Часть 1 – Системный анализ проблемы проектирования и оценки систем физической защиты: монография / А.С. Боровский, А.Д. Тарасов. – Самара; Оренбург: СамГУПС. 2012. – 155 с., ил. Усл. печ. л. 9,7.

2. Боровский, А.С. Автоматизированное проектирование и оценка систем физической защиты потенциально-опасных (структурно-сложных) объектов. В 3-х ч. Ч. 2. Модели нечетких систем принятия решений в задачах проектирования систем физической защиты: монография / А.С. Боровский, А.Д. Тарасов. – М.: Издательство «Омега-Л»; Оренбург: Издательский центр ОГАУ. 2013. – 248 с. Усл. печ. л. 14,4.

Публикации в изданиях, рекомендованных ВАК

3. Боровский, А.С. Особенности идентификации предметной области «категорирование потенциально-опасных объектов» в нечеткой постановке / А.С. Боровский, А.Д. Тарасов // Информационные системы и технологии, научный журнал, ОрелГТУ. – №3(59) май-июнь 2010 г. – С. 63–71.

4. Боровский, А.С. Интегрированный подход к разработке общей модели функционирования систем физической защиты объектов / А.С. Боровский, А.Д. Тарасов // Труды ИСА РАН, научный журнал. – Том 61, выпуск №1. 2011 г. – С. 3–14.

5. Боровский, А.С. Общая математическая модель системы физической защиты объектов / А.С. Боровский, А.Д. Тарасов // Вестник компьютерных и информационных технологий, научно-технический и производственный журнал. – № 10(88). 2011 г. – С. 21–30.

6. Боровский, А.С. Метод обработки экспертной информации на основе нечетких гиперграфов для проектирования систем физической защиты / А.С. Боровский, А.Д. Тарасов // Информационные технологии, теоретический и прикладной научно-технический журнал. – №2(186). 2012 г. – С. 67–73.

7. Боровский, А.С. Принятие проектных решений на основе модели «ситуация – стратегия управления – действие» для модернизации системы физической защиты / А.С. Боровский, А.Д. Тарасов // Труды ИСА РАН, научный журнал. – Том 62, выпуск №3. 2012 г. – С. 48–55.

8. Боровский, А.С. Метод оценки защищенности потенциально-опасных объектов при проектировании систем физической защиты с использованием нечеткого логического вывода / А.С. Боровский, А.Д. Тарасов // Вестник компьютерных и информационных технологий. – №4(94). 2012. – С. 47–53.

9. Боровский, А.С. Приближенная оценка защищенности потенциально-опасных объектов. Структурные параметры защищенности объектов / А.С. Боровский, А.Д. Тарасов // Программные продукты и системы. – №3(103). 2013 г. – С. 235–243.

10. Боровский, А.С. Автоматизированное проектирование систем физической защиты на основе функциональной и структурно – логической потоковых моделях / А.С. Боровский, А.Д. Тарасов // Информационные технологии, теоретический и прикладной научно-технический журнал. – №6(202). 2013 г. – С. 43–48.

11. Тарасов, А.Д. Адаптивный генетический алгоритм в задаче проектирования систем физической защиты критически важных объектов / А.Д. Тарасов // Вестник компьютерных и информационных технологий. – №1(139). 2016 г. – С. 23–31.

12. Тарасов, А.Д. Эффективность работы генетического алгоритма в задаче проектирования систем физической защиты / А.Д. Тарасов // Информационные технологии, теоретический и прикладной научно-технический журнал. – Том 22, №4. 2016 г. – С. 243–249.

13. Боровский, А.С. Программный комплекс информационной поддержки решения задачи проектирования системы физической защиты / А.С. Боровский, А.Д. Тарасов // Системы управления и информационные технологии. – №4.1(66). 2016 г. – С. 122–128.

Публикации в других изданиях

14. Боровский, А.С. Использование методов нечеткой логики для моделирования объектов и процессов систем физической защиты / А.С. Боровский, А.Д. Тарасов // Материалы IV международной научно-технической конференции «Информационные технологии в науке, образовании и производстве», г. Орел, 22–23 апреля 2010 г. – В 5-ти т. Т. 2 / под общ. ред. д-ра техн. наук проф. И.С. Константинова. – Орел: ОрелГТУ, 2010. – 200 с.

15. Тарасов, А.Д. Система физической защиты на основе агентно-ориентированного подхода и нечеткой логики / А.Д. Тарасов // Труды XII Международной конференции «Проблемы управления и моделирования в

сложных системах» (21–23 июня 2010 г., Самара) – Самарский научный центр РАН, 2010. – С. 650–656.

16. Тарасов, А.Д. Анализ защищенности объекта с помощью лингвистической модели принятия решений / А.Д. Тарасов // Труды XIII Международной конференции «Проблемы управления и моделирования в сложных системах» (15–17 июня 2011 г., Самара) – Самарский научный центр РАН, 2011. – С. 539–546.

17. Боровский, А.С. Поиск стратегии управления по нечетким ситуационным сетям для принятия проектных решений в системе физической защиты объектов / А.С. Боровский, А.Д. Тарасов // Materiály VIII mezinárodní vědecko – praktická conference «Dny vědy – 2012», 27 марта – 5 апреля 2012 г. – Díl 82. Matematika: Praha. Publishing House «Education and Science», 2012. – 96 stran.

18. Тарасов, А.Д. Математические методы обработки нечеткой информации в задаче оценки защищенности потенциально-опасных объектов / А.Д. Тарасов // Труды XV Международной конференции «Проблемы управления и моделирования в сложных системах» (25–28 июня 2013 г., Самара) – Самарский научный центр РАН, 2013. – С. 153–165.

19. Боровский, А.С. Методы и алгоритмы в задачах проектирования систем физической защиты объектов информатизации на основе обработки нечеткой информации / А.С. Боровский, А.Д. Тарасов // Труды Пятой Международной научной конференции «Информационные Технологии и Системы» 24–28 февраля 2016 г. – Челябинск: Издательство Челябинского государственного университета, 2016. – С. 168–172.

20. Костин, В.Н. Проблемы и задачи концептуального проектирования систем физической защиты критически важных объектов / В.Н. Костин, А.С. Боровский, А.Д. Тарасов // Новые информационные технологии и системы: сб. науч. ст. XIII Междунар. науч.-техн. конф. (г. Пенза, 23–25 ноября 2016 г.). – Пенза : Изд-во ПГУ, 2016. – С. 215–217.

21. Тарасов, А.Д. Адаптивный генетический алгоритм в задаче проектирования систем физической защиты / А.Д. Тарасов, А.С. Боровский, В.Н. Костин // Новые информационные технологии и системы: сб. науч. ст. XIII Междунар. науч.-техн. конф. (г. Пенза, 23–25 ноября 2016 г.). – Пенза : Изд-во ПГУ, 2016. – С. 226–228.

Свидетельства о регистрации программ для ЭВМ

22. Алгоритм моделирования предметной области проектирования систем физической защиты объектов с использованием экспертной информации в нечеткой форме. Свидетельство о регистрации электронного ресурса №17490 / А.С. Боровский, А.Д. Тарасов; Зар. в Институте научной информации и мониторинга – Объединенный фонд электронных ресурсов «Наука и образование» 11.10.2011 г. – 2 с.

23. Свидетельство № 2012612863 Российская Федерация FuzzyConclusion: свидетельство о государственной регистрации программы для ЭВМ / А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2012610792; заявл. 08.02.2012; зарегистр. 22.03.2012. – 1 с.

24. Свидетельство № 2012618396 Российская Федерация DefencePath: свидетельство о государственной регистрации программы для ЭВМ / А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2012616362; заявл. 26.07.2012; зарегистр. 17.09.2012. – 1 с.

25. Свидетельство № 2013614186 Российская Федерация SFZproject: свидетельство о государственной регистрации программы для ЭВМ / Н.А. Арзамасков, А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2013611729; заявл. 05.03.2013; зарегистр. 25.04.2013. – 1 с.

26. Свидетельство № 2013619591 Российская Федерация Hypergraphmodel: свидетельство о государственной регистрации программы для ЭВМ / Н.А. Арзамасков, А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2013617325; заявл. 13.08.2013; зарегистр. 10.10.2013. – 1 с.

27. Свидетельство № 2013619592 Российская Федерация ItsoEquip: свидетельство о государственной регистрации программы для ЭВМ / Н.А. Арзамасков, А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2013617322; заявл. 13.08.2013; зарегистр. 10.10.2013. – 1 с.

28. Свидетельство № 2014615742 Российская Федерация GenalgSfz: свидетельство о государственной регистрации программы для ЭВМ / А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2014613355; заявл. 15.04.2014; зарегистр. 02.06.2014. – 1 с.

29. Свидетельство № 2015612261 Российская Федерация GenalgFuzzy: свидетельство о государственной регистрации программы для ЭВМ / А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2014664199; заявл. 31.12.2014; зарегистр. 16.02.2015. – 1 с.

30. Свидетельство № 2015660282 Российская Федерация Оптимальное размещение ИТСО на территории защищаемого объекта – адаптивный генетический алгоритм GenalgSfz2: свидетельство о государственной регистрации программы для ЭВМ / А.Д. Тарасов, А.С. Боровский; заявитель и правообладатель ФГБОУ ВПО Оренб. гос. агр. ун-т. – № 2015616967; заявл. 29.07.2015; зарегистр. 25.09.2015. – 1 с.

Диссертант  Тарасов А.Д.