УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

УДК 658.29-049.5

МАЛИКОВ
Владимир Викторович

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СИСТЕМ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Минск 2010

Работа выполнена в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **Борботько Тимофей Валентинович**, кандидат технических наук, доцент, доцент кафедры защиты информации учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Официальные оппоненты: **Голенков Владимир Васильевич**, доктор технических наук, профессор, заведующий кафедрой интеллектуальных информационных технологий учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Хижняк Александр Вячеславович, кандидат технических наук, доцент, заведующий кафедрой автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь»

Оппонирующая организация: Открытое акционерное общество **«АГАТ-СИСТЕМ»** (г. Минск)

Защита состоится « 11 » ноября 2010 г. в 16^{00} часов на заседании совета по защите диссертаций Д 02.15.06 при учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, г. Минск, ул. П. Бровки, 6, корп. 1,

КРАТКОЕ ВВЕДЕНИЕ

В настоящее время обеспечение информационной и инженерно-технической защиты критически важных объектов (КВО) является одной из приоритетных задач современного общества. Данная проблема приобретает сегодня особую значимость и для Республики Беларусь в связи с научным и технологическим развитием в промышленности, проектированием и строительством собственной атомной станции, а также иных объектов государственной важности с режимом ограниченного доступа.

Проблема информационной и инженерно-технической безопасности КВО заключается в следующем: создатель объекта и его составляющих, в том числе средств автоматизации, стремиться к обеспечению наибольшей эффективности объекта. Однако, ввиду наличия угроз информационной и инженерно-технической безопасности КВО, разработчик систем защиты независимо от его решений вынужден снижать эффективность объекта. Для того чтобы степень снижения эффективности лежала в рамках допустимых значений, целесообразно выполнение следующих мероприятий:

- объединение информационной и инженерно-технической подсистем защиты в единую систему безопасности;
- разработка новой системы управления, позволяющей обеспечить поддержку и принятие решений по функционированию системы защиты;
- внедрение новых систем защиты и модернизация существующих должна быть экономически целесообразной, что требует разработки методик оценки их эффективности.

Актуальность работы состоит в решении наиболее важных составляющих указанной выше проблемы.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Связь работы с крупными научными программами (проектами) и темами

Работа выполнялась в Учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» в период с 2006 по 2010 гг. в рамках:

- научно-исследовательской работы: «Исследование вариантов и выбор структуры модернизированной системы передачи информации о проникновении и пожаре «АСОС Алеся» с учетом особенностей и специфики охраняемых в республике объектов на современном этапе» в рамках Государственной комплексной программы научных исследований «Национальная безопасность» - «Исследование особенностей и разработка алгоритмов функционирования и

программно-технических средств для силовых ведомств с целью их использования в телекоммуникационных системах с общим и санкционированным доступом» (2006 - 2009 гг., № г.р. 20066846);

научно-исследовательской работы: «Разработка и согласование с заинтересованными организациями «Концепции информационной безопасности развития и функционирования атомной энергетики Республики Беларусь» в соответствии с нормативной базой Республики Беларусь и рекомендациями МАГАТЭ, а также нормативные, методические и организационные мероприятия и НИОКР по реализации Концепции» (2010 г., № г.р. 20100177) в рамках Государственной программы «Научное сопровождение развития атомной энергетики в Республике Беларусь на 2009 - 2010 годы и на период до 2020 года» (Постановление Совета Министров Республики Беларусь от 28.08.2009 г. № 1116).

Тема диссертационной работы соответствует приоритетным направлениям фундаментальных и прикладных исследований Республики Беларусь в области информационной и инженерно-технической безопасности, создания современных системы защиты информации.

Основные результаты работы включены в учебные программы:

1. Повышения квалификации работников военизированной охраны гражданской авиации в Учреждении образования «Минский государственный высший авиационный колледж» в 2008 - 2009 гг.

2. Повышения квалификации сотрудников подразделений Департамента охраны МВД Республики Беларусь в Учреждении образования «Учебный центр Департамента охраны» МВД Республики Беларусь в 2008 - 2010 гг.

3. Первоначальной подготовки военнослужащих Службы безопасности Президента Республики Беларусь в Учреждении образования «Учебный центр Департамента охраны» МВД Республики Беларусь в 2008 - 2009 гг.

Цель и задачи исследования

Целью работы является разработка методики проектирования системы информационной и инженерно-технической защиты критически важных объектов и методического подхода к формированию требований по их комплексной защите и оценке эффективности.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ статистических данных по современным методам и средствам обеспечения информационной и инженерно-технической защиты критически важных объектов от несанкционированного доступа.

2. Разработать методику проектирования системы информационной и инженерно-технической защиты критически важных объектов.

3. Разработать методический подход к формированию требований по информационной и инженерно-технической защите критически важных объектов.

4. Провести оценку эффективности информационных и инженерно-технических систем защиты критически важных объектов.

Объектом исследования являются информационные и инженерно-технические системы защиты критически важных объектов.

Предметом исследования является методика построения комплексной системы информационной и инженерно-технической защиты критически важных объектов.

Положения, выносимые на защиту:

1. Методика построения комплексной системы информационной и инженерно-технической защиты критически важных объектов, основанная на реализации системой защиты оперативного аудита реальных и прогнозирования потенциальных угроз критически важным объектам, обеспечении их оперативной локализации и ликвидации, чем достигается предотвращение несанкционированного доступа к объекту и тем самым снижается риск нанесения ущерба защищаемому объекту.

2. Методика классификации критически важных объектов, основанная на группировании объектов по критерию близости как по определяющему показателю - доступ к объекту, так и по таким классификационным показателям и численным значениям их параметров как значимость объекта и его ресурсов, структура управления, функционально-экономическая организация, оценка риска, что позволяет в последующем обосновано и конкретизировано формулировать на базе современных нормативных документов требования к информационной и инженерно-технической защите критически важных объектов от несанкционированного доступа, который может привести к причинению экономического ущерба и/или возникновению чрезвычайных ситуаций радиационного, биологического или социально-политического характера.

3. Методический подход и программное обеспечение на его основе, предназначенные для проектирования комплексной системы информационной и инженерно-технической защиты критически важных объектов и оценки ее эффективности, которые позволяют проводить динамическую коррекцию параметров системы для оптимизации конфигурации профилей защиты со снижением затрат времени на проектирование систем комплексной защиты до 20% и уменьшением экономических затрат на средства и системы защиты критически важных объектов до 15%.

Личный вклад соискателя

Основные научные и практические результаты диссертационной работы, а также положения, выносимые на защиту, разработаны и получены лично автором.

В совместно опубликованных работах автору принадлежат: методика проектирования системы информационной и инженерно-технической защиты критически важных объектов, а также методический подход к формированию требований по их комплексной защите. Соавторами основных публикаций являются научный руководитель, к.т.н., доцент Борботько Т. В. который осуществлял определение целей и постановку задач исследования, выбор методов исследований, принимал участие в планировании работ и обсуждении результатов, а также д.т.н., профессор Лыньков Л. М., который осуществлял научное редактирование материалов монографии.

Апробация результатов диссертации

Материалы, вошедшие в диссертационную работу, докладывались и обсуждались на III, IV, VI, VII, VIII Белорусско-российских научно-технических конференциях «Технические средства защиты информации» (Минск, 2005, 2006, 2008, 2009, 2010 гг.); XII, XIII, XIV Международных научно-технических конференциях «Современные средства связи» (Минск, 2007, 2008, 2009 гг.); 3, 4 Международных научных конференциях по военно-техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения (Минск, 2007, 2009 гг.); VI, VII Международных научно-практических конференциях «Управление информационными ресурсами» (Минск, 2008, 2009 гг.).

Опубликованность результатов диссертации

Материалы по теме диссертации опубликованы в 5-ти научных работах (8,9 авторских листа), соответствующих п. 18 Положения о присуждении ученых степеней и присвоении ученых званий в Республике Беларусь, включая:

- 4 статьи в научных журналах, из них 3 в соавторстве. Автору принадлежит - 2,1 авторских листа.
- 1 монография в соавторстве. Автору принадлежит - 6,8 авторских листа.

Опубликовано 8 статей в материалах конференций, 5 тезисов докладов в сборниках тезисов конференций, а также 4 статьи в научно-технических сборниках и журналах, 1 производственно-практическое пособие (рецензируемое).

Структура и объем диссертации

Диссертация состоит из введения, общей характеристики работы, четырех глав с краткими выводами по каждой главе, заключения, списка использованных источников и пяти приложений, оформленных в виде отдельной части.

В первой главе проведен анализ статистических данных по современным методам и средствам обеспечения информационной и инженерно-технической защиты критически важных объектов от несанкционированного доступа. Во второй главе предложена методика проектирования системы информационной и инженерно-технической защиты критически важных объектов. В третьей главе представлены результаты разработки методического подхода к формированию требований по информационной и инженерно-технической защите критически важных объектов. В четвертой главе проведена оценка эффективности информационной и инженерно-технической защиты критически важных объектов.

Общий объем диссертационной работы составляет 174 страницы, из которых 85 страниц основного текста. Она включает 30 рисунков на 23 страницах, 36 таблиц на 53 страницах, библиографию из 134 наименований (из них 23 собственные публикации соискателя) на 13 страницах.

Приложения оформлены в виде отдельной части: 5 приложений на 218 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** приведена область исследования диссертационной работы и обоснована ее актуальность.

В **общей характеристике** работы сформулированы цель и задачи работы, изложены основные положения, выносимые на защиту.

В первой главе проведен анализ статистических данных по современным методам и средствам обеспечения информационной и инженерно-технической защиты КВО от несанкционированного доступа и выявлены следующие существенные недостатки:

- отсутствие единых концептуальных подходов в решении задач обеспечения защиты КВО;
- до настоящего времени не определены, как методические, так и практические основы по порядку выбора и применения типовых аппаратно-программных и инженерно-технических средств и систем защиты КВО;
- отсутствие научно обоснованной системы показателей и критериев принятия решений, а также методических основ проектирования систем защиты КВО;
- отсутствие классификации КВО по комплексным показателям информационной и инженерно-технической защиты КВО;
- до настоящего времени не разработан единый каталог требований для его применения к типовой группе КВО, сформированной из объектов, близких по определенному перечню параметров или характеристик;

- не определены требования по информационной и инженерно-технической защите КВО;

- не разработан единый методологический подход по оценке эффективности защиты КВО от несанкционированного доступа.

Во второй главе предложена методика проектирования системы информационной и инженерно-технической защиты КВО. Для анализа общей ситуации в области информационной и инженерно-технической защиты объектов проведено «Статистическое исследование в области информационной и инженерно-технической защиты объектов от несанкционированного доступа в Республике Беларусь», по результатам которого, в качестве системообразующего документа в области информационной и инженерно-технической безопасности КВО предложен проект «Концепции обеспечения безопасности критически важных объектов в Республике Беларусь», позволяющий сформировать концептуальные основы проектирования систем информационной и инженерно-технической защиты КВО.

Разработаны методические основы выбора и применения типовых аппаратно-программных и инженерно-технических средств и систем защиты КВО: базовой операционной системы, систем управления базами данных, аппаратно-программных средств и систем защиты информации, технических средств и систем охраны, средств противопожарной защиты и оповещения, средств инженерно-технической укрепленности, автоматических систем контроля и управления доступом, систем охранного телевидения, каналов сопряжения и коммуникации. Проведенные исследования показали, что эффективность проектирования комплексных систем защиты, в том числе за счет использования разработанных методических основ, позволяет получить значительный экономический эффект за счет снижения до 20 % от времени необходимого для существующего типового проектирования систем защиты.

Предложена методика построения комплексной (11 видов систем охраны и жизнеобеспечения) системы информационной и инженерно-технической защиты КВО, основанная на оперативном аудите угроз для объекта, позволяющая обеспечить их локализацию и предотвратить развитие вторжения на территорию объекта при введении объединенной (до 4-х служб) оперативно-дежурной службы, охватывающей не менее 90% территории Республики, а также существенно снизить уязвимость КВО и его информационной системы (рисунок 1). Предлагаемая структура распределенной системы информационной и инженерно-технической защиты КВО состоит из трех уровней: объектового, каналов сопряжения и телекоммуникации, обеспечения и управления безопасностью. Для обеспечения эффективного управления распределенной системой информационной и инженерно-технической защиты КВО введены 5 специализированных служебных сигналов: $СИС_{1,2,3}$, $СИС_{СПИ}$, РИПС.

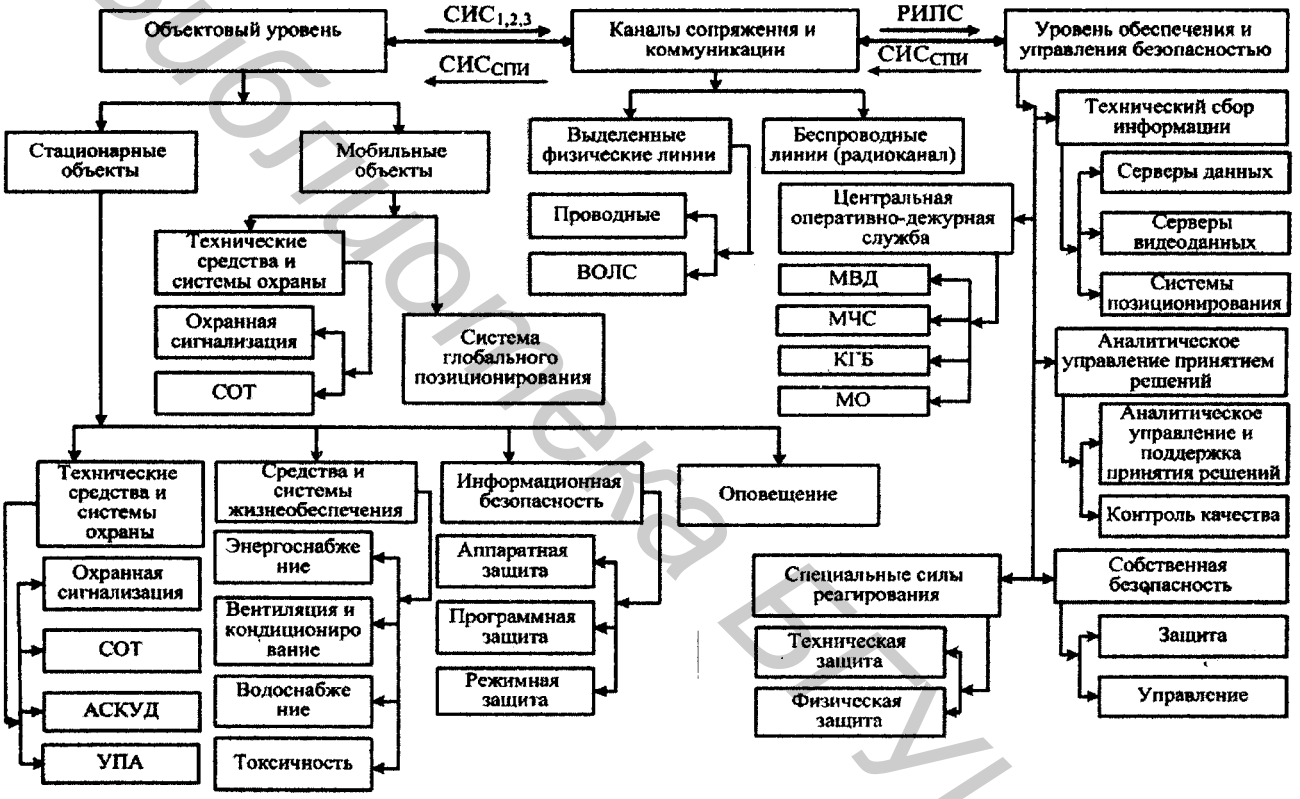

Рисунок 1 – Структурная схема разработанной комплексной системы защиты КВО

В целях снижения общих затрат на проектирование, мониторинг, техническое обслуживание средств и систем защиты для крупных организаций, ведомств Республики Беларусь, а также обеспечения должного реагирования на сигналы «тревога», предложено построение системы информационной и инженерно-технической защиты КВО на базе эксплуатируемой системы АСОС «Алеся» Департамента охраны МВД Республики Беларусь (рисунок 2).

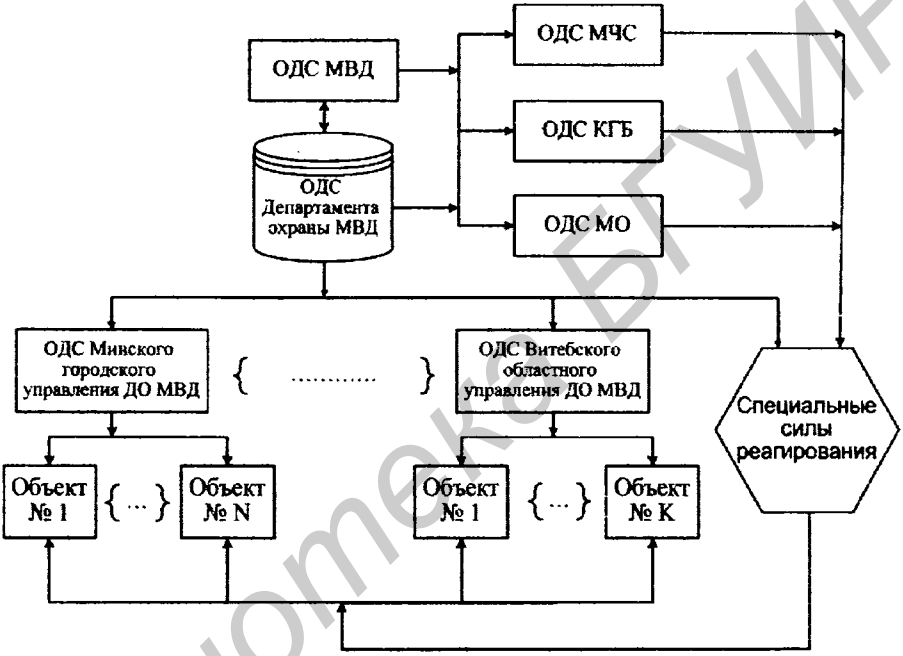

Рисунок 2 – Структура управления информационной и инженерно-технической защитой КВО

На примере Республики Беларусь предложено следующее построение территориальной структуры системы информационной и инженерно-технической защиты КВО: главный (республиканский) центр (г. Минск), областные центры, районные центры мониторинга и управления.

В третьей главе предложен методический подход к формированию требований по информационной и инженерно-технической защите КВО, в рамках которого разработана методика классификации КВО (рисунок 3), основанная на группировании объектов по критерию близости как по определяющему показателю - доступ к объекту, так и по таким классификационным показателям и численным значениям их параметров как

значимость объекта и его ресурсов, структура управления, функционально-экономическая организация, оценка риска нанесенного ущерба.

Рисунок 3 – Схема проведения классификации КВО по комплексным показателям информационной и инженерно-технической защиты с учетом особенностей доступа

Результаты проведенной классификации объектов приведены в таблице (знак «Х» - параметр показателя присутствует).

Разработаны комплексные требования по защите КВО, учитывающие существующие каталоги по информационной безопасности, и накопленный багаж требований по инженерно-технической защите таких объектов. Данные требования включают в себя как краткую характеристику КВО как объекта защиты, так и описание среды защиты КВО в целом.

Таблица - Классификация объектов с учетом особенностейдоступа к ним

Показатель	Параметр показателя	Категории объектов (критерий близости – уровень доступа)				
		Упрощенный доступ	Ограниченный доступ	Важный доступ (КВО)	Доступ с расширенной защитой (КВО)	Доступ с максимальной защитой (КВО)
1. Организационная структура управления объектом	1.1 Республиканский уровень	-	-	-	x	x
	1.2 Региональный уровень	-	x	x	-	-
	1.3 Местный уровень	x	-	-	-	-
2. Функционально-экономическая организация процесса деятельности	2.1 Деятельность не регулируется государством	x	-	-	-	-
	2.2 Деятельность частично регулируется государством	x	x	-	-	-
	2.3 Деятельность регулируется государством	-	x	x	x	x
3. Риск нанесения ущерба	3.1 Особо крупный ущерб	-	-	-	-	x
	3.2 Крупный ущерб	-	-	-	x	-
	3.3 Значительный ущерб	-	x	x	-	-
	3.4 Средний ущерб	x	x	-	-	-
	3.5 Мелкий ущерб	x	-	-	-	-

В рамках требований предложен подход и проведена классификация угроз (8 видов, 17 подвидов) для системы информационной и инженерно-технической защиты КВО, основанный на учете этапов их жизненного цикла, который позволяет усовершенствовать процесс проектирования и обеспечить гарантированную защиту КВО (рисунок 4).

Рисунок 4 –Разработанная классификация угроз системы информационной и инженерно технической защиты КВО с учетом этапов ее жизненного цикла

Предложен методический подход по оценке эффективности информационной и инженерно-технической защиты КВО от НСД на основе профилей защиты, который позволяет проводить анализ и динамическую коррекцию результатов оценки, основанный на формировании оценочных матриц угроз и технической оснащенности системы информационной и инженерно-технической защиты КВО, построенных по структуре многоуровневых реляционных баз данных (рисунок 5).

Практическое использование указанного методического подхода позволяет снизить затраты на проектирование (до 20 % от времени необходимого для проектирования комплексных систем защиты) и обеспечить гарантированную защиту КВО).

В качестве показателей эффективности обеспечения безопасности КВО введенными средствами и системами защиты предлагается использование:

1. Технического показателя эффективности средств и систем защиты – $K_{эф/т}$:

- позволяет определить техническую эффективность введенных средств и систем защиты, т.е. вероятность отражения атак (0 ÷ 1);

а) б)

а) схема методического подхода по оценке эффективности;

б) схема формирования оценочной матрицы угроз;

Рисунок 5 – Схема методического подхода по оценке эффективности информационной и инженерно-технической защиты КВО

- определяется на основе оценочной матрицы технической оснащенности информационной и инженерно-технической защиты КВО;

- вероятность успешного отражения атаки примем при $K_{ЭФ/Т} = 0{,}9 \div 1{,}0$;

- обеспечение $K_{ЭФ/Т} = 0{,}9 \div 1{,}0$ является условием проведения дальнейшего анализа по экономическому показателю эффективности;

- общий технический показатель эффективности по h - уровням безопасности определяется как вероятность независимых совместных событий.

2. Экономический показатель эффективности средств и систем защиты - $К_{ЭФ/Э}$:

- позволяет определить экономическую эффективность введенных средств и систем защиты, т.е. соотношение стоимости введенных технических средств и систем защиты $S_{ЗАЩ}$ к суммарной стоимости потерь по ресурсам объекта P, которая определяется критериями: ущерб репутации организации, без-

опасность персонала, разглашение коммерческих сведений, финансовые потери и др.;

- определяется на основе оценочной матрицы угроз иерархической системы информационной и инженерно-технической защиты КВО;

- рекомендуемое значение экономического показателя средств и систем защиты примем равным $K_{Э\Phi/Э} \geq 1$:

$$К_{ЭФ/Э} = \left(\frac{Р \times К_{ЭФ/Т} - S_{защ}}{S_{защ}}\right).$$

В четвертой главе проведена оценка эффективности информационных и инженерно-технических систем защиты КВО, а также разработано программное обеспечение (ПО) для автоматизации методического подхода по оценке эффективности защиты КВО от несанкционированного доступа с учетом разработанных концептуальных основ и методики проектирования системы информационной и инженерно-технической защиты КВО.

Программное обеспечение обеспечивает оценку системы комплексной защиты: оценку уровня угроз и уровня технической оснащенности. Результатом оценки эффективности существующей информационной и инженерно-технической системы защиты КВО будет являться численная оценка параметров эффективности с учетом затрат на обеспечение защиты объектов.

Для обеспечения разграничения доступа к ресурсам ПО предусмотрено введение следующих категорий доступа:

1. Администратор – редактирование структуры и / или оценочных коэффициентов ПО. После внесения изменений в ПО проводится сохранение с указанием номера версии и даты экспертных оценочных баз.

2. Пользователь – доступ к режиму оценки эффективности существующей информационной и инженерно-технической системы защиты объекта (рисунок 6).

В результате проведенных расчетов уровня безопасности двух типовых КВО показано, что затраты (денежное выражение) на обеспечение информационной и инженерно-технической защиты КВО с учетом всех разработанных требований могут превышать расчетный уровень риска нанесенного ущерба (денежное выражение). Проведение оценки эффективности информационной и инженерно-технической защиты КВО рекомендуется проводить по программе аудита средств и систем защиты с отражением результатов в аудиторском заключении.

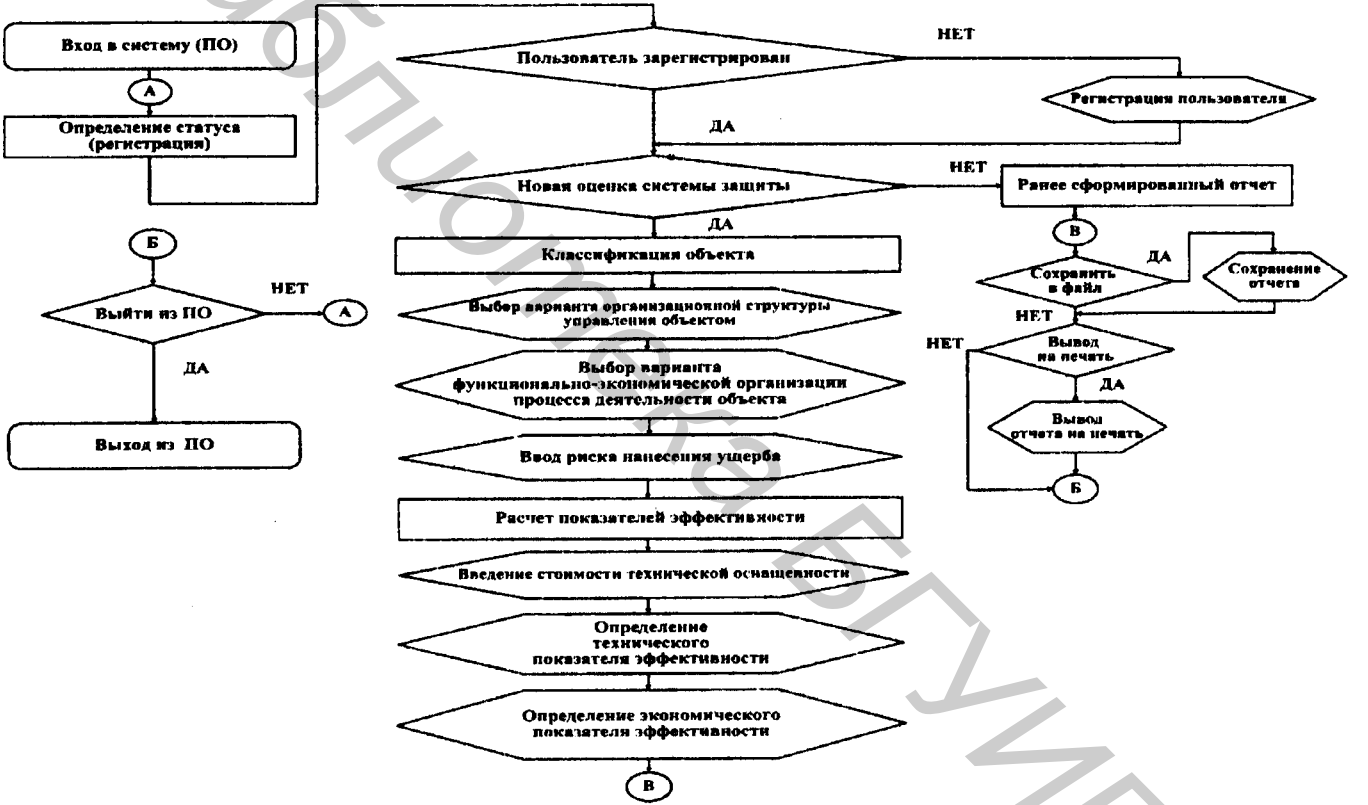

Рисунок 6 – Алгоритм работы ПО в режиме «Пользователь»

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. По результатам проведенного статистического исследования и анализа нормативно-правового обеспечения в области безопасности объектов, в качестве системообразующего документа в области информационной и инженерно-технической безопасности КВО предложен проект «Концепции обеспечения безопасности критически важных объектов в Республике Беларусь», позволяющий сформировать концептуальные основы проектирования систем информационной и инженерно-технической защиты КВО. В рамках Концепции проведен анализ видов угроз безопасности КВО, дана классификация источников угроз безопасности КВО, предложен методический подход по обеспечению безопасности КВО в Республике Беларусь [18-А].

2. Предложена и обоснована (на примере Республики Беларусь) необходимость введения единого информационно-аналитического центра по сбору, отработке и принятию решений по вопросам безопасности (4 оперативно-дежурных службы), что позволяет реализовать эффективную систему защиты КВО, с учетом оперативного аудита реальных и прогнозирования потенциальных угроз КВО, обеспечении их оперативной локализации и ликвидации [2-А, 12-А, 22-А].

3. Предложена методика построения комплексной (11 видов систем охраны и жизнеобеспечения) системы информационной и инженерно-технической защиты КВО [6-А], состоящая из трех уровней: объектового, каналов сопряжения и телекоммуникации, обеспечения и управления безопасностью [6-А, 10-А]. Для обеспечения эффективного управления комплексной системой защиты КВО введены 5 специализированных служебных сигналов [2-А]. Предложены схемы их формирования с учетом обеспечения защиты от угроз конфиденциальности, целостности и доступности по всем трем уровням системы.

4. Разработана методика классификации КВО, основанная на группировании объектов по критерию близости как по определяющему показателю - доступ к объекту, так и по таким классификационным показателям и численным значениям их параметров как значимость объекта и его ресурсов, структура управления, функционально-экономическая организация, оценка риска, что позволяет в последующем обосновано и конкретизировано формулировать на базе современных нормативных документов требования к информационной и инженерно-технической защите КВО от НСД, который может привести к причинению экономического ущерба и /или возникновению чрезвычайных ситуаций радиационного, биологического или социально – политического характера. [3-А].

5. Предложен методический подход по оценке эффективности информационной и инженерно-технической защиты КВО от НСД на основе профилей защиты, который позволяет проводить анализ и динамическую коррекцию результатов оценки [16-А, 21-А], основанный на формировании оценочных матриц угроз и технической оснащенности системы информационной и инженерно-технической защиты КВО, построенных по структуре многоуровневых реляционных баз данных.

6. Предложены формулы математического расчета показателей эффективности защиты КВО на основе использования технического и экономического показателей эффективности, которые позволяют получить численные значения оценки эффективности с учетом затрат на обеспечение защиты [7-А], а также проводить динамическую коррекцию параметров системы для оптимизации конфигурации профилей защиты со снижением затрат времени на проектирование систем комплексной защиты до 20% и уменьшением экономических затрат на средства и системы защиты КВО до 15%.

Рекомендации по практическому использованию результатов

1. Использование разработанных методических основ выбора и применения типовых аппаратно-программных и инженерно-технических средств и систем защиты КВО [8-А, 12-А, 23-А] позволяет систематизировать подход к комплексному проектированию комплексных систем защиты КВО. Проведенные исследования (приложение Д) показали, что эффективность проектирования комплексных систем защиты, в том числе за счет использования разработанных методических основ, позволяет получить значительный экономический эффект за счет снижения до 20 % от времени необходимого для существующего типового проектирования систем защиты.

2. Разработаны комплексные требования по защите КВО, учитывающие существующие каталоги по информационной безопасности, и накопленный багаж требований по инженерно-технической защите таких объектов. Данные требования включают в себя как краткую характеристику КВО как объекта защиты, так и описание среды защиты КВО в целом. В рамках требований предложен подход и проведена классификация угроз (8 видов, 17 подвидов) для системы информационной и инженерно-технической защиты КВО, основанный на учете этапов их жизненного цикла, который позволяет усовершенствовать процесс проектирования и обеспечить гарантированную защиту КВО [15-А].

3. Разработанное программное обеспечение по оценке эффективности системы информационной и инженерно-технической защиты КВО может быть использовано в организациях занимающихся проектированием, аудитом и тендерными изысканиями по комплексным системам защиты объектов, а также для целей подготовки квалифицированных кадров в сфере обеспечения безопасности.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ ПО ТЕМЕ ДИССЕРТАЦИИ

Монография:

1–А. Лыньков, Л.М. Защита объектов различных форм собственности от несанкционированного доступа: монография / Л.М. Лыньков, В.В. Маликов, Т.В. Борботько; под ред. Л.М. Лынькова. – Минск: Полиграфический центр МВД Респ. Беларусь, 2008. – 187 с.

Статьи в научных журналах:

2–А. Маликов, В.В. Многоаспектная распределенная корпоративная система безопасности функционирования объектов / В.В. Маликов, Т.В. Борботько // Вестник Военной академии Респ. Беларусь. – 2007. – № 4 (17). – С. 128 – 132.

3–А. Маликов, В.В. Профили безопасности объектов различных форм собственности / В.В. Маликов // Доклады БГУИР. – 2009. – № 2 (40). – С. 99 – 104.

4–А. Маликов, В.В. Классификация угроз иерархической системы информационной и инженерно-технической защиты объектов от несанкционированного доступа / В.В. Маликов, Т.В. Борботько // Инженерный вестник. – 2009. – № 1 (27). – С. 69 – 72.

5–А. Маликов, В.В. Метод оценки эффективности иерархической системы информационной и инженерно-технической защиты объектов от несанкционированного доступа / В.В. Маликов, Т.В. Борботько // Доклады БГУИР. – 2009. – № 8 (46). – С. 119 – 123.

Статьи в научно-технических сборниках и журналах:

6–А. Маликов, В.В. Разработка структуры многоаспектной системы безопасности функционирования объектов / В.В. Маликов // Сетевые решения. – 2007. – № 10. – С. 9 – 15.

7–А. Маликов, В.В. Профили защиты безопасности функционирования объектов и методы их оценки / В.В. Маликов // Сетевые решения. – 2008. – № 4. – С. 68 – 80.

8–А. Маликов, В.В. Проблемы обеспечения комплексной информационной и инженерно – технической защиты объектов / В.В. Маликов // Технологии безопасности. – 2009. – № 1 (4). – С. 46 – 47.

9–А. Маликов, В.В. Методика классификации угроз иерархической системы комплексной защиты объектов различных категорий / В.В. Маликов // Безопасность. Достоверность. Информация. – 2009. – № 3–4 (84–85). – С. 18 – 21.

Статьи в материалах конференций:

10–А. Маликов, В.В. Интегрированные системы технических средств охраны банковских учреждений / В.В. Маликов // Технические средства защиты информации: материалы докладов и краткие сообщения 3–ей Белорусско–российской НТК, Минск, 23 – 27 мая 2005 г. / БГУИР; редкол.: М.П. Батура [и др.]. – Минск, 2005. – С. 89 – 90.

11–А. Маликов, В.В. Проблемы обеспечения безопасности банковских учреждений техническими средствами охраны в Республике Беларусь / В.В. Маликов // Технические средства защиты информации: материалы докладов и краткие сообщения 4–ой Белорусско–российской НТК, Минск, 29 мая – 2 июня 2006 г. / БГУИР; редкол.: В.Ф. Голиков [и др.]. – Минск, 2006. – С. 62 – 64.

12–А. Маликов, В.В. Использование систем цифровой видеорегистрации сигнала в обеспечении безопасности банковских учреждений / В.В. Маликов // Современные информационные технологии: материалы докладов и краткие сообщения IX Международной школы–семинара аспирантов, магистрантов и студентов, Браслав, 2-8 июля 2006 г. / БГУИР; редкол.: М.П. Батура [и др.]. – Минск, 2006. – С. 167 – 169.

13–А. Маликов, В.В. Безопасность функционирования объектов / В.В. Маликов // Современные средства связи: материалы 12–ой Международной НТК, Минск, 24 – 28 сентября 2007 г. / ВГКС; редкол.: М.А. Баркун [и др.]. – Минск, 2007. – С. 107 – 108.

14–А. Маликов, В.В. Обеспечение гарантированной безопасности функционирования объектов с применением профилей защиты / В.В. Маликов // Управление информационными ресурсами: материалы 6–ой международной НПК, Минск, 24 апреля 2008 г. / Акад. упр. при Президенте Респ. Беларусь; редкол.: А.С. Гринберг [и др.]. – Минск, 2008. – С. 180 – 182.

15–А. Маликов, В.В. Методика оценки угроз и анализа рисков многоаспектной распределенной корпоративной системы безопасности объектов / В.В. Маликов // Современные средства связи: материалы 13–ой Международной НТК, Минск, 7 – 9 октября 2008 г. / ВГКС; редкол.: М.А. Баркун [и др.]. – Минск, 2008. – С. 177 – 178.

16–А. Маликов, В.В. Оценка эффективности системы информационной и инженерно–технической защиты объектов различных категорий / В.В. Маликов // Современные средства связи: материалы 14–ой Международной НТК, Минск, 29 сентября – 1 октября 2009 г. / ВГКС; редкол.: М.А. Баркун [и др.]. – Минск, 2009. – С. 171.

17–А. Маликов, В.В. Разработка иерархической структуры управления информационной и инженерно–технической защитой объектов различных категорий / В.В. Маликов // Управление информационными ресурсами: материалы 7–ой международной НПК, Минск, 25 ноября 2009 г. / Акад. упр. при Прези-

денте Респ. Беларусь; редкол.: В.А. Богуш [и др.]. – Минск, 2009. – С. 193 – 194.

Тезисы докладов:

18–А. Маликов, В.В. Разработка концепции безопасности корпоративных систем / В.В. Маликов // 3–я Международная научная конференция по военно–техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения: тез. докл., Минск, 23–24 мая 2007 г. / ГУ «БелИСА»; редкол.: В.Е. Кратенок [и др.]. – Минск, 2007. – С. 41 – 43.

19–А. Маликов, В.В. Методика формирования и оценки профилей защиты / В.В. Маликов // Технические средства защиты информации: материалы докладов и краткие сообщения 6–ой Белорусско–российской НТК, Минск, 21 – 22 мая 2008 г. / БГУИР; редкол.: В.Ф. Голиков [и др.]. – Минск, 2008. – С. 95.

20–А. Маликов, В.В. Обеспечение эффективной информационной и инженерно–технической защиты объектов различных форм собственности / В.В. Маликов // 4–ая Международная научная конференция по военно–техническим проблемам, проблемам обороны и безопасности, использованию технологий двойного применения: тез. докл., Минск, 20–21 мая 2009 г. / ГУ «БелИСА»; редкол.: В.Е. Кратенок [и др.]. – Минск, 2009. – С. 269 – 271.

21–А. Маликов, В.В. Комплексная система защиты объектов различных категорий / В.В. Маликов // Технические средства защиты информации: материалы докладов и краткие сообщения 7–ой Белорусско–российской НТК, Минск, 23 – 24 июня 2009 г. / БГУИР; редкол.: Л.М. Лыньков [и др.]. – Минск, 2009. – С. 8.

22–А. Маликов, В.В. Разработка структуры управления информационной и инженерно-технической защитой объектов / В.В. Маликов, Е.В. Якименко // Технические средства защиты информации: тезисы докладов 8-ой Белорусско–российской НТК, Браслав, 24 – 28 мая 2010 г. / БГУИР; редкол.: Л.М. Лыньков [и др.]. – Минск, 2010. – С. 125 – 126.

Производственно-практическое пособие:

23–А. Маликов, В.В. Технические средства и системы охраны: нормативное произв. – практич. пособие / В.В. Маликов. – Минск: Бестпринт, 2009. – 78 с.

РЭЗЮМЭ

Малікаў Уладзімір Віктаравіч

Павышэнне эфектыўнасці інфармацыйных і інжынерна-тэхнічных сістэм абароны крытычна важных аб'ектаў

Ключавыя словы: крытычна важны аб'ект, методыка праектавання, методыка класіфікацыі, профіль абароны, класіфікацыя пагроз, этапы жыццёвага цыкла, ацэнка эфектыўнасці.

Мэта работы: распрацоўка методыкі праектавання сістэмы інфармацыйнай і інжынерна-тэхнічнай абароны крытычна важных аб'ектаў, а таксама метадычнага падыходу да фарміравання патрабаванняў па іх комплекснай абароне і ацэнцы эфектыўнасці.

Метады даследавання: аналітычна-разліковы метад, метад экспертных ацэнак, статыстычнае даследаванне, функцыянальна-вартасны аналіз.

Атрыманыя вынікі і іх навізна: распрацаваны адзіны падыход у пытаннях пабудовы і ацэнкі эфектыўнасці комплексных сістэм інфармацыйнай і інжынерна-тэхнічнай абароны для крытычна важных аб'ектаў з улікам аператыўнага аўдыту рэальных і прагназавання патэнцыйных пагроз крытычна важным аб'ектам, забеспячэнні іх аператыўнай лакалізацыі і ліквідацыі. Распрацавана методыка класіфікацыі крытычна важных аб'ектаў, заснаваная на групаванні аб'ектаў па крытэры блізкасці як па вызначае паказчыку - доступ да аб'екта, так і па такіх класіфікацыйным паказчыках і лікавым значэнняў іх параметраў як значнасць аб'екта і яго рэсурсаў, структура кіравання, функцыянальна-эканамічная арганізацыя, ацэнка рызыкі. Прапанаваны метадычны падыход і праграмнае забеспячэнне, распрацаванае на яго аснове, прызначаныя для праектавання комплекснай сістэмы абароны крытычна важных аб'ектаў і ацэнкі яе эфектыўнасці.

Рэкамендацыі па выкарыстанні: вынікі работы могуць быць выкарыстаны для фарміравання комплексных патрабаванняў па абароне крытычна важных аб'ектаў, а таксама для ацэнкі эфектыўнасці інфармацыйных і інжынерна-тэхнічных сістэм абароны такіх аб'ектаў ад несанкцыянаванага доступу.

Вобласці ўжывання: праектаванне, аўдыт і тэндэрныя пошукі па сістэмах інфармацыйнай і інжынерна-тэхнічнай абароны крытычна важных аб'ектаў ад несанкцыянаванага доступу, а таксама для мэт падрыхтоўкі кваліфікаваных кадраў у сферы забеспячэння бяспекі.

РЕЗЮМЕ

Маликов Владимир Викторович

Повышение эффективности информационных и инженерно-технических систем защиты критически важных объектов

Ключевые слова: критически важный объект, методика проектирования, методика классификации, профиль защиты, классификация угроз, этапы жизненного цикла, оценка эффективности.

Цель работы: разработка методики проектирования системы информационной и инженерно-технической защиты критически важных объектов, а также методического подхода к формированию требований по их комплексной защите и оценке эффективности.

Методы исследования: аналитически-расчетный метод, метод экспертных оценок, статистическое исследование, функционально-стоимостной анализ.

Полученные результаты и их новизна: разработан единый подход в вопросах построения и оценки эффективности комплексных систем информационной и инженерно-технической защиты для критически важных объектов с учетом оперативного аудита реальных и прогнозирования потенциальных угроз критически важным объектам, обеспечения их оперативной локализации и ликвидации. Разработана методика классификации критически важных объектов, основанная на группировании объектов по критерию близости как по определяющему показателю - доступ к объекту, так и по таким классификационным показателям и численным значениям их параметров как значимость объекта и его ресурсов, структура управления, функционально-экономическая организация, оценка риска. Предложен методический подход и программное обеспечение, разработанное на его основе, предназначенные для проектирования комплексной системы защиты критически важных объектов и оценки ее эффективности.

Рекомендации по использованию: результаты работы могут быть использованы для формирования комплексных требований по защите критически важных объектов, а также для оценки эффективности информационных и инженерно-технических систем защиты таких объектов от несанкционированного доступа.

Область применения: проектирование, аудит и тендерные изыскания по системам информационной и инженерно-технической защиты критически важных объектов от несанкционированного доступа, а также для целей подготовки квалифицированных кадров в сфере обеспечения безопасности.

THE ABSTRACT

Malikov Vladimir Viktorovich

Increasing of efficiency of information and technical systems of critically importance object protection

Keywords: critically importance object, design technique, classification technique, protection profile, threat classification, life cycle stages, performance evaluation.

The research purpose: a design technique development of information and technical protection system of critically importance object, and also the methodical approach to forming requirements on their complex protection and performance evaluation.

Research methods: analytically-design method, expert evaluation method, statistical investigation, functional-cost analysis.

The received results and their novelty: a general approach in questions of design and performance evaluation of complex systems of information and technical protection is developed for critically importance object taking into account on-line audit of predictions of real and potential critically importance object threats, and also support of their on-line localization and elimination. The classification technique of the critically importance object based on grouping objects by similarity criterion as a index which defines the access to object, and also classification indexes and their numerical values as object significance and its resources, management structure, the functional-economic organization, a risk assessment is developed. The methodical approach and the software developed on its basis are used to design complex system of critically importance object protection and its efficiency estimation are proposed.

Usage considerations: work results can be used for forming complex requirements on critically importance object protection, and also for information and technical systems performance evaluation of such object protection from illegal access.

Application field: designing, audit and tender researches on systems of information and technical protection of critically importance object from illegal access, and also for objectives of qualified personnel preparation in security field.

Научное издание

Маликов Владимир Викторович

ПОВЫШЕНИЕ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННЫХ И ИНЖЕНЕРНО-ТЕХНИЧЕСКИХ СИСТЕМ ЗАЩИТЫ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Автореферат
диссертации на соискание ученой степени
кандидата технических наук

по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность

Подписано в печать 04.10.2010. Формат 60x84 1/16. Бумага офсетная.
Гарнитура «Таймс». Отпечатано на ризографе. Усл. печ. л. 1,63.
Уч.-изд. л. 1,4. Тираж 60 экз. Заказ 690.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6.