ВОРОНЕЖСКИЙ ИНСТИТУТ МВД РОССИИ

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ЦЕНТРОВ

Методические рекомендации

Воронеж
2023

ББК 22.1
УДК 519.6

Коллектив авторов: С.А. Гречаный, А.В. Сидоров, О.В. Толстых, Ю.С. Никитина

Рецензенты: Е.В. Спиридонов, начальник ФГКУ «УВО ВНГ России по Воронежской области», полковник полиции;
З.Г. Омаров, начальник УВО по г. Махачкале – филиала «УВО ВНГ России по Республике Дагестан», полковник полиции.

Разработка математической модели оценки эффективности системы безопасности информационных центров: методические рекомендации [Электронный ресурс] / С.А. Гречаный [и др.]. // Воронеж: Воронежский институт МВД России – 2023 г. – 39 с.

Методические рекомендации посвящены вопросам организации безопасности информационных центров. В работе проанализированы нормативные документы, регламентирующие организацию охраны информационных центров, проблемы и перспективные направления развития технической оснащенности информационных центров; разработана структурно-параметрическая модель системы безопасности и программа их реализации, обеспечивающие оценку эффективности системы безопасности информационных центров в интересах выбора оптимального варианта.

Издание предназначено для курсантов и слушателей Воронежского института МВД России, обучающихся по специальности 11.05.02 Специальные радиотехнические системы, а также для слушателей факультета заочного обучения, обучающихся по профилю подготовки 11.03.01 Радиотехника.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

ИСБ – интегрированные системы безопасности
ИЦ – информационный центр
КСБ – комплексная система безопасности
ОПС – охранно-пожарная сигнализация
СКУД – система контроля и управления доступом
СОУЭ – система оповещения и управления эвакуацией
СИТСЗ – система инженерно-технических средств физической защиты
ТСО – технические средства и системы охраны

ВВЕДЕНИЕ

Оценка современного состояния решаемой проблемы: достижения научно-технического прогресса оказывают влияния на все сферы деятельности человека. Применение новых технологий облегчает информационной обмен, повышает эффективность производственных процессов, формирует новые подходы к организации рабочей деятельности.

Эти изменения повлекли изменения в требованиях организации охраны объекта, его внутреннего пространства, периметра и территории, прилегающей к нему, организации охраны труда, безопасности жизнедеятельности, организации контроля рабочего процесса, порядка и требований доступа на охраняемый объект.

Масштабы таких предприятий играют ключевую роль в проектировании и разработке системы охраны объекта, формирования перечня требований в соответствии с техническими особенностями объекта и деятельности, осуществляемой в его пределах.

Указанные процессы характерны и для правоохранительных органов. ИЦ в системе правоохранительных органов является головной организацией в областях:

– обеспечения статистической, оперативно-справочной, разыскной, криминалистической, архивной и научно-технической информацией;

– оказание государственных услуг в целях обеспечения реализации предусмотренных законодательством Российской Федерации полномочий органов внутренних дел Российской Федерации;

– планирования, координации и контроля процессов создания, внедрения, использования, развития современных информационных технологий, автоматизированных информационных систем общего пользования и интегрированных банков данных общего пользования, средств вычислительной техники и системного программного обеспечения к ним.

Исходя, из вышесказанного для организации безопасности ИЦ необходимо применять концепцию безопасности, заключающейся в использовании системного и комплексного подхода, сочетающего методы организационного, технического и физического характера.

1. ПРАВОВЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ ОСНОВЫ ОРГАНИЗАЦИИ КОМПЛЕКСНЫХ СИСТЕМ БЕЗОПАСНОСТИ

Современные объекты представляет собой большое количество разнородных элементов, объединенных в сложную систему для выполнения поставленных целей, которые в процессе функционирования объекта могут модифицироваться. ИЦ можно представить совокупностью следующих элементов: люди (персонал, посетители); техника (технические средства и помещения в которых они установлены) и программное обеспечение (посредник между человеком и техническими средствами). Таким образом, наличие человека является характерной особенностью объектов такого рода.

Наиболее рациональным способом обеспечения безопасности ИЦ является объединение всех ТСО, методов и мероприятий в единый комплекс, т.е. разработка КСБ. Исходя из этого, решение задачи по обеспечению безопасности ИЦ осуществляется с позиции системного подхода выявление всех возможных угроз безопасности объекта, оценки возможного ущерба при реализации угроз и создания комплекса ТСО. Задачей системного подхода является оптимизация всего объекта, а не его отдельных элементов. Это связано с тем, что, улучшение одного показателя приводит к ухудшению других, необходимо найти компромисс противоречивых требований и характеристик.

Системный подход к построению КСБ включает в себя:

– категорирование объекта;

– своевременное выявление угроз безопасности объекту;

– создание условий, обеспечивающих предупреждение и ликвидацию угроз безопасности объекту;

– создание условий оперативного реагирования на угрозы безопасности;

– создание условий для максимального возмещения и локализации ущерба;

– соотношение всех внутренних и внешних факторов;

– возможность дополнительных изменений в процессе построения системы и полную организацию всего процесса от начала до конца.

Угрозы безопасности могут быть направлены на людей, материальные и информационные ресурсы, учитывая цели защиты можно выделить главные элементы КСБ (рисунок 1).

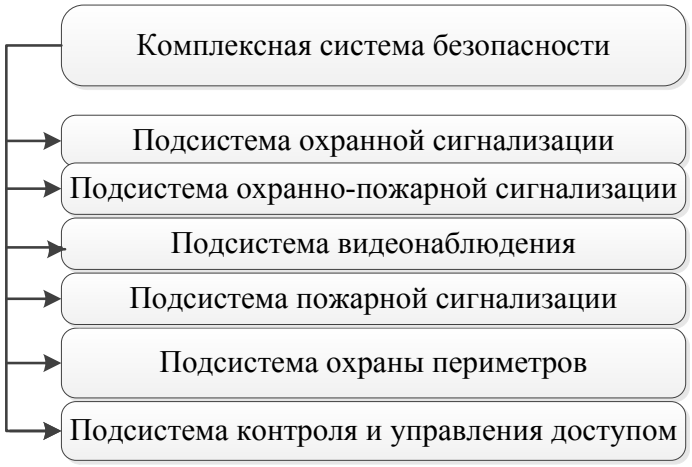

Рис. 1. Составляющие КСБ

Такое деление условно и на практике может не быть четкого функционального разделения. Например, подсистема контроля и управления доступом может эффективно решать задачу по обеспечению санкционированного доступа к информации и информационным ресурсам.

1.1. Общие положения организации комплексной безопасности на объекте

Для рассмотрения нормативно-правовых основ обеспечения безопасности зданий и сооружений в первую очередь целесообразно рассмотреть само понятие безопасности.

Понятие «безопасность» многие правоведы раскрывали через статью 1 Закона РФ от 5 марта 1992 г. № 2446-1 «О безопасности», определяющим безопасность как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». Однако, во-первых, данное понятие весьма обширно и не раскрывает в полной мере интересующую нас область, а во-вторых, данный акт правотворчества на данный момент утратил юридическую силу. Новый же одноименный Федеральный закон от 28 декабря 2010 г. № 390-ФЗ понятия безопасности не раскрывает и так же, как и его «предшественник», определяет широкий предмет своего регулирования, главным образом включающий общественную безопасность и безопасность государства. Таким образом, Федеральное законодательство на текущий момент не раскрывает понятие безопасности, и уж тем более – комплексной безопасности.

В этом случае целесообразным представляется определить более узкую проблематику определения понятийного аппарата и обратиться к терминологии национальных стандартов России. ГОСТ Р 53195.1-2008 «Безопасность функциональная связанных с безопасностью зданий и сооружений систем. Часть 1. Основные положения», рассматривающий здания и сооружения как функционально сложные подсистемы, определяет весьма конкретную роль и место их безопасности, а также систем безопасности, определяя комплексную безопасность как «безопасность при наличии нескольких видов и/или источников опасности», а комплексную систему безопасности как «систему безопасности, одновременно выполняющую несколько функций безопасности, снижающих риски, обусловленные несколькими видами и/или источниками опасностей».

Однако широко известный среди специалистов по обеспечению безопасности ГОСТ Р 53704-2009 устанавливает более конкретную терминологию. Связано это с тем, что возникает необходимость выделить различия между КСБ и интегрированными системами безопасности.

ИСБ отличают:

- единый программно-аппаратный комплекс;
- общая информационная среда;
- единая база данных;
- объединенные технические подсистемы и технические средства.

КСБ:

- разрабатывается для конкретного объекта;
- организационно-технически открыта;
- алгоритмически интегрированные, но функционально самостоятельные технические подсистемы и технические средства.

Нельзя не отметить, что 1 июня 2018 года в действие был введен другой национальный стандарт РФ, затрагивающий ИСБ – ГОСТ Р 57674-2017 «Интегрированные системы безопасности. Общие положения», действие которого распространяется на ИСБ противокриминальной защиты. Среди прочей устанавливаемой терминологии в стандарте вводится такое определение ИСБ, как «система безопасности объекта, объединяющая в себе целевые функциональные системы, предназначенные для защиты от угроз различной природы возникновения и характера проявления».

После определения базового понятийного аппарата, следует перейти к вопросу назначения КСБ, которое напрямую вытекает из ее задач, а точнее – угроз, которым она призвана противостоять. Можно определить назначение КСБ как комплексная защита объекта охраны от криминальных покушений, техногенных угроз и угроз возгорания, а также в отдельных случаях – воздействий природно-климатического характера, их последствий и ошибочных действий обслуживающего персонала объекта. Функционал КСБ при соблюдении соответствующих стандартов могут дополнить подсистемы защиты информации и контроля технических процессов.

Отличительные черты КСБ – техническая открытость и функциональная самостоятельность подсистем при их алгоритмической интеграции, поэтому в структурной взаимосвязи элементы КСБ являются централизовано управляемыми, взаимосвязанными по определенным алгоритмам и выполняющими свои неотделимые функции. В структуру КСБ также входят дополнительные подсистемы и устройства обеспечения функционирования основных подсистем – сети связи, инженерного обеспечения и другие подсистемы.

Каждая КСБ разрабатывается индивидуально, следовательно и состав КСБ и взаимосвязь ее элементов выбираются с учетом назначения объекта, его значимости, индивидуальных особенностей, находящихся на его территории материальных и культурных ценностей, а также общественного резонанса при возникновении на нем чрезвычайной или аварийной ситуации. с учетом того, что одним из главных критериев при выборе элементов КСБ является ее технико-экономическое обоснование.

1.2. Состав комплексных систем безопасности

С учетом федерального законодательства в области защиты от природных и техногенных чрезвычайных ситуаций, охраны окружающей среды пожарной безопасности, а также национальных стандартов в области построения систем мониторинга и управления инженерными сетями, систем тревожной сигнализации, с целью обеспечения безопасности в чрезвычайных ситуациях, национальными стандартами в области систем безопасности определяется весьма широкий состав КСБ. Рассмотрим лишь те из них, которые играют непосредственную роль в области обеспечения безопасности объекта охраны от криминальных

посягательств и техногенных угроз, вызванных пожарами и возгораниями на объекте, так как количество таких чрезвычайных ситуаций относительно преобладает в повседневной деятельности людей относительно других, и такие угрозы являются наиболее вероятными.

Дежурно-диспетчерские подсистема может строиться по централизованному или зонально-распределенному принципу в зависимости от индивидуальных особенностей объекта: занимаемой площади, протяженности периметра, количества и геометрии зон контроля, количества зданий, сооружений, этажей, помещений и т.д. Основные задачи дежурно-диспетчерской подсистемы – периодический контроль всей КСБ и обстановки на объекте с помощью информации, полученной от подсистем; логирование (регистрация) всех событий, происходящих в системе, с указанием конкретных обстоятельств (время, место и т.д.); организация обмена информацией между подсистемами; оповещение дежурного персонала объекта о нештатной или чрезвычайной ситуации, а также передача соответствующего извещения на пульт централизованной с квитированием передачи и получением обратных команд управления. Дежурный персонал дежурно-диспетчерской подсистемы должен иметь в своем распоряжении планы действия в чрезвычайных и нештатных ситуациях, планы зданий, сооружений и помещений, уметь пользоваться управляющим оборудованием КСБ и иметь навыки работы с ним.

Подсистемы ОТС и ОПС должны носить централизованный характер (в исключительных случаях – автономный характер) и обеспечивать круглосуточный контроль защищённости объекта от криминальных угроз и угрозы пожара, периодический контроль охранных и пожарных извещателей и обеспечивать передачу информации об их состоянии в дежурно-диспетчерскую подсистему в установленных сроки. Монтаж охранных извещателей должен осуществляться с учетом рекомендаций ФКУ «НИЦ «Охрана» Росгвардии, а пожарных – в соответствии со сводами правил по системам противопожарной защиты МЧС России. Состав оборудования, его функциональные и технических возможности, порядок построения и режим работы определяется видами возможных угроз с учетом индивидуальных особенностей объекта.

Элементы подсистемы контроля и управления доступом (СКУД), устанавливаемой в соответствии с ГОСТ Р 51241-2008, размещаются на путях прохода (проезда) в помещения (на территории) с ограниченным

доступом с целью недопущения несанкционированного прохода, при этом для прохода в зоны свободного доступа элементы СКУД не должны создавать препятствий. Основная задача СКУД – обеспечение соблюдения внутриобъектового режима персоналом и посетителями объекта, а также автотранспортом на территории объекта.

Подсистема охранного телевидения или видеонаблюдения, построенная с учетом требований национального стандарта РФ 51558-2014, позволяет дежурному персоналу (охране) объекта осуществлять визуальный контроль обстановки на объекте и прилегающей к нему территории. В зависимости от разрешающей способности матрицы и фокусного расстояния видеокамеры, подсистема позволяет на определенном расстояния до объекта наблюдения осуществлять обнаружение, распознавание и идентификацию этого объекта. При организации подсистемы видеонаблюдения появляться возможность организации видеозахвата изображения, архивирования и хранения в течении установленного срока, что позволяет использовать видеоматериал при анализе обстановки или расследовании различных инцидентов; но вне зависимость от того, какого типа подсистема будет развернута в составе КСБ, ее аппаратный и программный центр должен находиться в дежурно-диспетчерском пункте под охраной дежурного персонала объекта.

Подсистема досмотра и поиска включает в себя, главным образом, средства обнаружения предметов, материалов и веществ: металлические изделия, химически опасные, взрывоопасные вещества, радиоактивные материалы, взрывные устройства и другие запрещенные к проносу на территорию объекта предметы. К таким средствам обнаружения относятся металлообнаружители, детекторы металла, рентгеновские установки, анализаторы спектра, дозиметрические приборы, тепловизионное оборудование и т.п.

Подсистемы пожарной автоматики (пожаротушения, противодымной защиты, оповещения, эвакуации) организуются в соответствии с положениями стандарта ГОСТ Р 12.1.004-91 по общим требованиям пожарной безопасности и сводам правил МЧС России, затрагивающим вопросы противопожарной защиты. К задачам подсистемы относятся:

– обнаружение пожара (возгорания) в его начальной стадии;

– оповещение персонала и посетителей объекта о возникновении угрозы пожара, руководство эвакуацией людей в автоматическом режиме;

– локализация пожара (возгорания) на время, необходимое для принятия мер по его тушению оперативными силами и средствами пожаротушения, защита людей от повышенных концентраций летучих продуктов горения, горячего воздуха с целью обеспечения своевременной эвакуации;

– тушение возгорания вплоть до его полной ликвидации, при этом подсистема должна обеспечивать подачу огнетушащего вещества (вода, воздушно-эмульсионная, воздушно-пенная смесь, порошок) в необходимом объеме.

Подсистемы пожарной автоматики должны иметь автоматический и(или) ручной способ включения в зависимости от условий конкретного объекта. При автоматическом способе включения подсистемы пожарной автоматики являются исполнительным звеном подсистемы ОПС.

СОУЭ, помимо того, что является составной частью подсистемы пожарной автоматики, может реализовывать и дополнительный функционал, такой как управление, координация, информирование, персонала и посетителей объекта. СОУЭ, помимо устройств светового, звукового и(или) речевого оповещения, может включать абонентские проводные аналоговые или цифровые телефонные аппараты, радиоаппаратуру, систему громкой связи (совмещенную с системой речевого оповещения), мобильные, пейджинговые и другие средства связи. При наличии аппаратно-программной интеграции подсистем пожарной автоматики, в частности СОУЭ, ОПС и СКУД обеспечивается дистанционное управление запирающими устройствами эвакуационных выходов, преграждающими устройствами и т.д. При организации СОУЭ 5го типа (СП 3.13130-2009 «Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности») возможна организация различных направлений и путей эвакуации людей, что позволяет дежурно-диспетчерскому персоналу, например, путем оценки ситуации по информации, полученной с помощью подсистемы охранного телевидения(видеонаблюдения), организовать наиболее оптимальный маршрут эвакуации людей из различных зон эвакуации.

Подсистема инженерно-технических средств физической защиты (СИТСЗ) устанавливаются с целью воспрепятствования несанкционированному проникновению на объект минуя организованные

точки прохода (проезда). В свою очередь, средства СИТСЗ подразделяются на:

– средства инженерной защиты, использованием которых достигается защита периметра объекта или отдельных территорий объекта, примером таких средств могут служить естественные препятствия (крутые склоны, обрывы, водные преграды), строительно-земляные сооружения (земляные валы, насыпи, котлованы), искусственные ограды (основные, дополнительные, в том числе противоподкопные ограждения, противотаранные устройства);

– средства технической укрепленности панелей, стен, перекрытий, оконных, дверных, вентиляционных и технических проемов зданий, сооружений, помещений.

Материал изготовления защитных конструкции может быть различным. Национальные стандарты в области КСБ допускают использование металлических сплавов, неметаллических соединений, а также комбинирование этих различных видов материалов.

Средства СИТСЗ должны обеспечивать, помимо защитной, и предупредительную функцию, т.е. предупреждать находящихся в непосредственной близости лиц о нахождении возле территории охраняемого объекта.

Немаловажным будет отметить и то, что средства СИТСЗ ни в коем случае не должны препятствовать функционированию подсистем пожарной автоматики и являться препятствиям при эвакуации людей с территории объекта при возникновении чрезвычайных ситуаций.

Грамотно организованная подсистема освещения и электропитания является важным условием функционирования не только подсистем КСБ, но и всех технических систем объекта.

Для организации работы устройств КСБ на территории объекта могут быть организованы следующие виды электрического освещения, каждый из которых реализует свой частный функционал:

– рабочее – обеспечение работы систем охранного телевидения (видеонаблюдения), освещение территорий, зон, помещений объекта с целью соблюдения санитарных норм;

– дежурное – является частью рабочего освещения или отдельной системой, обеспечивающей освещение охраняемой территории с целью обеспечения работы подсистемы охранного телевидения

(видеонаблюдения) и осуществления физической охраны объекта в нежимное время;

– аварийное – выполняет сигнальную функцию при возникновении чрезвычайной ситуации и освещают территорию объекта при возникновении аварии или неисправности в работе подсистем рабочего и(или) дежурного освещения;

– тревожное – выполняет сигнальную функцию при несанкционированном проникновении или попытке несанкционированного проникновения на охраняемую территорию и полностью или выборочно (участок проникновения, зона обнаружения проникновения) освещает территорию объекта с целью демаскировки нарушителя(ей) и обеспечения деятельности сотрудников охраны объекта и(или) сотрудников группы немедленного реагирования вневедомственной охраны по поимке нарушителя(ей);

– эвакуационное освещение – используется при возникновении нештатной ситуации и обеспечивает своевременную и безопасную эвакуацию персонала и посетителей объекта.

Электропитание подсистем КСБ осуществляется по первой категории электроснабжения согласно Правилам устройства электроустановок. Устройства основного и резервного электропитания должны устанавливаться в помещениях с ограниченным доступом людей и соответствовать Правилам устройства электроустановок и Правилам технической эксплуатации электроустановок потребителей.

1.3. Нормативно-технические требования к проектированию комплексных систем безопасности

После анализа общих требований по составу КСБ и общих положений по их организации следует перейти к вопросам непосредственно проектирования КСБ.

Состав подсистем КСБ и их оборудования, как уже было сказано выше, определяется с учетом индивидуальных особенностей объекта безопасности и указывается в техническом задании на проектирование КСБ.

Задание на проектирование составляется с учетом требований ГОСТ Р 21.101-2020 «Система проектной документации для строительства. Основные требования к проектной и рабочей

документации» после проведения экспертного обследования объекта, проводимого с целью определения полного комплекса проводимых мероприятий и мер, направленных на защиту объекта оправданными техническими решениями от определенных технических угроз. При проведении экспертного обследования осмотру подлежат: территория объекта и прилегающая (смежная) территория, объекты и сооружения инженерно-технической укрепленности периметра, здания, сооружения, объекты электроснабжения, освещения, средства инженерного обеспечения, пути подъезда. Учитывается также удаленность до пунктов управления единых дежурно-диспетчерских систем территориальных пунктов правопорядка и противодействия чрезвычайным ситуациям.

Результаты обследования оформляются в установленном порядке. В акте обследования указываются: содержания выполненных работ, их результаты, выводы и рекомендации по проектированию КСБ на объекте, организации взаимодействия с территориальными пунктами единой дежурно-диспетчерской системы.

В отдельных технически обоснованных случаях, таких как довольно малая площадь, занимаемая объектом охраны, малое количество оборудования КСБ и относительная простата его развертывания и пуско-наладки, национальными стандартами допускается выполнять работы по развертыванию КСБ без выполнения работ по проектированию на основе акта обследования в соответствии с нормами и правилами, утвержденными Минстроем России.

Проектирование КСБ осуществляется с учетом требований к проектной и рабочей документации для строительства и единой системы конструкторской документации.

Открытая КСБ, проектируемая с учетом требований ряда национальных стандартов, должна удовлетворять ряду требований:

– рациональности, которая достигается проведением его финансовой и условной оптимизацией при сохранении заданной при проектировании эксплуатационной надежности;

– целостности, достигающейся выбором наиболее оптимальным сочетанием и взаимодействием частей КСБ;

– комплексности, заключающейся в балансе всех составных частей, взаимодействующих с целью выполнения общих задач КСБ с учетом возможностей эксплуатирующей организации;

– перспективность КСБ, состоящей в возможности развития системы с учетом возникающих обстоятельств и новых достижений науки и техники;

– динамичности, означающей работу системы в заданных условиях эксплуатации при сохранении тактико-технических характеристик с учетом естественного износа оборудования при воздействии условий окружающей среды.

Работы по проектированию должны проводиться физическими лицами или организациями, имеющими полученные в установленном порядке разрешительные документы.

Техническое задание на проектирование, соответствующие установленным требованиям, должно содержать следующие разделы:

– список возможных криминогенных и техногенных угроз, которым должна противодействовать КСБ;

– требования, предъявляемые к системе с указанием индивидуальных особенностей объекта;

– состав оборудования, средств и устройств составных подсистем КСБ и отдельных устройств

– требования к отдельным подсистемам;

– требования к организации эвакуации персонала и посетителей объекта с его территории в условиях чрезвычайных ситуаций;

– исходные данные для выполнения отдельных инженерных расчетов;

– перечень необходимых нормативных и технических документов, необходимых для выполнения проекта.

Также в задании указываются технические и эксплуатационные показатели системы, положения техники безопасности и по соблюдению требований в области охраны окружающей среды.

По результатам получения технического задания проектировщиком или проектной организацией составляется рабочий проект, который содержит поэтажные планы и (или) планы территории объекта с указанием мест установки устройств подсистем КСБ, структурные схемы подсистем, сборочные и установочные схемы и чертежи, пояснительные записки и прочее технические документы, необходимые для проведения монтажных работ по национальным и межгосударственным стандартам, строительным нормам и правилам Минстроя России.

2. ОБСЛЕДОВАНИЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ УКРЕПЛЕННОСТИ ОБЪЕКТА ОХРАНЫ

Первым этапам в обеспечении комплексной безопасности объекта является организация инженерно-технической укрепленности объекта, под которой понимается совокупность различных прочностных свойств, характеристик, параметров элементов периметрального ограждения, зданий, сооружений, помещений и строительных конструкций, предназначенных для создания препятствий проникновения нарушителей на территорию охраняемого объекта с целью совершения противоправных действий. Методическими рекомендациями ФКУ «НИЦ «Охрана» Росгвардии Р 078-2019 определяются, что каждому объекту соответствует определенный класс защиты конструктивных элементов здания, к которым относятся: защитные конструкции – периметральные ограждения как постоянной, так и временной конструкции, ворота, калитки, шлагбаумы, двери в воротах; строительные конструкции – внешние, внутренние стены помещений, кладовых, хранилищ, перегородки, вентиляционные короба, а также потолочные и межэтажные перекрытия; дверные конструкции различного расположения – входные, запасные (эвакуационные, аварийные), внутренние, охраняемых помещений; оконные конструкции различного расположения; замки, запирающие устройства различных конструкций и расположения.

К средствам инженерно-технической укрепленности предъявляются следующие требования:

– создание препятствий для нарушителей при попытке несанкционированного проникновения на объект в «обход» организованных точек прохода;

– создание условий, затрудняющих использование средств взлома при несанкционированном проникновении;

– сохранение установленной пропускной способности организованных точек прохода на территорию объекта;

– отсутствие влияния на работу технических средств охраны объекта;

– сохранение своих тактико-технических и прочностных характеристик в течении всего срока службы в заданных условиях эксплуатации.

Только при соответствии средств инженерно-технической укрепленности всем предъявляемым требованиям и классу защиты в зависимости от класса объекта может быть достигнута достаточная защищенность объекта охраны от внешних преступных посягательств, что

является первым условием построения системы охраны объекта с применением подсистем комплексной защиты.

При проектировании системы безопасности учтены требования ряда нормативных документов в сфере безопасности объектов внутренних дел Российской Федерации от преступных посягательств.

Согласно требованиям приказа МВД России от 31 декабря 2014 г. № 1152 «Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств» необходимо обеспечить инженерно-техническую укрепленность и повысить уровень антитеррористической защищенности объекта. Осуществить обследование подразделением отделения вневедомственной охраны на инженерно-техническую укрепленность объекта от преступных посягательств дать рекомендации и оценку состояния их защищенности.

Для обеспечения антитеррористической защищенности объекта необходимо выполнить ряд требований:

– обеспечить наличием на объекте организационно-распорядительных документов по организации защиты объекта от возможных террористических актов и назначить должностных лиц, ответственных за мероприятия по антитеррористической защищенности объекта;

– разработать порядок взаимодействия должностных лиц объекта и подразделений с органами исполнительной власти субъектов Российской Федерации, а также медицинскими учреждениями и аварийно-спасательными службами по вопросам обмена информацией, проведения совместных учений (тренировок) и реагирования на сообщения об угрозе террористического акта;

– организовать охрану объекта;

– оборудовать контрольно-пропускной пункт досмотровой техникой, специальными инженерно-техническими сооружениями, препятствующими несанкционированному проходу и проезду;

– выделить особо охраняемые зоны объекта по степени наибольшей террористической уязвимости и масштабов последствий террористических актов;

– обеспечить личный состав дежурной смены по охране объекта переносными и стационарными средствами связи и табельным оружием в соответствии с требованиями правовых актов МВД России;

– исключить доступ посторонних лиц к эксплуатационной документации и во внутренние компьютерные сети объекта;

– обеспечить должное обслуживание и контроль за наличием и работоспособностью всех систем обеспечения безопасности объекта.

В здании объекта располагаются специальные помещения МВД, к которым относятся: помещение дежурной части, комнаты хранения оружия, боеприпасов, взрывчатых веществ и специальных средств, помещения для хранения средств защиты, связи, специальной, оперативной и криминалистической техники архивы, хранилища и кассы. Их инженерно-техническая укрепленность и оснащенность КСБ должна соответствовать требованиям действующих ведомственных нормативных документов, регламентирующих их защищенность.

2.1. Анализ угроз безопасности информационных центров

В наши дни ухудшение состояния террористической обстановки в стране, усиление межнациональных связей, организованных террористических, экстремистских и криминальных групп, рост технической оснащенности, их финансовой мощи, дает основание полагать, что в ближайшее время оперативная обстановка в стране не изменится к лучшему. При этом основной задачей нарушителя при совершении преступления на объекте, является скрытное преодолении средств технической укрепленности.

В целях обеспечения безопасности объектов ОВД разработана и утверждена приказом МВД России от 31 декабря 2014 г. № 1152 «Инструкция по обеспечению инженерно-технической укрепленности и повышению уровня антитеррористической защищенности объектов органов внутренних дел Российской Федерации от преступных посягательств».

Для объектов правоохранительных органов, характерны следующие виды угроз:

1. Угроза обстрела – возможность разрушения здания, причинение вреда здоровью сотрудников полиции, граждан и другим лицам повреждений путем обстрела.

2. Угроза захвата объекта и (или) транспортных средств (ТС) – возможность захвата, установления над ним контроля силой или угрозой применения силы, или путем любой другой формы запугивания.

3. Угроза взрыва – комнаты хранения оружия, специальных средств, вещественных доказательств и наркотических средств, архивных

документов и (или) ТС – возможность разрушения, уничтожения или нанесения повреждения путем взрыва, создающего угрозу жизни или здоровью сотрудников полиции, граждан и других лиц.

5. Угроза блокирования – возможность создания препятствия, делающего невозможным движение ТС или ограничивающего функционирование действующим сотрудникам, угрожающим жизни или здоровью, граждан и других лиц.

6. Угроза хищения – возможность совершения хищения оружия, специальных средств, вещественных доказательств и наркотики, архивных документов, которое может привести их в негодное для эксплуатации состояние, угрожающее жизни или здоровью сотрудников полиции, граждан и населения.

При этом можно разделить угрозы на криминальные и террористические (таблица1).

Таблица 1

Виды угроз безопасности отдела полиции

№ п/п	Вид угроз	Вероятные места проявления	Последствия
1.	Террористические	– разрушение или взрыв здания; – разрушение или взрыв комнаты хранения оружия, специальных средств, вещественных доказательств и наркотических средств, архивных документов и транспортных средств; – захват заложников на территории.	– материальные потери, опасность для жизни и здоровью людей; – экологическое загрязнение; – экономические затраты; – опасность для жизни и здоровья людей.
2.	Криминальные	– причинение вреда жизни и здоровью сотрудников полиции, находящихся на территории; – хищение материальных ценностей с объекта; – вандализм; – поджог; – вооруженное нападение.	– опасность для жизни и здоровья людей; – экологическое загрязнение; – материальные потери.

2.2. Результаты обследования информационного центра

Согласно положениям приказа МВД России от 31 декабря 2014 г. № 1152 объект относится к первой категории и состоит из одного отдельно стоящего здания. В здании имеются: касса, бухгалтерия, кабинеты сотрудников, архив, комната хранения оружия, комната выдачи оружия, дежурная часть, комната отдыха, зал совещаний, приемные руководителей, санузлы, коридоры, подсобные помещения, один центральный вход, один запасной выход. На территории расположены пожарные емкости, контрольно-пропускной пункт, на котором имеется проходная и пункт осмотра.

Наиболее уязвимыми местами являются: центральный и запасной входы, архив.

На рисунке 2 представлена схема распространения и устранения угроз на объекте защиты.

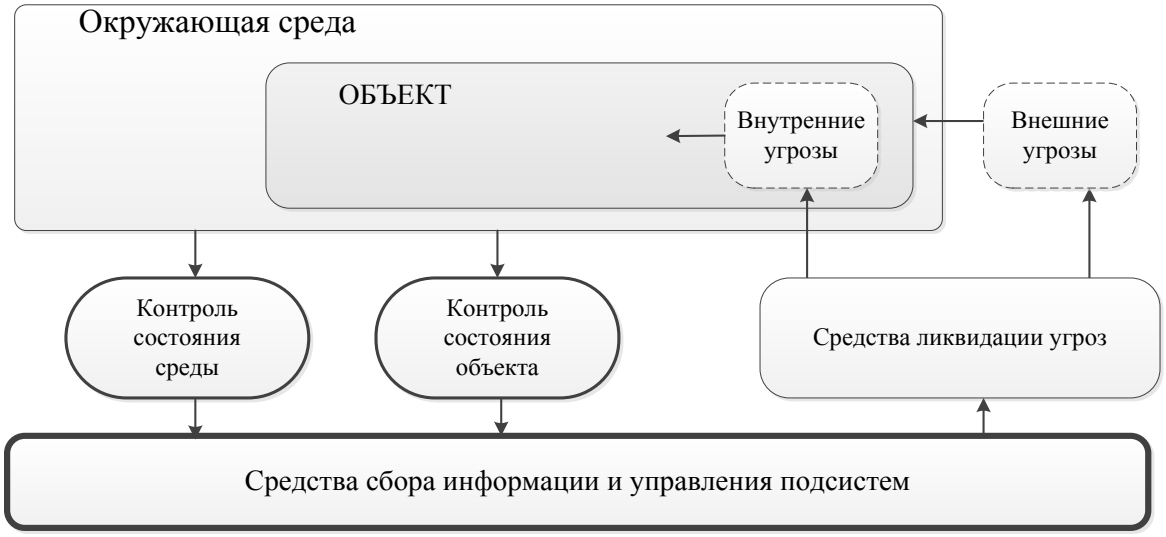

Рис. 2. Схема распространения угроз и устранение угроз на объекте

Основным свойством КСБ является взаимодействие ее функциональных подсистем, таким образом при выборе оборудования для подсистем КСБ и всей системы в целом следует учитывать интеграционные свойства.

В национальных стандартах РФ в области обеспечения безопасности выделяются следующие виды взаимодействия подсистем КСБ:

1) аппаратное – взаимодействие на аппаратном уровне посредством коммутации управляющего оборудования подсистем с обменом простыми управляющими сигналами;

2) программное – взаимодействие за счет организации общей программной среды, организованной на базе персонального компьютера;

3) аппаратно-программное – взаимодействие, при котором подсистемы объединены аппаратно с обменом управляющими и информационными сигналами по протоколу при наличии компьютера (контроллера) с установленным программным обеспечением, осуществляющим дополнительный обмен данными.

Рассмотрим системы безопасности, включенные в Список технических средств безопасности, удовлетворяющих «Единым требованиям к системам передачи извещений, объектовым техническим средствам охраны и охранным сигнальнопротивоугонным устройствам автотранспортных средств, предназначенным для применения в подразделениях вневедомственной охраны войск национальной гвардии Российской Федерации»:

1) интегрированная система безопасности «Рубеж»;

2) интегрированная система охраны «Орион»;

3) интегрированный комплекс безопасности «Кодос».

Другие системы, включенные в выше названный список, имеют аппаратную интеграцию «Ладога-А», «Стрелец-Интеграл»), либо программную («Пахра»).

Проектирование комплексной системы безопасности информационного центра, в частности проектирование подсистемы охранно-тревожной и пожарной сигнализации выбран прибор приемно-контрольный охранный ППКО «Ладога-А» с дополнительным оборудованием.

Краткая техническая характеристика: до 80 зон (64 адресных, 80 радиоканальных или 80 радиальных); 32 независимых раздела; работа при коротком замыкании адресного шлейфа; более 10 типов зон; до 16 клавиатур, до 16 устройств постановки/снятия, до 28 контролируемых выходов, до 35 релейных выходов; возможность управления внешними оповещателями, программирование с ПК, видеорегистрация и удаленная передача видеоизображений с 4 видеокамер. Подключение до 4-х адресных блоков питания, контролируемых по интерфейсу. Выход RS 232. Объединение до 8-ми приборов. Передача сообщений по ТЛФ линии в формате Contact ID. Работа в составе СПИ «Заря». Возможность охраны взрывоопасных помещений с помощью блока расширения «Ладога-Ех». В состав системы на основе прибора «Ладога-А» входит система охранная телевизионная «ТелеВизард-В».

3. ФОРМАЛИЗАЦИЯ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ОБЪЕКТА

Основой формального описания систем безопасности можно считать модель системы безопасности, в которой рассматривается взаимодействие следующих множеств:

$U = \{u_i\}$ – множество угроз безопасности,

$O = \{o_j\}$ – множество элементов защищенного объекта,

$S = \{s_k\}$ – множество механизмов безопасности.

Качественные методы оценки КСБ предполагают оценку уровня защищенности, анализ рисков и тестирование КСБ. Оценка уровня защищенности ИЦ позволяет на основе некоторого набора исходных данных (организационная структура и функциональная схема ИЦ, наличие и характер взаимодействия с другими объектами и др.) выявить качественное соответствие или несоответствие КСБ определенным требованиям. Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к защищенности ИЦ, характера принимаемых во внимание угроз и эффективности потенциальных контрмер.

Анализ рисков необходим для выбора подхода к управлению рисками. Такими подходами являются: уменьшение риска, уклонение от риска, изменение характера риска или принятие риска.

Тестирование системы безопасности проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к угрозам, а также с целью поиска уязвимостей и может проводиться на основе следующих методов.

В основе метода экспертных оценок комплексной безопасности объектов лежит понятие профиля защиты. Формально описать вероятности отдельных угроз, эффективности отдельных концепций безопасности очень сложно. В связи с этим, для получения количественной оценки риска используются экспертные оценки, основанные на использовании кластера исходов.

Сущность графового метода состоит в построении оценки защищенности объектов на основе характеристик защитных для этого объекта механизмов и определении достаточности КСБ. Объект исследования представляется в виде графа, вершинами которого являются элементы ИЦ и ТСО, а связями – возможные пути продвижения

нарушителя. Результат исследования должен отображать степень защищенности объекта, а оценка может быть представлена как выдача статистического параметра «время преодоления рубежа охраны».

Эффективность, в зависимости от имеющихся ресурсов, знаний разработчиков и других факторов, может быть достигнута в той или иной мере, при этом возможны альтернативные пути ее реализации. Она имеет непосредственную связь с другими системными свойствами, в том числе качеством, надежностью, управляемостью, помехозащищенностью, устойчивостью. Поэтому количественная оценка эффективности позволяет измерять и объективно анализировать основные свойства систем на всех стадиях их жизненного цикла, начиная с этапа формирования требований и эскизного проектирования. Для предприятия эффективность, прежде всего, связана с экономическими вопросами. Оценка экономической эффективности возможна на основе формальной модели КСБ с использованием вероятностного подхода.

3.1. Оценка рисков

Качественные методы оценки безопасности предполагают оценку уровня ИБ, анализ рисков и тестирование КСБ. Оценка уровня безопасности позволяет на основе некоторого набора исходных данных выявить качественное соответствие или несоответствие КСБ определенным требованиям.Существуют различные подходы к оценке рисков. Выбор подхода зависит от уровня требований, предъявляемых в организации к уровню безопасности, характера принимаемых во внимание угроз и эффективности защитных мер.

Анализ рисков необходим для выбора подхода к управлению рисками. Такими подходами являются: уменьшение риска, уклонение от риска, изменение характера риска или принятие риска.

Тестирование системы безопасности проводится с целью проверки эффективности используемых в ней механизмов защиты, их устойчивости к угрозам, а также с целью поиска уязвимостей и может проводиться по методу «белого ящика» или по методу «черного ящика».

3.2. Методы количественной оценки систем безопасности

Формально описать вероятности отдельных угроз, эффективности

отдельных концепций безопасности очень сложно. В связи с этим, для получения количественной оценки риска используются экспертные оценки, основанные на использовании кластера исходов.

Сущность графового метода состоит в построении оценки защищенности объектов на основе характеристик защитных для этого объекта механизмов и определении достаточности системы безопасности. Объект представляется в виде графа, вершинами которого являются элементы КСБ и элементы ИЦ, а связями – возможные пути продвижения нарушителя. Результат исследования должен отображать степень защиты объекта, а оценка может быть представлена как выдача статистического параметра «время взлома». Исходными данными для оценки по методу весовых коэффициентов служат результаты анкетирования субъектов отношений, предназначенные для уяснения направленности их деятельности, предполагаемых приоритетов целей безопасности, условий расположения и эксплуатации объекта. На основании анализа составляется матрица взаимосвязи источников угроз и уязвимостей.

3.3. Комплексный подход к оценке эффективности систем информационной безопасности

Решение задачи обеспечения комплексной безопасности объекта требующие количественной оценки характеристик. Такие данные, полученные экспериментально или путем математического моделирования, должны раскрывать свойства КСБ. Основным из них является эффективность, под которой понимается степень соответствия результатов уровня безопасности объекта поставленной цели.

Эффективность, в зависимости от имеющихся ресурсов, знаний разработчиков и других факторов, может быть достигнута в той или иной мере, при этом возможны альтернативные пути ее реализации. Она имеет непосредственную связь с другими системными свойствами, в том числе качеством, надежностью, управляемостью, помехозащищенностью, устойчивостью. Поэтому количественная оценка эффективности позволяет измерять и объективно анализировать основные свойства систем на всех стадиях их жизненного цикла, начиная с этапа формирования требований и эскизного проектирования.

Для объекта эффективность, прежде всего, связана с экономическими вопросами. Оценка экономической эффективности возможна на основе формальной модели КСБ с использованием вероятностного подхода.

4. РАЗРАБОТКА ИМИТАЦИОННОЙ МОДЕЛИ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОГО ЦЕНТРА

ИЦ могут подвергаться различным типам угроз безопасности. Как правило, КСБ строится на основе обеспечения безопасности элементов объекта. Так как существуют различные пути распространения угроз безопасности на объекте, целесообразным является учет возможностей распространения и устранения угроз безопасности, что позволяет повысить эффективность КСБ объекта. Учитывая, что распространение и устранение угроз безопасности происходит не одномоментно их можно представить динамической системой, описывающей этот процесс во времени.

С помощью сетей Петри разработана математическая модель функционирования ИЦ оснащенного КСБ в условиях воздействия угроз безопасности

Сеть Петри состоит из четырех элементов: множество позиций *P,* множество переходов *T,* входная функция *I,* выходная функция *O.*

Входная и выходная функции связаны с переходами и позициями. Входная функция *I* отображает переход t_j в множестве позиций $I(t_j)$, называемых входными позициями перехода. Выходная функция *O* отображает переход t_j в множестве позиций $O(t_j)$, называемых выходными позициями перехода.

Графическим представлением сетей Петри является ориентированный двудольный граф.

В соответствии с тем, что сеть Петри включает множества переходов и позиций, граф сети Петри обладает двумя типами вершин: кружки соответствуют позициям, а чёрточки (планки) - переходам (рисунок 3).

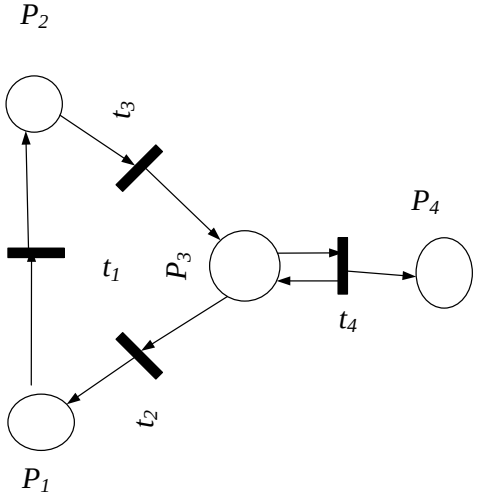

Рис. 3. Граф сети Петри

Присвоение фишек позициям сети Петри называется маркировкой μ. При выполнении сети Петри могут изменяться положение и количество фишек. В нашей модели фишка будет соответствовать угрозе безопасности.

Под маркировкой μ сети Петри *C=(P, T, I, O)*понимается функция, которая отображает множество позиций P в множество неотрицательных чисел N.

$$\mu: P \to N.$$

Далее будем рассматривать только маркированные сети Петри.

Маркированная сеть Петри $M = (C, \mu)$ это совокупность структуры сети Петри *C= (P, T, I, O)* и маркировки μ и может быть записан в виде $M = (P, T, I, O, \mu)$.

Количество маркировок сети Петри может быть бесконечно большим.

Выполнением переходов сети Петри управляют фишки, которые находятся в кружках. При запуске переходов сеть выполняется, то есть переход запускается удалением фишек из его входных позиций и образованием новых фишек, помещаемых в его выходные позиции.

Переход может запускаться только в том случае, когда он разрешен. Переход называется разрешенным, если каждая из его входных позиций имеет число фишек, по крайней мере, равное числу дуг из позиции в переход. Кратные фишки необходимы для кратных входных дуг. Фишки во входной позиции, которые разрешают переход, называются его разрешающими фишками.

Переход t_j в маркированной сети Петри с маркировкой μ может быть запущен всякий раз, когда он разрешен. В результате запуска разрешенного перехода t_j образуется новая маркировка μ'.

Для анализа сетей Петри применяют два основных метода: дерево достижимости и метод, связанный с матричными уравнениями.

Рассмотрим работу алгоритма на примере фрагмента, состоящего из двух элементов объекта, во избежание громоздкости описания.

В сетях Петри допускается возможность существования конфликтов, если с элемента объекта, которому соответствует позиция, угроза безопасности i-го типа может распространяться на несколько других элементов, т. е. маркирующая эту угрозу фишка удаляется из позиции. Кроме того, удаление фишки из позиции означало бы исчезновение угрозы

на соответствующем элементе, что противоречит логике решаемой задачи (рисунок 5).

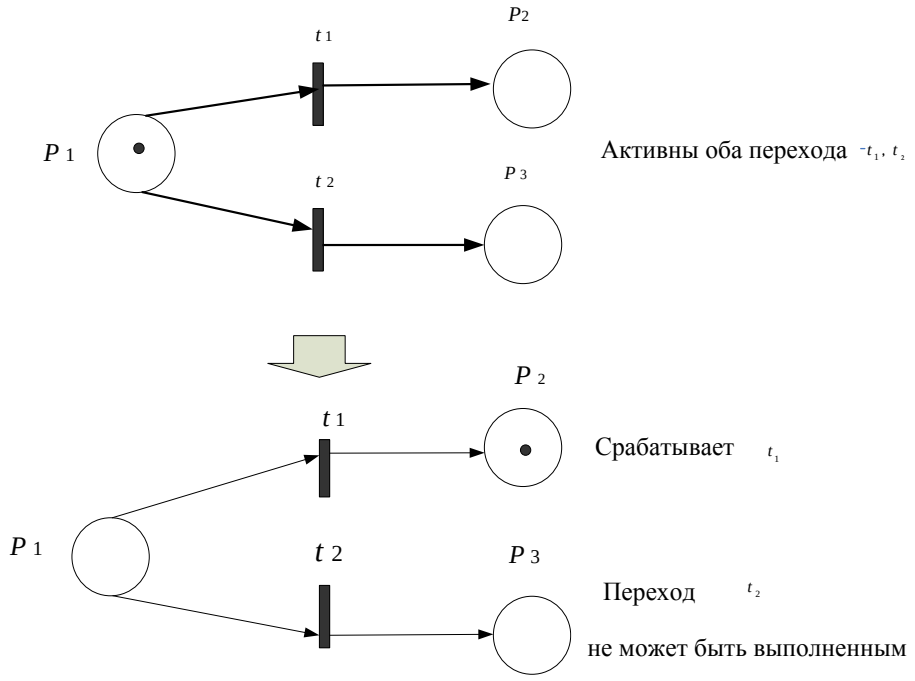

Рис. 5. Пример возникновения конфликта в сети Петри

Этого недостатка можно избежать, если каждую позицию, соответствующую элементу, преобразовать в так называемую «ловушку», т. е. позицию, которую не может покинуть ни одна фишка. Для этого можно применить преобразование, показанное на рисунке 6.

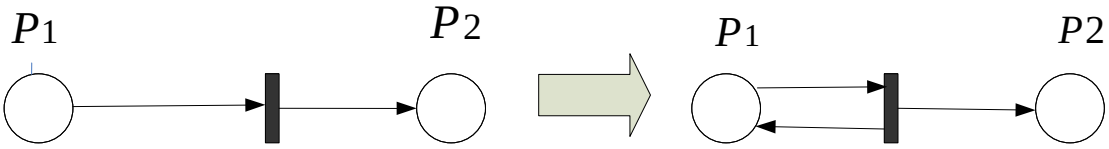

Рис. 6. Пример преобразования исключения конфликта в сети Петри

Рассмотрим моделирование действий элементов КСБ, осуществляющих устранение угроз безопасности на элементах. Такие элементы можно моделировать с помощью введения дополнительно позиций-ловушек. Их действие показано на рисунке 7.

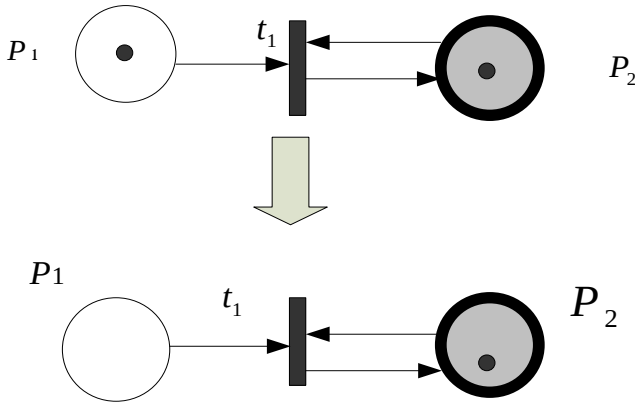

Рис. 7. Фрагмент сети Петри, содержащей позицию ловушку, соответствующую элементу КСБ, устраняющему угрозу безопасности на элементе объекта

На рисунке 8 представлена сеть, содержащая элементы КСБ.

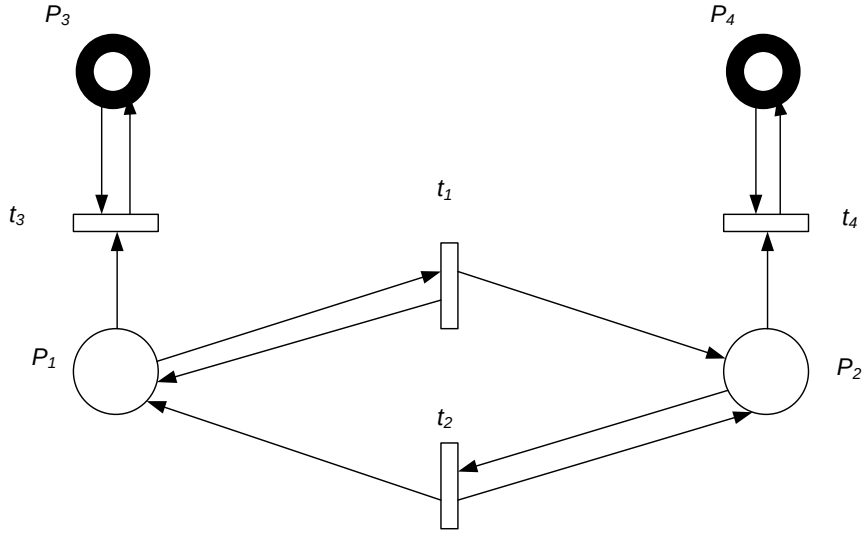

Рис. 8. Сеть Петри, содержащая элементы КСБ

Выделенными позициями (P_3,P_4) обозначены элементы КСБ.

Для данной сети возможны 2^4=16 вариантов маркировки (таблица 3).

Таблица 3

Возможные варианты маркировки

1) 0000	5) 0100	9) 1000	13) 1100
2) 0001	6) 0101	10) 1001	14) 1101
3) 0010	7) 0110	11) 1010	15) 1110
4) 0011	8) 0111	12) 1011	16) 1111

С точки зрения обеспечения безопасности ИЦ, первые четыре варианта маркировки не представляют интереса, т.к. в этих случаях маркировки попадание фишки в позиции P_1, P_2 невозможно. Для программной реализации данной модели был применен численный метод, в основе которого лежит матричное представление сетей Петри.

Программная реализация была разработана на языке С++. В представленной версии были использованы следующие ограничения, которые могут быть значительно снижены: количество элементов объекта и элементов КСБ – до 100; количество каналов распространения и устранения угроз – до 100.

Программа позволяет определять вероятности нахождения элементов под угрозами на основе имитационного моделирования описанных выше сетей Петри. Введем обозначения:

– M – маркировка;

– Q – вероятность срабатывания перехода;

– S – вероятность нахождения элемента под угрозой или признак включения элемента КСБ (1 – включено, 0 – не включено).

Для демонстрации работы модели используем описанный выше фрагмент объекта, включающий два элемента, моделируемые позициями P_1, P_2, и элементы КСБ, моделируемые позициями P_3, P_4. Были заданы следующие вероятности срабатывания переходов Q=(0,2; 0,1; 0,5; 0,8).

Рассмотрим последовательно варианты маркировки:

1. M = (0100) (рисунок 9) – это означает, что первоначально угроза находилась только на втором элементе, а средства КСБ были отключены.

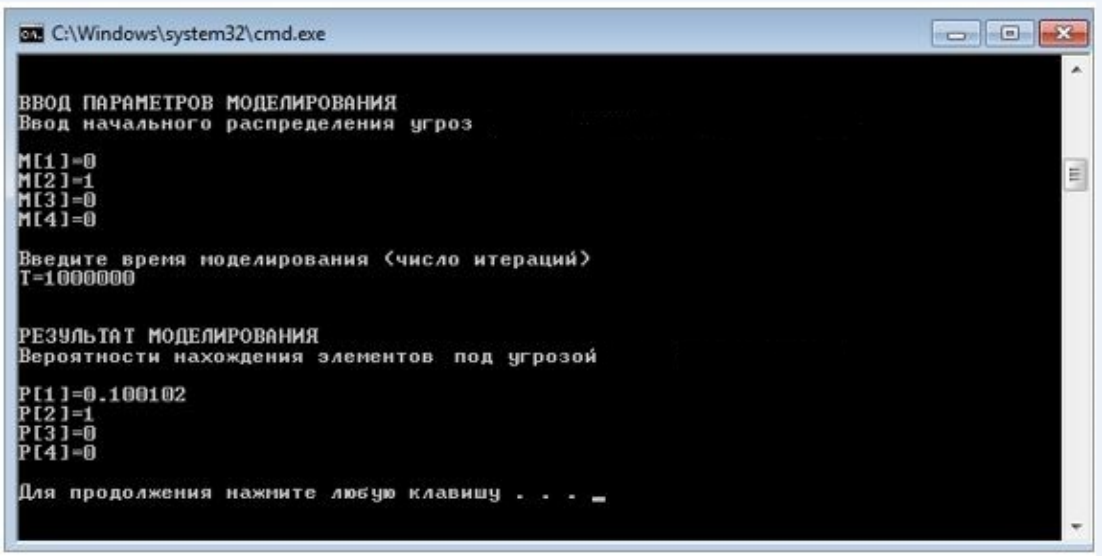

Рис. 9. Результаты работы программы для M=(0100)

Вероятности нахождения элементов ИЦ под угрозой безопасности S_1=(0,1; 1; 0; 1).

Аналогично получим данные для других маркировок.

2. M=(0101). В данном случае первоначально могут сработать переходы t_2, t_4. После срабатывания перехода t_4 фишка попадает в позицию P_4 и угроза для P_2 устраняется (рисунок 10).

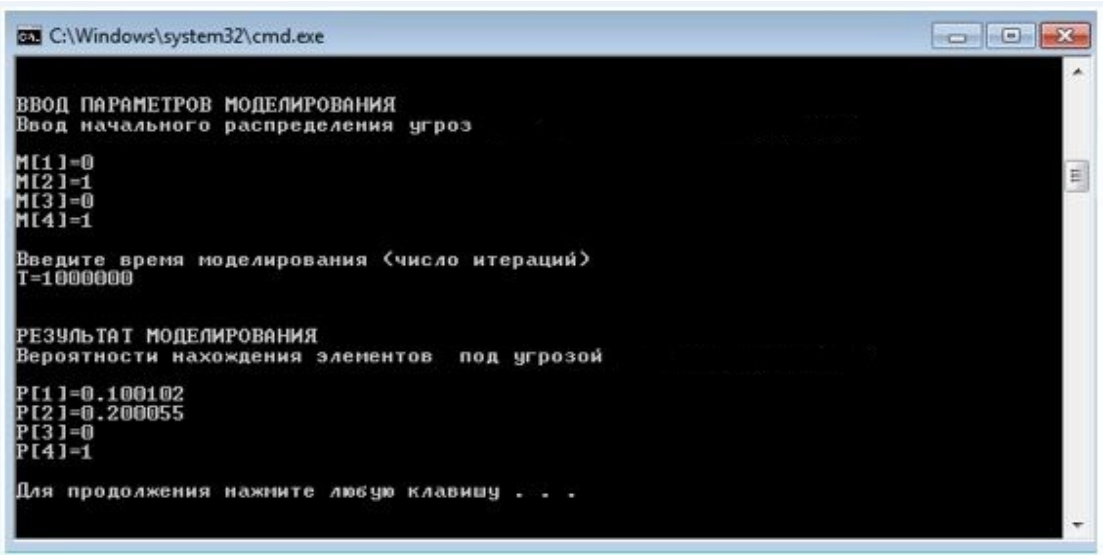

Рис. 10. Результаты работы программы для M=(0101)

Вероятности нахождения элементов ИЦ под угрозой безопасности S_2=(0,1; 0,2; 0; 1)

3. В случае M=(1010) первоначально могут сработать переходы t_1,t_3 (рисунок 11).

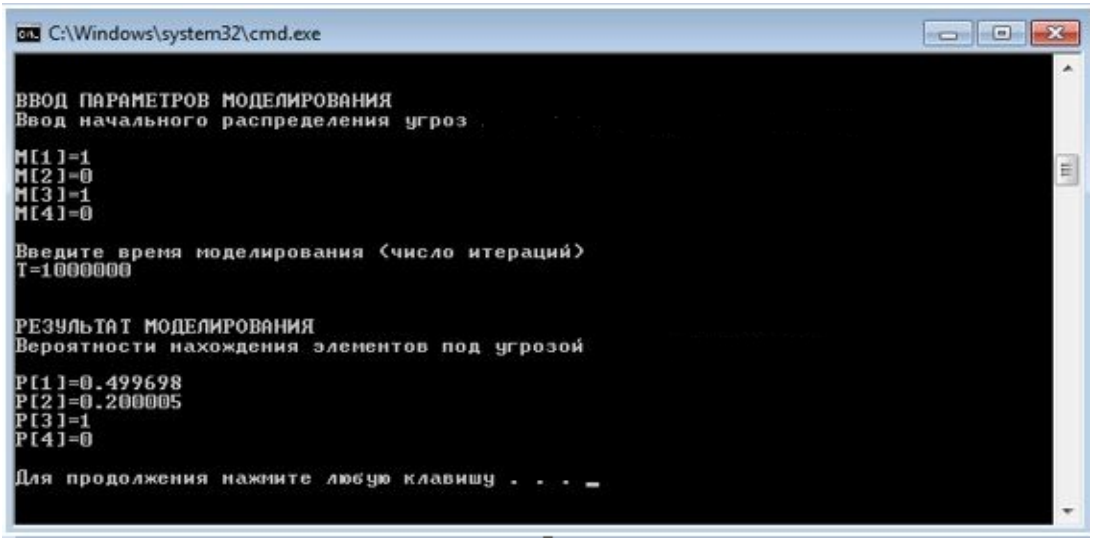

Рис. 11. Результаты работы программы для M=(1010)

Вероятности нахождения элементов ИЦ под угрозой безопасности S=(0,499698; 0,2; 0; 1)

Результаты выполнения всех маркировок отражены в таблице 4.

Таблица 4

Вероятности нахождения элементов под угрозой

№ п/п	Маркировка M	Вероятность нахождения компьютера под угрозой S
1.	0000	Не представляют интерес, так как попадание фишки в позиции P_1и P_2 невозможно
2.	0001	
3.	0010	
4.	0011	
5.	0100	(0,1; 1; 0; 0)
6.	0101	(0,1; 0,2; 0; 1)
7.	0110	(0,1; 1; 1; 0)
8.	0111	(0,1; 0,2; 1; 1)
9.	1000	(1; 0,2; 0; 0)
10.	1001	(1; 0,2; 0; 1)
11.	1010	(0,499698; 0,2; 0; 1)
12.	1011	(0,499698; 0,2; 1; 1)
13.	1100	(1; 1; 0; 0)
14.	1101	(1; 0,360144; 0; 1)
15.	1110	(0,54994; 1; 1; 0)
16.	1111	(0,54994; 0.360144; 1; 1)

Таким образом, на основе теории сетей Петри разработана математическая модель КСБ ИЦ, позволяющая определить вероятности нахождения элементов ИЦ под угрозой безопасности. Полученные результаты могут быть использованы в задаче проектирования КСБ для выбора оптимального варианта КСБ.

В результате взаимодействия с предприятием-изготовителем («Научно-производственного предприятия РИЭЛТА»), были разработаны макет охранно-пожарной подсистемы на базе приемно-контрольного прибора «Ладога» и макет охранно-пожарной подсистемы на базе приемно-контрольного прибора «Ладога-А» позволяющие имитировать функционирование ОПС на охраняемом объекте в результате воздействия неблагоприятных факторов на элементы объекта.

ЗАКЛЮЧЕНИЕ

Безопасность представляется как практическая деятельность по направлению предотвращения несанкционированного доступа и комплекса деструктивных и негативных действий в отношении защищаемого объекта.

Главной целью комплексной системы безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности от противоправных преступных посягательств, а также не допущение хищения материальных ценностей, разглашения, утечки, утраты, искажения и уничтожения служебной информации, обеспечение нормальной служебной деятельности всех элементов объекта, как в повседневной деятельности, так и в чрезвычайных ситуациях.

Для оптимизации процессов обеспечения безопасности информационных центров ведутся работы в направлении совершенствования методологии математического моделирования, т.е. в разработке методического аппарата для исследования процессов защиты информационного центра от угроз различного типа в целом.

Концепция построения математических моделей и алгоритмов их реализации заключается в количественном обосновании способов повышения эффективности комплексной системы безопасности и выбора оптимального варианта системы безопасности.

Базовым инструментарием повышения точности любых математических моделей, выступает критерий оценки адекватности результатов моделирования и проверка их на валидность, а также экспериментальное тестирование моделей.

На основе разработанной математической модели реакции комплексной системы безопасности на возмущающие воздействия разработан алгоритм имитации функционирования комплексной системы безопасности информационного центра и может быть осуществлен выбор оптимального варианта комплексной системы безопасности исходя из анализа значений вероятности нахождения элементов информационного центра под угрозой безопасности для выбранного варианта комплексной системы безопасности.

СПИСОК ЛИТЕРАТУРЫ

Нормативная правовая:

1. Об обеспечении безопасности объектов органов внутренних дел Российской Федерации от преступных посягательств: приказ Министерства внутренних дел Российской Федерации № 1152, от 31.12.2014 // Режим доступа: http://www.consultant.ru/.

2. Системы аварийной сигнализации и оповещения : сборник ГОСТов / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2005 – 251 с.

3. ГОСТ Р 51241-2008. Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний : национальный стандарт Российской Федерации : дата введения 2009-09-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2009 – 31 с.

4. ГОСТ Р 52435-2015. Технические средства охранной сигнализации. Классификация. Общие технические требования и методы испытаний (с Изменением № 1) : национальный стандарт Российской Федерации : дата введения 2016-05-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2019 – 37 с.

5. ГОСТ Р 52436-2005. Приборы приемно-контрольные охранной и охранно-пожарной сигнализации. Классификация. Общие технические требования и методы испытаний : национальный стандарт Российской Федерации : дата введения 2006-09-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2006 – 16 с.

6. ГОСТ Р 52551-2016. Системы охраны и безопасности. Термины и определения : национальный стандарт Российской Федерации : дата введения 2017-07-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2016 – 28 с.

7. ГОСТ Р 53704-2009. Системы безопасности комплексные и интегрированные. Общие технические требования : национальный стандарт Российской Федерации : дата введения 2010-09-01 / Федеральное

агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2010 – 30 с.

8. ГОСТ Р 54455-2011 (МЭК 62599-1:2010). Системы охранной сигнализации. Методы испытаний на устойчивость к внешним воздействующим факторам : национальный стандарт Российской Федерации : дата введения 2012-06-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2019 – 20 с.

9. ГОСТ Р 55017-2012. Пульты централизованного наблюдения для использования в системах противокриминальной защиты. Требования к информации : национальный стандарт Российской Федерации : дата введения 2013-09-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2014 – 14 с.

10. ГОСТ Р 56102.1-2014 Системы централизованного наблюдения. Часть 1. Общие положения (Переиздание) : национальный стандарт Российской Федерации : дата введения 2016-01-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2015 – 10 с.

11. ГОСТ Р 56102.2-2015. Системы централизованного наблюдения. Часть 2. Подсистема объектовая. Общие технические требования и методы испытаний (Переиздание) : национальный стандарт Российской Федерации : дата введения 2017-01-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2016 – 15 с.

12. ГОСТ Р 56102.3-2019. Системы централизованного наблюдения. Часть 3. Подсистема передачи информации. Общие технические требования и методы испытаний : национальный стандарт Российской Федерации : дата введения 2019-05-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2019 – 11 с.

13. ГОСТ Р 57674-2017. Интегрированные системы безопасности. Общие положения : национальный стандарт Российской Федерации : дата введения 2018-06-01 / Федеральное агентство по техническому регулированию и метрологии. – Изд. официальное. – Москва : Стандартинформ, 2017 – 11 с.

14. Р 78.36.052-2015. Типовые проектные решения оснащения техническими средствами охраны объектов органов внутренних дел Российской Федерации, отнесенных к первой категории : методические рекомендации : дата введения 2015-12-25 / ГУВО МВД России. – Изд. официальное. – Москва : ФКУ «НИЦ «Охрана» МВД России, 2015– 191 с.

15. Р 071-2017. Технические средства систем безопасности объектов. Обозначения условные графические элементов технических средств охраны, систем контроля и управления доступом, систем охранного телевидения : рекомендации : дата введения 2017-06-30 / ФС ВНГ РФ. – Изд. официальное. – Москва : ФКУ «НИЦ «Охрана» Росгвардии; Саратов : Амирит, 2017 – 20 с.

16. Р 078-2019. Инженерно-техническая укрепленность и оснащение техническими средствами охраны объектов и мест проживания и хранения имущества граждан, принимаемых под централизованную охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации : методические рекомендации : дата введения 2019-04-04 / ФС ВНГ РФ. – Изд. официальное. – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2017 – 58 с.

17. Р 089-2022. Рекомендации по охране особо важных объектов с применением интегрированных систем безопасности : рекомендации : дата введения 2022-03-1 / ГУВО МВД России. – Изд. официальное. – Москва : ФКУ «НИЦ «Охрана» МВД России, 2022– 96 с.

18. Р 063-2022. Обследование объектов, охраняемых или принимаемых под охрану подразделениями вневедомственной охраны войск национальной гвардии Российской Федерации : методические рекомендации : дата введения 2017-08-11 / ФС ВНГ РФ. – Изд. официальное. – Москва : ФКУ «НИЦ «Охрана» Росгвардии, 2022 – 50 с.

Основная:

19. Ворона В. А. Теоретические основы обеспечения безопасности объектов информатизации [Текст] : учебное пособие : рек. УМО ВО / В. А. Ворона, В. А. Тихонов, Л. В. Митрякова. – Москва : Горячая линия – Телеком, 2016. - 304 с.

20. Ворона В. А. Концептуальные основы создания и применения системы защиты объектов [Текст] : учебное пособие / В. А. Ворона, В. А. Тихонов. – Москва : Горячая линия – Телеком, 2017. – 196 с.

21. Котов В.Е. Сети Петри / В.Е. Котов. – М.: Наука, 1984. – 160 с.

22. Оре О. Теория графов. – М.: Наука, 1980. – 336 с.

23. Питерсон Дж. Теория сетей Петри и моделирование систем / Дж. Питерсон. – М.: Мир, 1984. – 264 с.

24. Татт У. Теория графов: Пер. с англ. - М.: Мир, 1988. - 424 с.

Дополнительная:

25. Толстых А.В. Имитационное моделирование угроз информационной безопасности с помощью сетей Петри / А.В. Толстых, В.В. Меньших// Актуальные вопросы эксплуатации систем охраны и защищенных телекоммуникационных систем: сборник материалов Всероссийской научно-практической конференции. – Воронеж: Воронежский институт МВД России, 2014, с. 216 – 218.

26. Толстых О.В. Разработка структурно-параметрических моделей систем защиты информации объектов информатизации органов внутренних дел: автореф. дис. … канд. техн. наук / О.В. Толстых. – Воронеж: ВИ МВД России, 2012. – 16 с.

Сергей Анатольевич Гречаный
Александр Викторович Сидоров
Ольга Владимировна Толстых
Юлия Сергеевна Никитина

РАЗРАБОТКА МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ЦЕНТРОВ

Методические рекомендации

В авторской редакции.
Компьютерный набор О.В. Толстых
Объем 0,6 Мб.

Воронежский институт МВД России
394065, Воронеж, просп. Патриотов, 53