МЕЖРЕГИОНАЛЬНОЕ ОБЩЕСТВЕННОЕ УЧРЕЖДЕНИЕ
«ИНСТИТУТ ИНЖЕНЕРНОЙ ФИЗИКИ»
(г. Серпухов Московской области)

На правах рукописи

Ковалев Максим Сергеевич

ОПТИМИЗАЦИЯ РАЗМЕЩЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УЗЛАХ КОММУТАЦИИ VPN СЕТИ

05.12.13 – «Системы, сети и устройства телекоммуникаций»

Диссертация
на соискание ученой степени кандидата технических наук

Научный руководитель: Цимбал Владимир Анатольевич, заслуженный деятель науки РФ, доктор технических наук, профессор

Серпухов – 2017

С О Д Е Р Ж А Н И Е

ВВЕДЕНИЕ

Современное общество является информационным обществом. Это обусловлено тем, что в экономику, социальную сферу и другие области деятельности государства, социальных групп и отдельных людей глубоко проникли и стали востребованными информационные технологии. Принятие различных решений органами государственной власти, руководством предприятий большого, среднего и малого бизнеса, банковской сферой, сферой образования и здравоохранения, а также другими сферами производственной, общественной и личной жизни требует обработки больших объемов информации и соответствующего информационного обмена между участниками того или иного управленческого процесса. Все это реализуется на компьютерах различной производительности и объектной ориентации, объединенных соответствующими локально-вычислительными сетями (ЛВС), а также различными сетями связи (от местных до глобальных), создающими транспортную среду для нужд информационного обмена. При этом наиболее распространенными сетями управленческого типа являются виртуальные частные сети (VPN), реализованными на базе сетей типа NGN или пост-NGN [107]. Ярким примером такой сети является телекоммуникационная сеть для государственных нужд, реализуемая в рамках Федеральной целевой программы (ФЦП) «Электронная Россия» [115].

В обобщенном виде VPN сеть содержит совокупность территориально разнесенных ЛВС, каждая из которых включает некоторое множество персональных компьютеров (хостов) и сервер, при этом хосты и сервер, как правило, взаимодействуют по принципу «клиент-сервер». Подчеркнем, что на сервере, как правило, реализуется некоторая объектно-ориентированная база данных, нужная для принятия того или иного управленческого решения. Взаимосвязь совокупности ЛВС в рамках VPN осуществляется с помощью пограничных маршрутизаторов, реализующих функции прокладки и поддержания маршрутов между совокупностью ЛВС, и сегментов

транспортной сети общего назначения, выделенных в интересах данной VPN. Отметим, что при этом внутри транспортной сети (например, NGN сети) также имеются свои маршрутизаторы [107].

Одной из важных задач, решаемых VPN сетью, является задача обеспечения устойчивости функционирования самой сети, а также обеспечение безопасности циркулирующей в ней информации [107]. Злоумышленники, хакеры, вандалы и другие нарушители способны организовать атаки различного рода как на элементы сети (маршрутизаторы, узлы коммутации, хосты), так и на сегменты самой сети для достижения тех или иных целей. Кроме того, атакам могут быть подвержены серверы с размещенными на них базами данных. В настоящее время известно много примеров подобных атак [2, 9, 40, 77, 97, 110]. В рамках данного исследования все объекты VPN сети, подвергаемые в потенциале атакам нарушителей, называются информационными объектами сети (ИОС).

Атаки на VPN сеть реализуются в основном с целью блокирования тех или иных узлов коммутации путем переполнения их буферной памяти, а также искажением и модификацией маршрутных таблиц. Атаки на серверы ЛВС, содержащие базы данных, организуются с целью копирования, модификации и искажения содержащейся в них информации [9, 40, 77]. Такие атаки способны вывести VPN сеть (сегмент VPN сети) на срок до десятков часов, а серверы от часов до нескольких суток. Все это приводит к огромным материальным и финансовым потерям (ущербу) [2, 9, 40].

Парирование данных угроз в VPN сетях реализуется путем использования различных средств защиты информации (СЗИ). К настоящему времени в распоряжении проектировщиков сетей связи имеется большое количество таких СЗИ и, как правило, все они сертифицированы ФСТЭК [7, 19, 31, 85, 119]. К ним относятся СЗИ от несанкционированного доступа на рабочих станциях и серверах (Secret Net), программно-аппаратные комплексы защиты от несанкционированного доступа («Соболь»), средства контроля доступа к каналу с модулем маршрутизатора (аппаратно-программный комплекс шифрования

«Континент») и другие (боле подробный перечень сертифицированных СЗИ представлен в приложении А). Все они отличаются совокупностью реализуемых функций защиты информации, форматом исполнения и, соответственно, стоимостью [85, 119].

В целом все средства защиты ИОС можно разделить на две большие группы: универсальные, решающие в полном объеме задачи защиты информации и неуниверсальные, реализующие только основные (профильные) функции защиты информации. Кроме того, обе группы средств могут быть однородными и неоднородными [119].

Проблема защиты информации в сетях телекоммуникаций широко освещена в трудах ведущих российских ученых Белова Е.Б., Галкина А.П., Герасименко В.А., Грушо А.А., Домарева В.В., Завгороднего В.И., В.Е. Касперского, Зегжды П.Д., Лося В.П., Лукацкого А.В., Малюка А.А., Медведковского И.Д., Молдовяна А.А., Никитина О.Р., Петракова А.В., Полушина П.А., Самойлова А.Г., Соколова А.В., Торокина А.А., Шаньгина В.Ф., Шелухина О.И., Хорева А.А., Ярочкина В.И., Монахова М.Ю., Куприянова А.И., Мазина А.В. Значительный вклад в решение выделен-ной проблемы внесли зарубежные исследователи M. Howard, R. Graham, D. Sanai, S. Manwani, M. Montoro, F. Cohen, J. Jung, D.Moore, C.Zou и другие.

Исследования показали, что достичь требуемого уровня защищенности информации в VPN сетях возможно, например, экстенсивным путем - увеличением числа размещаемых однотипных средств защиты на ИОС и их совершенствованием. Однако, это приводит к существенному удорожанию всей системы защиты. С другой стороны, существует интенсивный путь достижения требуемого уровня защищенности, базирующийся на оптимальном комплексном использовании СЗИ на ИОС [30].

В связи с изложенным, возникает следующее **противоречие**: с одной стороны, существует большое множество СЗИ для ИОС, решающих задачу обеспечения заданного уровня защищенности информации, с другой стороны отсутствует научно-методический аппарат оптимального размещения таких СЗИ

на ИОС, обеспечивающих заданный уровень защищенности информации при минимуме их стоимости.

Разрешение этого противоречия заключается в разработке научно-методического аппарата оптимального размещения известных СЗИ на ИО VPN сети, обеспечивающих заданный уровень защищенности информации при минимуме их стоимости.

Исходя из изложенного, актуальной является **тема диссертации** «Оптимизация размещения средств защиты информации в узлах коммутации VPN сети».

Цель исследования: повышение уровня информационной безопасности комплекса технических средств организации защищенного канала связи в VPN сети.

Объект исследования: комплекс технических средств организации защищенного канала связи в VPN сети.

Предмет исследования: методы, модели и механизмы обеспечения многоуровневой безопасности защищенного канала связи в VPN сети.

Научная задача исследования: научное обоснование моделей, методики и комплекса технических средств, обеспечивающих снижение уровня ущерба, наносимого информации в информационных объектах VPN сети нарушителем, за счет оптимального размещения СЗИ при минимуме их стоимости.

Для решения этой общей научной задачи в диссертации ставятся и решаются следующие подзадачи:

- обоснование и выбор показателя эффективности защиты информации в ИОС;
- разработка моделей воздействия нарушителя на информационные массивы ИОС, защищенные многоуровневой СЗИ, учитывающих ряд дополнительных факторов, присущих современным СЗИ сетей связи;
- разработка методики оптимизации размещения средств защиты на ИО VPN сети.

В ходе решения этих подзадач были сформированы следующие **научные результаты**, представляемые к защите:

1. Аналитические и имитационная модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети.

2. Автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат.

Научная новизна полученных в диссертационной работе результатов заключается в том, что:

- разработанные аналитические модели воздействия нарушителя построены на основе математического аппарата конечных марковских цепей, что позволяет, в отличие от известных, учитывать предысторию вскрытия отдельных уровней защиты и динамику их восстановления как по времени, так и по решению администратора сети, что характерно для современных сетевых систем защиты информации;

- оптимизация размещения разнотипных и разнородных средств защиты на информационных объектах сети, содержащих большое количество массивов информации различной важности, в отличие от известных подходов, впервые выполнена на основе пошаговой процедуры, реализующей сочетание динамического и вероятностно-игрового методов.

Достоверность и обоснованность разработанного математического аппарата подтверждена совпадением основных получаемых результатов с результатами ручного счета известными апробированными математическими методами, корректностью и логической обоснованностью постановки частных подзадач исследования и принятых допущений, а также тем, что все разработанные модели, средства защиты и методика доведены до программной реализации и могут быть непосредственно использованы для модернизации существующих и разработки перспективных сетевых СЗИ.

Практическая значимость полученных результатов состоит в том, что только за счет оптимизации размещения имеющихся средств защиты (без

дополнительных финансовых затрат) уровень ущерба, который может быть нанесен информации, используемой на исследуемом ИОС, может быть снижен на 17-25%.

Диссертация состоит из введения, трех разделов, заключения и списка использованных источников.

Результаты опубликованы в 31-й публикации, из них: 29 статей в научно-технических сборниках, в том числе 5 статей в журналах из Перечня ВАК; 1 отчёт об ОКР и 1 патент на полезную модель.

Результаты работы внедрены:

1. В МОУ «Институт инженерной физики» в СЧ ОКР «Модуль-ИИФ» (акт о реализации МОУ «ИИФ» от 17.11.2016 г.).

2. В АО «Центральный научно-исследовательский институт экономики информатики и систем управления» при обосновании размещения средств защиты информации в узлах коммутации VPN сети специального назначения в рамках ОКР «Заполье», ОКР «Ретранслятор» (акт о реализации АО «ЦНИИ ЭИСУ» от 19.01.2017 г.).

3. В филиале Военной академии РВСН имени Петра Великого в учебном процессе по кафедре «Автоматизированные системы боевого управления» при изучении дисциплины «Криптографические методы и средства защиты информации» (акт о реализации ФВА РВСН от 26.01.2017 г.).

Автор выражает искреннюю благодарность научному руководителю Заслуженному деятелю науки РФ, доктору технических наук, профессору Цимбалу В.А. за оказанную при написании диссертации, и критические замечания, высказанные при ее обсуждении.

1 СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ КАК СЛОЖНАЯ СИСТЕМА И ПОДСИСТЕМА ИТС

1.1 Анализ VPN сетей и подход к синтезу систем защиты информации ИТС на этой основе

1.1.1 Обобщенный анализ VPN сетей

Одним из признаков крупной территориально-распределенной корпоративной сети является применение глобальных связей для объединения отдельных локальных сетей филиалов предприятия и компьютеров его удаленных сотрудников с центральной локальной сетью [107].

Традиционный способ построения ведомственных или корпоративных сетей - использование выделенных (чаще всего арендованных у телекоммуникационных операторов) каналов связи для организации связей «сеть-сеть» и телефонных сетей общего пользования (ТфОП) для связи удаленных пользователей. Быстрое развитие IP-сетей (и прежде всего Интернета) породило новую тенденцию использование для построения глобальных корпоративных связей более дешевого и более доступного (по сравнению с выделенными каналами) транспорта пакетных сетей [107].

Однако такое заманчивое и дешевое решение - передача корпоративных данных через публичную пакетную сеть, например, через Интернет, представляет собой очевидную угрозу для безопасности сети любого предприятия, не говоря уж об органах государственной власти и управления. Внутренние ресурсы корпоративной сети становятся доступными для многочисленных пользователей Интернета, а конфиденциальный трафик может быть просмотрен злоумышленниками. Кроме этого, отказавшись от выделенных каналов с гарантированной пропускной способностью, предприятие вынуждено мириться с непредсказуемым характером каналов связи в Интернете в части производительности и надежности [34, 80].

Для решения этих проблем может быть использована технология виртуальных частных сетей VPN (Virtual Private Network) [107]. Эта технология позволяет превратить соединения в пакетных сетях общего пользования в защищенные каналы с гарантированной полосой пропускания. VPN обеспечивает безопасность и секретность как в традиционной частной сети, при сохранении стоимости устанавливаемых соединений, так и в сети общего пользования. Следовательно, такая услуга будет востребована многими предприятиями и организациями, не имеющими собственных сетевых ресурсов, прежде всего органами государственной власти и бюджетными организациями, ввиду ее экономичности и доступности.

VPN - это объединение удаленных локальных сетей или отдельных рабочих мест с использованием специальных аппаратных или программных устройств, осуществляющих информационную защиту транзитного трафика и его туннелирование поверх публичных сетей с пакетной передачей информации.

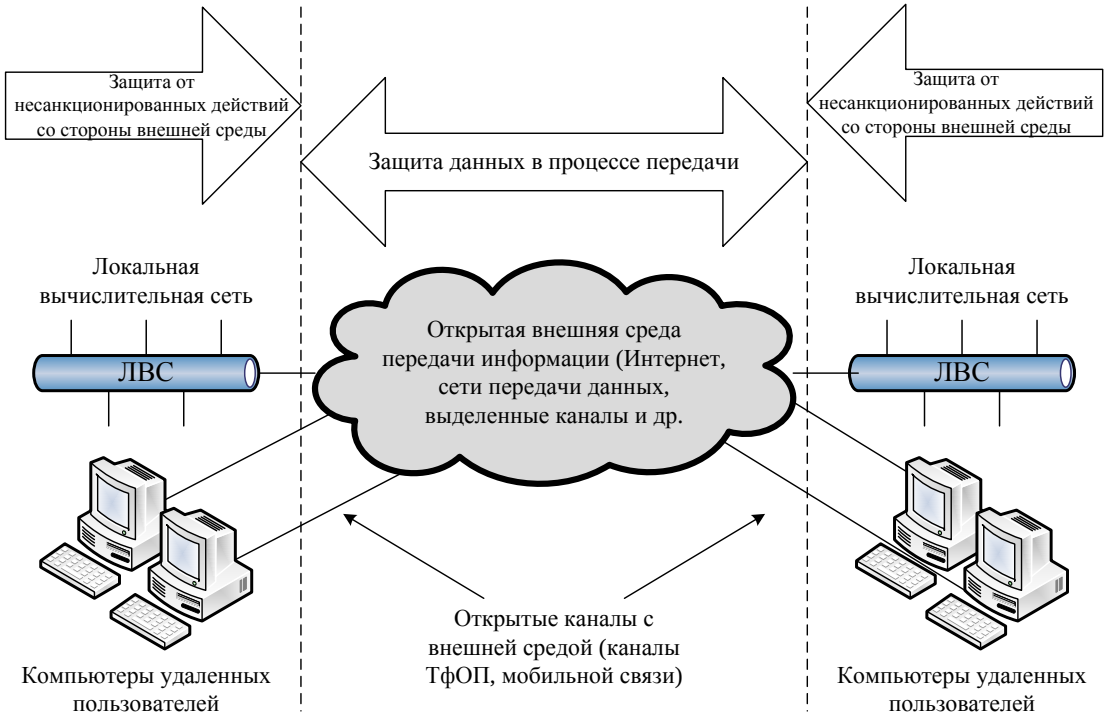


Рисунок 1.1 – Задачи по обеспечению безопасности информационного взаимодействия

Безопасность информационного взаимодействия как локальных сетей, так и отдельных компьютеров через открытые публичные пакетные сети, например, через сеть Интернет, требует качественного решения двух базовых задач (рисунок 1.1) [107]:

- защиты, подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;

- защиты информации в процессе передачи по открытым каналам связи.

Открытую внешнюю среду передачи информации можно разделить на среду скоростной передачи данных, в качестве которой может использоваться выделенная IP-сеть или Интернет, а также более медленные общедоступные каналы связи, в качестве которых чаще всего применяют каналы телефонной сети. Наиболее простым способом объединения локальных сетей и удаленных компьютеров является объединение на основе глобальной сети Интернет (рисунок 1.2) [107].

Организация виртуальных сетей на основе Интернета обладает рядом преимуществ:

- обеспечивает масштабируемую поддержку удаленного доступа к ресурсам локальной сети, позволяя мобильным пользователям связываться по местным телефонным линиям с поставщиками услуг Интернета и таким образом входить в свою корпоративную сеть;

- при организации удаленного доступа пользователей к локальной сети исключается необходимость в наличии модемных пулов, а трафиком дистанционного доступа можно управлять точно так же, как любым другим трафиком Интернета;

- сокращаются расходы на информационный обмен через открытую внешнюю среду:

а) использование Интернета для объединения локальных сетей значительно дешевле аренды каналов связи телефонных и других глобальных сетей,

например, ATM или Frame Relay, не говоря уже о стоимости самостоятельного построения сети;

б) при удаленном доступе вместо того, чтобы устанавливать дорогостоящие непосредственные соединения с локальной сетью по междугородной или международной телефонной связи, удаленные пользователи могут подключаться к Интернету и далее связываться с сетью своей организации через эту глобальную сеть [107].

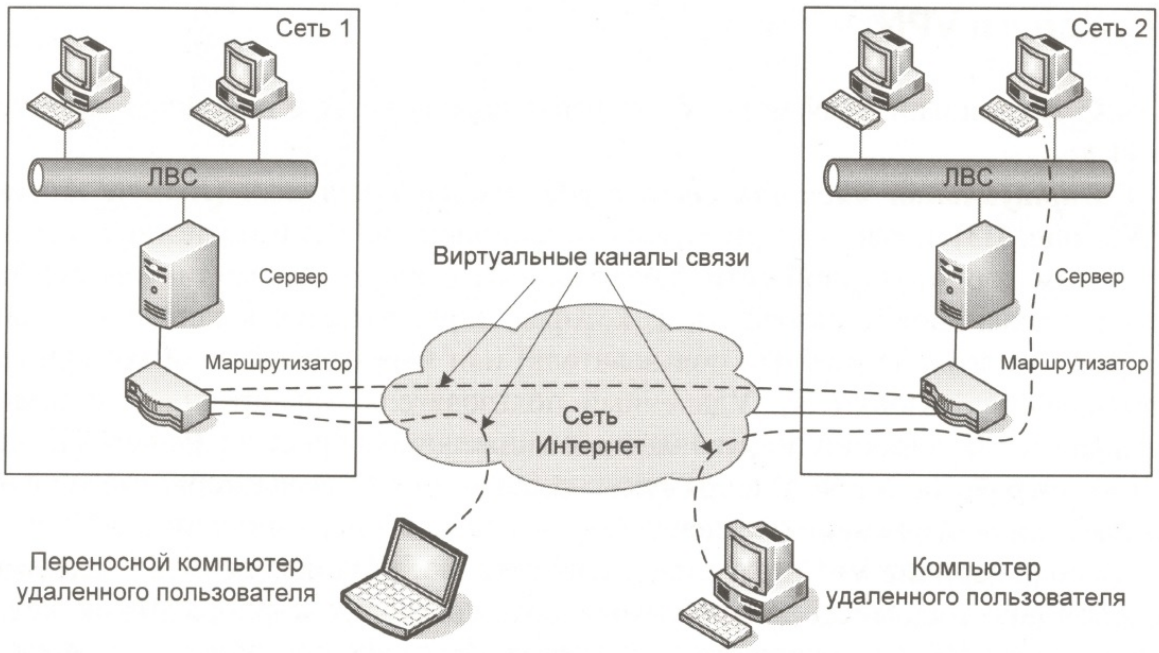


Рисунок 1.2 – Построение виртуальной частной сети на основе Интернета

Однако гарантированное качество обслуживания для потоков пользовательских данных, а также защиту их от возможного несанкционированного доступа или разрушения в полной мере могут обеспечить только выделенные IP-сети, а также сети ATM или Frame Relay, принадлежащие отдельным провайдерам. Использование публичных сетей ATM или Frame Relay в качестве основы для предоставления услуг VPN имеет одно несомненное преимущество по сравнению с Интернетом, а именно встроенную поддержку качества транспортного обслуживания. Однако повсеместная распространенность сетей на базе протокола IP, их универсальность и экономичность делает эти сети более привлекательной основой создания VPN для большинства предприятий и орга-

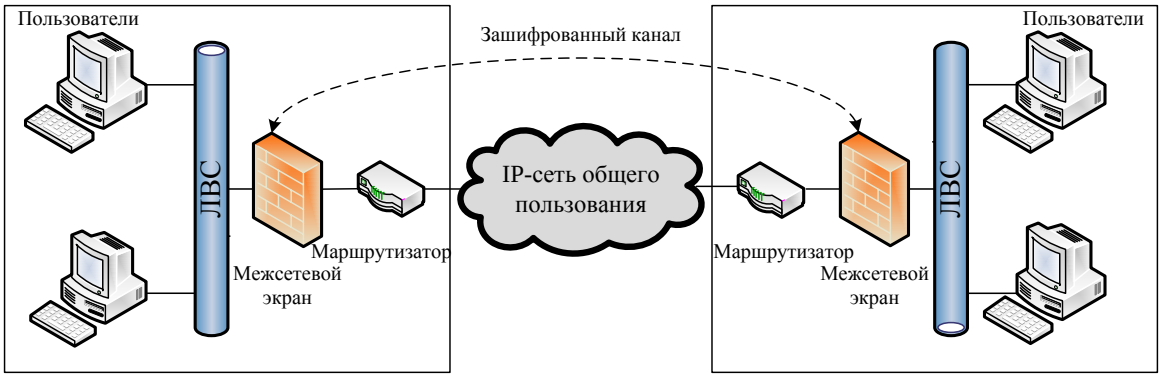
низаций. К тому же в выделенных IP-сетях начинают широко внедряться такие протоколы и технологии управления качеством обслуживания, как RSVP, DiffServ и MPLS [42, 107].

Существует несколько вариантов технической реализации VPN. Основными критериями выбора того или иного решения являются производительность средств построения VPN и, конечно, их стоимость. Для создания виртуальной частной сети могут использоваться аппаратные, программные средства или их комбинация. Обычно аппаратные средства являются более производительными, но и более дорогостоящими. Аппаратные методы шифрования обеспечивают более высокий уровень безопасности, чем программные, поскольку могут поддерживать ключи большей разрядности без увеличения задержки при передаче данных. Кроме того, аппаратные средства обеспечивают лучшую масштабируемость. Однако программные средства также имеют ряд преимуществ, главное из которых меньшая стоимость [107].

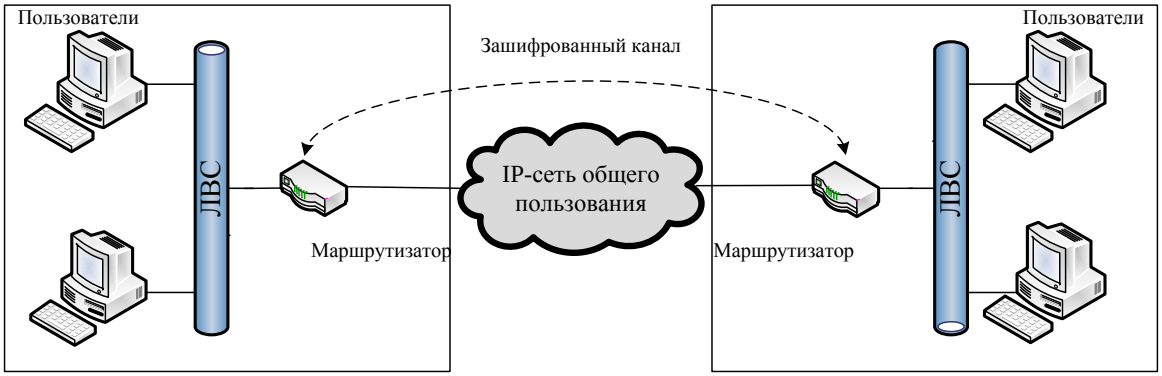
На рисунке 1.3 представлены следующие варианты технической реализации VPN сетей:

- VPN на базе межсетевых экранов (рисунок 1.3 а);
- VPN на базе маршрутизаторов (рисунок 1.3 б);
- VPN на базе программного обеспечения (рисунок 1.3 в);
- VPN на базе специализированных аппаратных средств (рисунок 1.3 г).

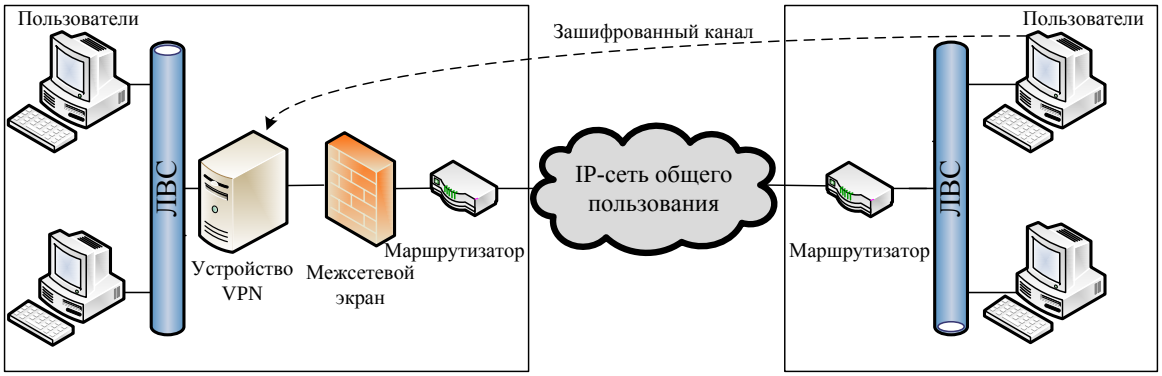
При построении виртуальных частных сетей большую роль играют отношения организации с провайдером VPN-услуг, в частности распределение между ними функций по конфигурированию и эксплуатации VPN-устройств. Под организациями здесь подразумеваются различные корпоративные пользователи, например, органы государственной власти, бюджетные организации, а также различные коммерческие предприятия [107].



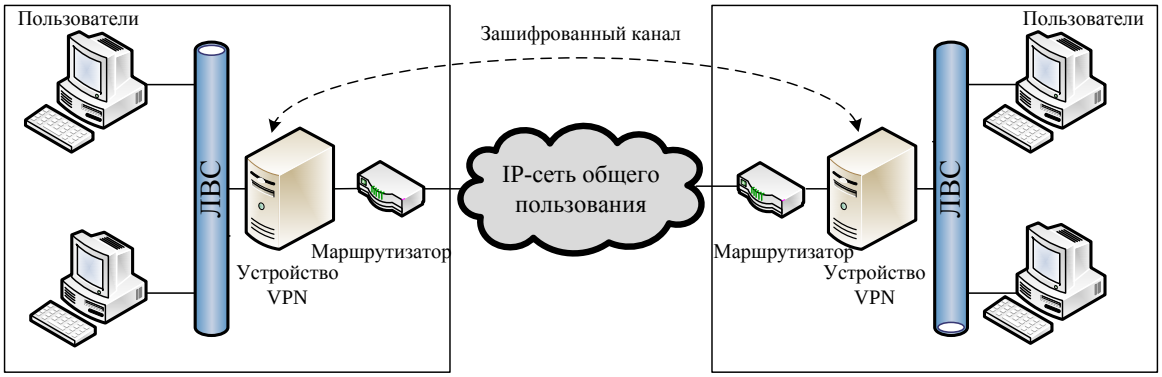
а)



б)



в)



г)

Рисунок 1.3 – Варианты технической реализации VPN

При создании защищенных каналов виртуальных сетей VPN-средства могут располагаться как в сети провайдера, так и в сети пользователя. В зависимости от этого фактора различают три схемы поддержки виртуальной сети [107]:

- корпоративная схема - все средства VPN размещаются в сети организации;

- провайдерская схема - все средства VPN размещаются в сети провайдера;

- смешанная схема - часть средств VPN размещаются в сети провайдера, а остальная часть - в сети организации.

При практической реализации VPN одной из главных задач является определение оптимального расположения VPN-устройств относительно других устройств защиты сети. Как правило, при построении VPN администратор сталкивается с тем, что для обеспечения безопасности корпоративной сети уже используется какое-либо защитное устройство (чаще всего это межсетевой экран или фильтрующий маршрутизатор, выполняющий эту функцию). В этом случае возникает задача размещения межсетевого экрана и VPN-шлюза. Совмещение функций межсетевого экрана и VPN-шлюза эту проблему снимает, но только частично. Во-первых, эта тенденция не абсолютна и имеет противников, а во-вторых, на сегодняшний день уже выпущено и продолжает выпускаться большое количество VPN-шлюзов без функций межсетевого экрана и межсетевых экранов без функций VPN-шлюзов [107].

При выборе варианта взаимного расположения VPN-шлюза и межсетевого экрана необходимо учитывать ряд факторов. Во-первых, межсетевой экран не может контролировать сетевой доступ на основании зашифрованных пакетов. Во-вторых, VPN-шлюз сам требует защиты от угроз из сети общего пользования. В-третьих, конфигурация связей, образованная шлюзом и межсетевым экраном, может повлиять на надежность соединения корпоративной сети с IP-сетью общего пользования [107].

Можно выделить следующие варианты взаимного расположения VPN-устройств в сети [107]:

- размещение шлюза перед межсетевым экраном;
- размещение шлюза позади межсетевого экрана;
- реализация функций шлюза в межсетевом экране;
- раздельное подключение шлюза и межсетевого экрана;
- подключение шлюза параллельно межсетевому экрану.

1.1.2 Технологии информационной безопасности в VPN-сетях

Обеспечение надежной защиты представляет собой самую острую проблему при реализации виртуальных частных сетей. Преимущества технологии VPN настолько убедительны, что уже сегодня многие компании начинают строить свою стратегию с учетом использования открытых сетей, и прежде всего Интернета, в качестве главного средства передачи информации, даже той, которая является уязвимой или жизненно важной. Поэтому международные и общественные организации, отдельные компании-производители программного обеспечения и оборудования начали предпринимать усилия по разработке открытых (свободных для распространения и реализации) протоколов и стандартов в области защиты информации. К ним, в частности, можно отнести следующие протоколы: PPTP, L2TP, IPSec, SKIP, SSL/TLS, SOCKS, SHTTP, S/MIME, PGP [38, 101].

Перечисленные протоколы предусматривают организацию защиты данных на различных уровнях Эталонной модели взаимосвязи открытых систем (ЭМВОС) [107].

В настоящее время на базе этих протоколов сформировался ряд подходов к организации защиты информации, что породило появление нескольких классов продуктов [107]:

- фильтров пакетов, базирующихся на протоколах сетевого и канального уровней;

- proxy-серверов на основе протокола SOCKS;

- продуктов, использующих протоколы прикладного уровня.

По крайней мере два первых класса можно отнести к продуктам, предназначенным для организации VPN. Также следует отметить некоторые общие закономерности при организации виртуальных сетей [107]:

- чем ниже уровень ЭМВОС, на котором организуется защита, тем она прозрачнее для приложений и незаметнее для пользователей; однако тем меньше набор реализуемых услуг безопасности и тем сложнее организация управления;

- чем выше уровень ЭМВОС, на котором реализуется защита, тем шире набор услуг безопасности, надежнее контроль доступа и проще конфигурирование правил доступа; однако тем «заметнее» становится защита для приложений и пользователей.

При любом подходе протоколы, используемые для организации VPN, прозрачны для протоколов защиты более высоких уровней (в частности, прикладного), и применение приложений, реализующих, например, SHTTP или S/MIME, наряду с защитой на более низком уровне, нисколько не уменьшает, а только увеличивает уровень безопасности.

Обеспечение безопасности в VPN на базе IP осуществляется следующими способами:

- шифрование - это кодирование данных в соответствии с определенным математическим алгоритмом. Алгоритм шифрования основан на преобразованиях данных при помощи кодовой комбинации, выполняющей функцию ключа. Чем больше в такой комбинации цифр, тем большее время потребуется потенциальному взломщику для перебора ключей. Следовательно, чем длиннее ключ, тем более надежную защиту обеспечивает данный алгоритм. Существует несколько видов шифрования - это симметричные (личные ключи), асимметричные (открытые ключи) [10, 13, 27, 37,102,108];

- аутентификация (authentication) («установление подлинности») предотвращает доступ к сети нежелательных лиц и обеспечивает санкционированный

вход для легальных пользователей. Фактически аутентификация - это процедура доказательства пользователем того, что он именно тот, за кого себя выдает, в частности, доказательство того, что именно ему принадлежит введенный им идентификатор [8, 109];

- авторизация - средства авторизации (authorization) контролируют доступ легальных пользователей к ресурсам системы, предоставляя каждому из них именно те права, которые были определены администратором. Кроме предоставления прав доступа пользователей к каталогам, файлам и принтерам, система авторизации может контролировать возможность выполнения пользователями различных системных функций, таких как локальный доступ к серверу, установка системного времени, создание резервных копий данных, выключение сервера и т.п. Применительно к VPN система авторизации может регулировать доступ пользователя к тем или иным средствам шифрования пакетов или даже в целом к определенным VPN-устройствам [24,25,26];

- туннелирование - при туннелировании пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Например, при туннелировании кадр Ethernet может быть размещен в пакете IP, а пакет IPX - в пакете IP. Возможен и такой вариант: пакет IP размещается в пакете IP. Туннелирование широко используется для безопасной передачи данных через публичные сети путем упаковки пакетов во внешнюю оболочку. Туннель создается двумя пограничными устройствами, которые размещаются в точках входа в публичную сеть.

Протоколы канального уровня PPTP, L2F и L2TP лучше всего подходят для защиты информационного взаимодействия при удаленном доступе к локальной сети [75, 107].

Указанные выше протоколы инкапсулируют кадры канального протокола в протокол сетевого уровня. С помощью последнего данные затем передаются по составной сети. Кроме того, эти протоколы близки также тем, что их главная область применения - решение задачи защищенного многопротокольного удаленного доступа к ресурсам корпоративной сети через публичную сеть, в

первую очередь через Интернет. Так как практически любое клиентское программное обеспечение использует сегодня для удаленного доступа стандартный протокол канального уровня PPP, то и протоколы PPTP, L2F и L2TP основаны на инкапсуляции кадров PPP в пакеты сетевого уровня. В таком качестве используется прежде всего IP-протокол.

При построении распределенных корпоративных сетей (интранет VPN и экстранет VPN) наиболее целесообразно использовать протоколы сетевого уровня SKIP и IPsec.

Протокол SKIP

SKIP (Simple Key management for Internet Protocol) - протокол управления криптографическими ключами в Интернете был разработан компанией Sun Microsystems в 1994 году и предложен в качестве стандарта Интернета. В основе протокола SKIP лежит криптография открытых ключей Диффи-Хеллмана. Протокол SKIP имеет, по сравнению с существующими системами шифрования трафика, ряд уникальных особенностей [75]:

-*универсальность* - он шифрует IP-пакеты, не зная ничего о приложениях, пользователях или процессах, их формирующих; установленный в компьютере непосредственно над пакетным драйвером, он обрабатывает весь трафик, не накладывая никаких ограничений ни на вышележащее программное обеспечение, ни на физические каналы, в которых он используется;

- *сеансонезависимостъ* для организации защищенного взаимодействия не требуется дополнительный информационный обмен (за исключением однажды и навсегда запрошенного открытого ключа партнера по связи);

- *независим от системы шифрования* - пользователь может выбирать любой из предлагаемых поставщиком или использовать свой алгоритм шифрования информации; могут использоваться различные (в разной степени защищенные) алгоритмы шифрования для закрытия пакетного ключа и собственно данных.

Система протоколов IPsec

Internet Protocol Security (IPSec) является системой открытых стандартов, которая имеет на сегодня вполне четко очерченное ядро и в то же время позволяет достаточно просто дополнять ее новыми протоколами, алгоритмами и функциями.

Система IPSec решает следующие основные задачи установления и поддержания защищенного канала [23]:

- аутентификацию пользователей или компьютеров при инициации защищенного канала;

- шифрование и аутентификацию передаваемых данных между конечными точками защищенного канала;

- автоматическое снабжение конечных точек канала секретными ключами, необходимыми для работы протоколов аутентификации и шифрования данных.

Для решения поставленных задач система IPSec использует протоколы трех типов [23]:

- *AH (Authentication Header*), который обеспечивает целостность и аутентификацию источника данных в передаваемых пакетах, а также опционально - защиту от ложного воспроизведения пакетов;

- *ESP (Encapsulation Security Payload*), обеспечивающий шифрование, аутентификацию и целостность передаваемых данных и опционально - защиту от ложного воспроизведения пакетов;

- *IKE (Internet Key Exchange*), определяющий способ инициализации защищенного канала, а также процедуры обмена и управления секретными ключами в рамках защищенного соединения.

Для шифрования данных в IPSec может быть применен любой симметричный алгоритм шифрования, использующий секретные ключи. Целостность и аутентификация данных выполняются с помощью вычисления дайджеста данных с помощью односторонней функции (называемой также хэш-функцией, или дайджест-функцией), в которой параметром является секретный ключ [23].

Основным ограничением IPSec является то, что он поддерживает только те приложения, которые использует для передачи данных на сетевом уровне протокол IP. Это значит, что приложения IPX или NetBEUI не могут непосредственно воспользоваться функциями защиты, обеспечиваемыми IPSec. Такое ограничение, правда, будет все меньше и меньше затруднять работу по защите передаваемых данных, так как в настоящее время в мире только малая часть компьютеров вообще не поддерживает IP. Подавляющее большинство компьютеров используют его либо как единственный протокол, либо в качестве одного из нескольких протоколов [107].

Но и для случая, когда через Интернет необходимо передать трафик по протоколу, отличному от IP, существует стандартное решение. IPSec может работать совместно с протоколами L2TP или L2F, которые выполняют только туннелирование, но не обеспечивают шифрование и аутентификацию данных. Эти протоколы создают через Интернет туннель для пакетов любых протоколов, упаковывая их в пакеты IP. А поскольку трафик с помощью L2F или L2TP оказывается упакованным в пакеты IP, то дальше уже можно использовать IPSec для его защиты. Таким образом, комбинирование IPSec с универсальными протоколами туннелирования типа L2F/L2TP решает задачу защиты данных и для протоколов, отличных от IP [42].

Протокол IPSec может защищать трафик как текущей версии протокола IPv4, применяемой сегодня в Интернете, так и трафик новой версии IPv6.

1.1.3 Общий подход к синтезу систем защиты информации информационной телекоммуникационной системы

Разнообразие природы различных систем, окружающих человека и в той или иной мере вовлекающих его в свою деятельность, привело и к многообразию определений понятия системы [15-18]. В данной работе используются два определения: вербальное: «Система – совокупность элементов, находящихся в отношениях и связях между собой, взаимодействующих с внешней средой и

образующих некоторое целостное единство для достижения цели, определенной заданными критериями при определенных ограничениях» и формальное, приведенное в [90, 104, 106]: «Система – это отношение на непустых абстрактных множествах

$$S \subset \times \{V_i : i \in I\} \tag{1.1}$$

где × – символ декартова произведения; I – множество индексов.

Множество V_i – объекты системы. Так как множество I в рассматриваемых в данной работе системах конечно, то (1.1) может быть записано в виде:

$$S \subset V_1 \times V_2 \times ... \times V_n \tag{1.2}$$

Среди большого класса систем выделяют так называемые информационные системы (ИС), под которыми понимается [94] организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, включая используемые средства вычислительной техники и связи, реализующие информационные процессы, а среди последних - информационные телекоммуникационные системы (ИТС), в которых априори предполагается наличие конфликтных ситуаций, в основном по вопросам защиты информации, отнесенной к категории ограниченного пользования. При этом под «защитой информации» понимается [23] комплекс правовых, организационных, технических и иных специальных мер по обеспечению информационной безопасности (утечки, хищения, утраты, искажения, подделки информации, несанкционированный доступ (НСД) и распространение).

Вместе с тем, в классе систем (в том числе и ИТС) выделяют так называемые сложные системы, которые характеризуются не просто большой размерностью, но и многокритериальностью, иерархичностью структуры, наличием подсистем различной природы, подчиненных единой для всей системы цели.

В ряде научных работ [48, 51, 94] доказано, что ИТС также являются сложными системами.

Система защиты информации имеет ряд особенностей. Во-первых, обеспечение заданного уровня защищенности является не самоцелью, а потребно-

стью предъявления качественной информации для управления объектами различного назначения с целью повышения эффективности их применения, т.е. имеет место иерархия целей, представленная на рисунке 1.4.

СЗИ характеризуется некоторым подмножеством внутренних параметров *{X}*, обеспечивающим формирование подмножества выходных параметров *{Y}*, которое в свою очередь является подмножеством входных параметров для ИТС, и характеризующих качество выдаваемой информации. В общем случае подмножество *Y* представляет собой объединение подмножеств, обеспечивающих $\{Y_0\}$ и не обеспечивающих *{Y*}* выполнение поставленных перед ИТС задач.

Таким образом:

$$\{X\} \Rightarrow \{Y\} = \{Y_0 \cup Y^*\} \qquad (1.3)$$

и, следовательно, задачей СЗИ является не только снижение второй составляющей объединения (1.3), но и перевод некоторого необходимого и достаточного подмножества $\{Y_1\} \subset \{Y^*\}$ из второй составляющей в первую.

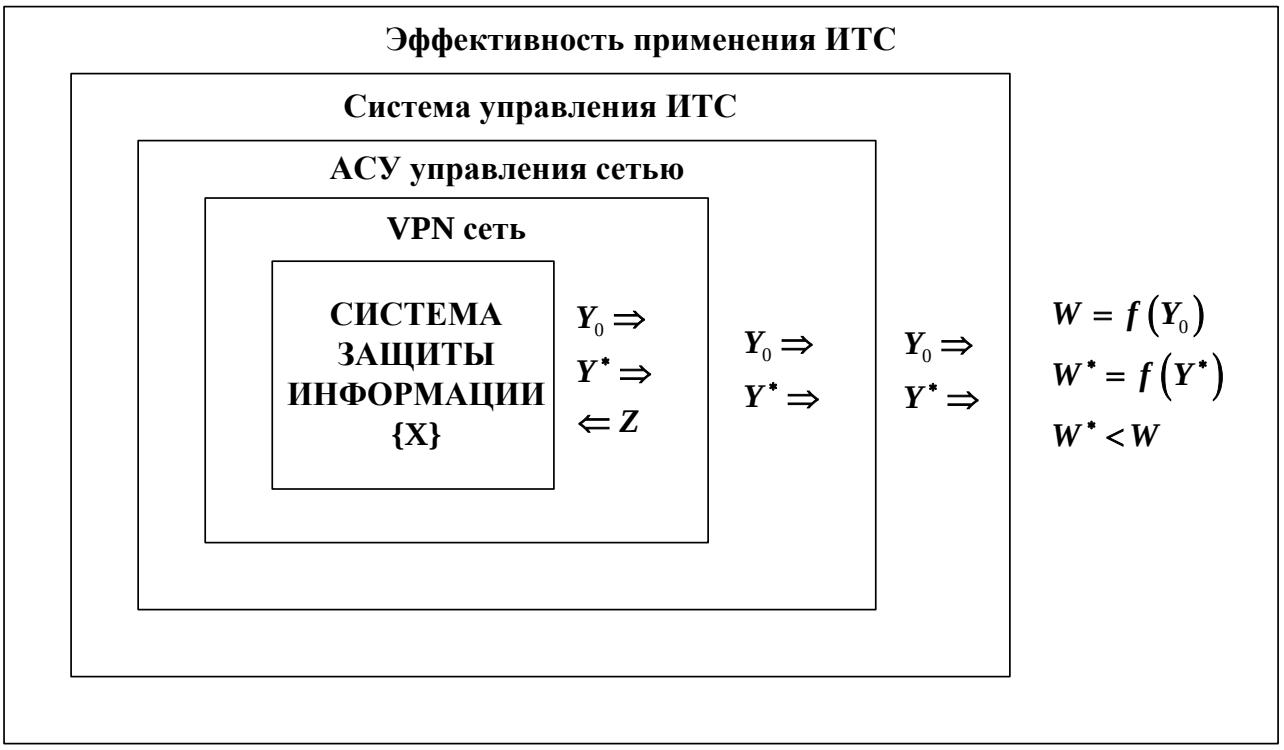


Рисунок 1.4. - Иерархия целей в использовании информации

Естественно, это может происходить только посредством расходования некоторого подмножества ресурсов $\{R\} \le \{R^{\partial}\}$ и в условиях ограниченного времени $\{T\} \le \{T^{\partial}\}$.

В такой интерпретации задача синтеза качественной СЗИ и эффективных алгоритмов ее функционирования может быть вербально сформулирована следующим образом:

найти такое подмножество внутренних параметров СЗИ (структуру системы - *S*, состав средств защиты – *A*, способов их использования – *L*) - $\{X\} \subset \{X^{\partial}\}$, при котором выходные параметры ИТС удовлетворяли бы заданным СУ ИТС требованиям по качеству доставки информации – {*K*} и при этом расходуемые ресурсы (финансовые и временные) не превысили допустимого уровня. Формальное представление задачи может быть представлено следующим образом:

Найти:

$$\{X\} \subset \{X^{\partial}\} \Rightarrow Y_0 \ge Y^{mp} \Rightarrow W \ge W^{mp}, \qquad (1.4)$$

при ограничениях $\{R\} \le \{R^{\partial}\}$ и $\{T\} \le \{T^{\partial}\}$.

По своему характеру задача (1.4) является оптимизационной и состоит в выборе такого набора значений $\{X\} \subset \{X^{\partial}\}$, который бы при условии некоторого (в общем случае случайного) подмножества входных воздействий – {*Z*}, обеспечил экстремум функционала полезности, задающего математическую модель СЗИ с ограничениями на {*Y*}, {*R*}, {*T*} и допустимые {*X*}:

$$Y = F\{X(S, A, L), Z, T\} \qquad (1.5)$$

где *Z, T* - отражают соответственно неопределенность как самих внешних воздействий, так и моментов их приложения.

Анализ построения и функционирования известных СЗИ как составной части ИТС, выполненный в ряде научных работ [57, 76, 95], показывает, что им присущи следующие характерные признаки:

ИТС предназначены для обеспечения информационного обмена, поэтому наличие конфликтной ситуации в вопросе защиты и нападения на обрабатываемую и передаваемую в ней информацию является важной особенностью ее функционирования. Внешняя среда имеет слабо предсказуемый динамический характер. Неопределенность поведения нарушителя, его целей приводит к необходимости использования рефлексивного подхода к исследованию процессов защиты информации, т.е. к учету различных вариантов действия нарушителя, рациональных с его точки зрения;

наличие взаимосвязанных единой общей целью обеспечения требуемой защищенности информации иерархических подсистем (например, в широко используемой СЗИ Secret Net [103]: подсистема внешней защиты, подсистема разграничения доступа к ресурсам, подсистема криптографической защиты). Связи между подсистемами нестабильны, их интенсивность меняется в зависимости от складывающейся ситуации;

объединение управляющей подсистемы (подсистема администрирования) и управляемой (подсистема средств защиты), способность выбирать альтернативы относительно своего поведения (разрешить или не разрешить данному пользователю доступ к требуемому ресурсу, продлить действие пароля или запретить и т. д.), т. е. принимать решения;

многомерность, обусловленная большим числом используемых однородных и неоднородных, универсальных и не универсальных средств защиты;

многообразие природы подсистем, их различная физическая сущность (коллективы людей – администраторы, аппаратные средства, программные средства, организационные и правовые методы и т.д.);

многокритериальность, определяемая разнообразием частных целей и комплексностью самого свойства - защищенность информации.

В соответствии с [16] системы, обладающие перечисленными характерными признаками, являются сложными системами и относятся к объектам исследования третьего методологического (системного) уровня, условно названного «организация–поведение». Для таких систем на практике построить доста-

точно обоснованный функционал (1.5) не представляется возможным, поэтому поставленная задача может рассматриваться как комбинаторная и формулироваться в терминах дискретного математического программирования [29, 117].

Однако, необходимость учета влияния множества факторов, ведет к чрезвычайно высокой размерности задачи и делает практически невозможным ее прямое решение на базе известных аналитических методов и средств, поэтому для исследования таких систем необходимо применять системный подход, технологическим инструментом которого является системный анализ, рассматривающий сложные системы как некоторое целое, состоящее из множества взаимосвязанных подсистем.

В связи с этим для достижения поставленной в работе цели воспользуемся важнейшими методами системного подхода: методом декомпозиции и методом целенаправленного перебора (с учетом интуиции и опыта исследователя) в сочетании с маргинальным подходом, суть которого состоит в варьировании одним из внутренних параметров СЗИ, при «закреплении» остальных.

Декомпозиция общей задачи позволяет выделить в ней следующие частные подзадачи:

синтез (выбор или разработка) опорного варианта СЗИ (построения и алгоритмов функционирования - подмножества внутренних параметров – $\{X\}$);

разработка (выбор) показателей оценивания степени защищенности информации и критериев выбора вариантов построения СЗИ;

оценивание выбранного варианта СЗИ, получение (вычисление) подмножества $\{Y\}$ при различных моделях воздействия нарушителя и принятие решения в соответствии с выбранными критериями о его использовании или совершенствовании.

Учитывая это и основываясь на общих закономерностях исследования систем третьего уровня, представим обобщенный алгоритм решения общей задачи в виде, изображенном на рисунке 1.5.

В соответствии с алгоритмом (рисунке 1.5) для решения общей задачи необходимо разработать:

математический аппарат теоретического обоснования требуемых норм защищенности информации, показателей и критериев оценивания степени ее защищенности в выбранном (разработанном) варианте СЗИ;

математический аппарат синтеза рациональных вариантов СЗИ для конкретных ИОС;

математический аппарат возможных (потенциальных) вариантов воздействия нарушителя и оценивания уровня защищенности информации при данном варианте СЗИ в ИОС.

Изучением общих закономерностей сложных систем занимается теория сложных систем (системология, общая теория систем). Суть этой теории заключается в том, что она ставит своей целью создание и изучение наиболее общих способов описания, законов функционирования и методов анализа и синтеза систем вне зависимости от их физической природы. Исследованием сложных технических систем занимается системотехника.

Учитывая тот факт, что информации как объекту переработки, и ИОС, как объекту ее использования, а СЗИ, как объекту обеспечения ее защищенности, присущи единичные, особенные характерные черты, для их исследования необходимо разработать в рамках названных наук специфический математический аппарат, позволяющий создавать качественные и эффективно используемые СЗИ в условиях, когда нарушитель стремится нанести объекту хранения максимальный ущерб.

В настоящее время имеются серьезные проработки вопросов обоснования требований [32,35,36,100], критериев и показателей [32,35,36,100], теоретических основ построения систем контроля и защиты информации [32,35,36,100], поэтому в данной работе основное внимание уделено совершенствованию математического аппарата оценивания степени защищенности информации в ИОС без и с СЗИ при различных моделях воздействия нарушителя, ограничившись только выбором показателей и критериев, необходимых для решения поставленной задачи.

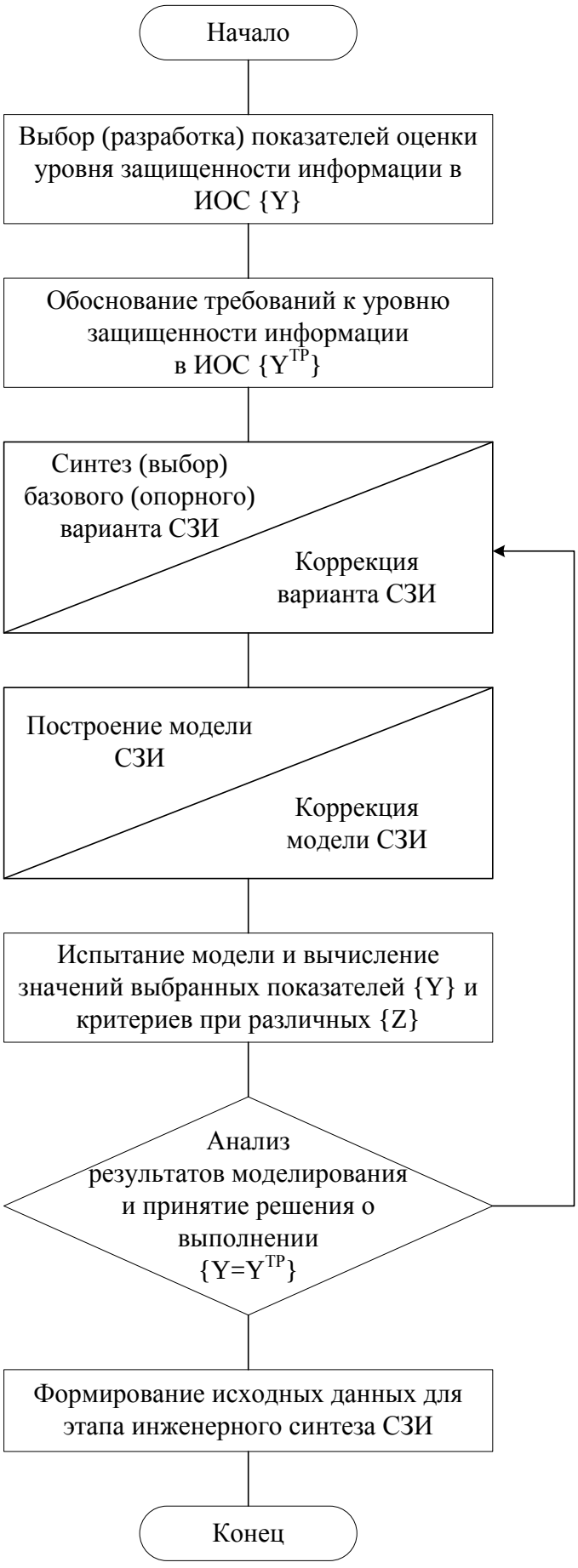


Рисунок 1.5 – Обобщенный алгоритм системного синтеза СЗИ ИТС

1.2 Обоснование и выбор критериев и показателей оценки защищенности информации в ИТС. Формализация задачи исследования.

Обобщая содержание дестабилизирующих факторов и угроз безопасности информации в ИОС ИТС, подробный анализ которых дан в [95,97], можно отметить, что совокупность множества источников, факторов и связанных с ними типов угроз, порождают некоторое подмножество, включающее:

нарушение физической и логической целостности информации;

ее несанкционированную модификацию, получение, размножение;

имитацию информации.

Из этого вывода следует, что необходимо осуществить обеспечение физической и логической целостности, предупреждение несанкционированной модификации, получения, размножения и имитации всей информации, хранимой и обрабатываемой в информационных объектах сети, а также передаваемой по каналам связи.

В результате такого анализа выделено некоторое наиболее важное (атрибутивное) свойство, характеризующее качество построения системы защиты и эффективность ее применения – защищенность информации**.**

Для проведения количественной оценки степени защищенности, формирования показателя качества системы защиты информации и эффективности ее применения в [46, 54] показано, что свойство защищенности информации есть комплексное свойство, характеризующее способность информации как предмета хранения, и ИОС, как объекта использования информации, противостоять различным типам угроз и включает следующие частные свойства: значимость (важность, стоимость), физическая и (или) логическая целостность (сохраняемость), копируемость, разглашаемость, динамичность (оперативность), верность (достоверность, точность), в которой в свою очередь выделяют безошибочность и истинность, кумулятивность и избирательность, конфиденциальность.

В таком случае объект исследования предлагается рассматривать, как комплекс технических средств, включающий [78, 79, 95]:

- средства хранения ключевой информации (закрытых ключей и сеансовых ключей) – SAD, физический носитель - оперативная память и долговременная память узла защищенного канала связи;

- средства обмена ключевой информации (режимы PSK, IKE, PKI) - физический носитель (для PSK), драйвер, аппаратный модуль;

- СЗИ от несанкционированного доступа на рабочих станциях и серверах (например, Secret Net);

- Программно-аппаратные комплексы защиты ПЭВМ от несанкционированного доступа (например, программно-аппаратное средство ЗИ «Соболь»);

- средства контроля доступа к каналу - модуль маршрутизатора (аппаратно-программный комплекс шифрования «Континент»);

- программные и программно-аппаратные МЭ с возможностью построения отказоустойчивых VPN (StoneGate Firewall/VPN);

- различное антивирусное ПО.

Будем считать, что для компрометации защищенного канала связи в сетях TCP/IP (VPN) злоумышленнику достаточно получить доступ хотя бы к одному из перечисленных технических средств организации защищенного канала связи (ТСОЗКС). Тогда безопасность защищенного канала можно рассматривать, как безопасность ТСОЗКС.

Многоуровневая безопасность каждого ТСОЗКС обеспечивается множеством средств защиты информации (ЗИ), которые реализуют один или несколько типовых механизмов: 1) идентификация/аутентификация; 2) контроль доступа; 3) шифрование; 4) экранирование; 5) контроль целостности; 6) туннелирование; 7) протоколирование и аудит.

Предположим, что каждый ТСОЗКС включает в себя следующие типовые средства ЗИ [52,62,72,73]:

а) стандартные средства операционной системы;

б) системы обнаружения и предотвращения вторжений - IDS/IPS (например, Snort, Snort inline, Cisco IPS);

в) антивирусное программное обеспечение (например, антивирус Касперского);

г) межсетевой экран (например, межсетевые экраны Cisco ASA);

д) средство доверенной загрузки (например, аппаратно-программный модуль доверенной загрузки «Соболь»);

е) аппаратное средство аутентификации (например, персональное средства аутентификации и хранения сертификатов Rutoken);

ж) аппаратное средство управления доступом (например, Secret Net).

Каждое типовое средство ЗИ может реализовывать тот или иной механизм защиты информации с некоторым показателем качества. Например, в качественной шкале «хорошо», «удовлетворительно», «плохо» получим:

Механизм / СЗИ	1	2	3	4	5	6	7
А	х	у	х	у	п	у	х
Б	п	п	п	х	у	п	х
В	п	п	п	п	х	п	х
Г	у	х	п	х	п	п	х
Д	х	х	х	п	х	п	у
Е	х	п	п	п	п	п	у
Ж	х	х	п	п	п	п	у

Учитывая многообразие и противоречивость оцениваемых свойств защищенности информации на основе теории квалиметрии в качестве показателя качества системы защиты и качества используемой в ИТС информации, целесообразно выбрать комплексный показатель, представляющий собой кортеж показателей частных атрибутивных свойств:

$$K = \langle k_1, k_2, ..., k_n \rangle, \qquad (1.6)$$

где k_i - показатель i-го атрибутивного свойства.

Для формирования критерия выбора того или иного варианта построения системы защиты информации (СЗИ), основываясь на выводах, сделанных в [50], выберем и методическую основу принятия решения - принцип принятия

решения. Если показатель качества, выбранного *j*-го варианта системы, описывается кортежем частных атрибутивных свойств (1.6), а показатель допустимого качества

$$K^{\partial} = \left\langle k_1^{\partial}, k_2^{\partial}, ..., k_n^{\partial} \right\rangle \tag{1.7}$$

есть множество (область) допустимых значений показателя, то критерии оценивания СЗИ: пригодности $\{G\}$, оптимальности $\{O\}$ и превосходства $\{S\}$ в векторной форме могут быть записаны в следующем виде:

$$G: \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial np} \right) \cong U, \ j = \overline{1,m} \tag{1.8}$$

$$O: \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial np} \right) \cap \left(K_{\langle n \rangle}^{j} = K_{\langle n \rangle}^{onm} \right) \cap \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial onm} \right) \cong U, \ j = \overline{1,m} \tag{1.9}$$

$$S: \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial np} \right) \cap \left(K^{j} \succeq\preceq K^{l} \right) \cong U, \ j = \overline{1,m}, \ l = 1,L, \ j \neq l, \tag{1.10}$$

где U - символ достоверного события.

В (1.8) - (1.10) $K^{\partial np}$, $K^{\partial onm}$ - соответственно области допустимых значений показателя качества пригодной и оптимальной СЗИ.

Такой подход позволяет логично и последовательно построить пригодную, оптимальную или даже превосходную по качеству СЗИ.

Однако, этот этап не может считаться окончательным, так как не учитывает расход ресурсов на обеспечение защищенности информации. Окончательное решение этой задачи получено на основе теории эффективности целенаправленных процессов, учитывающей ее праксеологический аспект, т.е. синтез «целевого» и «ресурсного» аспектов [68].

При этом в качестве показателя эффективности применения СЗИ по *i*-му свойству может быть принят одномерный показатель вида [52,72]:

$$w(u) = P(w_i^j \geq w_i^T, r_i^j \leq r_i^{\partial}), \tag{1.11}$$

где w_i^j - показатель целевого эффекта *j*-ого СЗИ по *i*-му свойству;

r_i^j - показатель затрат ресурсов в *j*-ом СЗИ для достижения целевого эффекта по свойству *i*;

w_i^T , r_i^∂ - соответственно требуемое и допустимое значение показателей целевого и ресурсного эффектов.

Тогда с учетом (1.6) и (1.7) для оценки эффективности применения СЗИ по всем каналам утечки (воздействия) можно использовать комплексный (векторный) показатель эффективности

$$W(J) = \langle w_1(j), w_2(j), ..., w_n(j) \rangle \qquad (1.12)$$

В такой интерпретации общая задача синтеза систем защиты информации может быть поставлена следующим образом:

найти такое подмножество вариантов внутренних параметров СЗИ $\{X\} \subset \{X^\partial\}$ - структуры системы, алгоритмов, методов и средств защиты, при котором выходные параметры ИТС – $\{Y\}$ удовлетворяли бы заданным системой управления требованиям по качеству доставки информации и при этом расходуемые ресурсы не превышали бы допустимого уровня, т.е. найти

$$\{X\} \subset \{X^\partial\} \Rightarrow Y_0 \geq\leq Y^T \Rightarrow W(k) \geq W^T, \qquad (1.13)$$

при ограничениях $\{R\} \leq \{R^\partial\}$ и $\{T\} \leq \{T^\partial\}$.

По своему характеру задача исследования является оптимизационной и состоит в нахождении (выборе) такого набора значений внутренних параметров СЗИ, который бы обеспечил экстремум функционала полезности, задающего математическую модель функционирования СЗИ с ограничениями на качество, ресурсы, время и количество допустимых вариантов построения системы в условиях реализации некоторой модели воздействия:

$$Y = F\{X, \hat{T}, \hat{M}\} \qquad (1.14)$$

где $\hat{M}$ - модель воздействия.

Вместе с тем, на основе анализа ряда научных работ [74,86,88,121,122,125,127] можно утверждать, что для решения некоторых достаточно важных частных задач по синтезу качественной СЗИ можно воспользоваться обобщенным свойством СЗИ – недоступностью, характеризующим защиту от несанкционированного доступа (НСД) и, соответственно, показате-

лем этого свойства - вероятностью защиты от НСД (вероятностью непреодоления СЗИ - $P_{нп}$) или вероятностью ее преодоления $P_п$. (что-либо сделать с информацией можно только получив доступ к ней). Для решения же задач оценки эффективности функционирования СЗИ в целевой эффект необходимо ввести ограничение по времени и тогда одномерный показатель эффективности СЗИ может быть представлен в виде главного показателя:

$$P_{нп} = P_{нп}\left(t \le t^{\partial}\right), \tag{1.15}$$

а показатели расхода других видов ресурсов (например, стоимостные) вынести в ограничительную часть постановки задачи исследования.

С учетом важности хранимой и обрабатываемой информации – *C* показатель эффективности СЗИ может быть представлен как ущерб - *w*, наносимый массиву информации при получении к нему несанкционированного доступа, что в общем виде может быть представлено следующим образом:

$$w_i = C_i \cdot P_{П_i}, \tag{1.16}$$

где $P_{П_i} = \left(1 - P_{нп\,i}\right)$ - вероятность преодоления СЗИ i – го массива, а суммарный вероятный ущерб, наносимый всем хранящимся на объекте массивам, как

$$W = \sum_{j=1}^{M} w_j . \tag{1.17}$$

Формализация задачи исследования

Для формализации постановки задачи исследования воспользуемся рекомендациями, приведенными в [20,21,62].

Пусть защита объекта $A_i \in A$, $i = \overline{1,n}$ определяется выбором совокупности M_j средств и методов защиты информации (в дальнейшем механизмов) $j = \overline{1,K}$, характеризующихся подуровнями защиты L_j. Вторая характеристика обеспечения защиты информации на объекте – $C_{\Sigma}(M)$ – суммарная стоимость реализа-

ции выбранных механизмов, которая не должна превышать базовой стоимости C_u информации на объекте. При этом уровень защищенности информации на объекте *Y(M)*, обеспечиваемый выбранной совокупностью механизмов защиты M_i, не должен быть меньше допустимого $Y^Д$.

Взлом (нарушение) системы защиты объекта характеризуется вероятностью взлома каждого механизма защиты $P(M_i)$ и всей совокупности механизмов в целом $P_Σ(M_i)$, суммарной стоимостью взлома всех механизмов $C_{BΣ}$, а также суммарными временными затратами $T_{BΣ}$, необходимыми для преодоления всех механизмов защиты, используемых для защиты информации на объекте A_i. При этом суммарная стоимость взлома всех механизмов должна быть больше допустимой $C_{ДΣ}$. Событие взлома *j*-го механизма определяет величину потерь (ущерба) w_i для *i*–го объекта. Суммарная величина ущерба $W_Σ$ при взломе всех средств системы не должна превышать стоимости (важности) всей информации, хранимой на объекте. Эффективность системы защиты существенно зависит от стоимости выбранных методов и средств защиты. Естественно предположить, что чем меньше стоимость реализации системы защиты (при равенстве всех других качественных показателей), тем выше ее эффективность.

Для определения задач защиты информации рассмотрим множество элементов $\{M_1(w_i), M_2(w_i), ..., M_r(w_i)\}$, где

$$M_r(w_i) \cup m_i(w_j) \subseteq M(w_j),\ j = \overline{1,r},\ r = \overline{1,\sigma}. \qquad (1.18)$$

Здесь {*i*,*r*} – подмножество механизмов защиты объекта, составляющих объединение методов и средств, используемых для защиты объекта A_i и обеспечивающих требуемый уровень его защиты

$$Y(w_i): Y_r \subseteq Y^T \forall r \qquad (1.20)$$

Таким образом, каждый элемент $M_r(w_i)$, $r = \overline{1,\sigma}$ представляет собой объединение такого подмножества механизмов защиты объекта, практическая реализация которых обеспечивает требуемый уровень защиты информации на объекте A_i.

В такой постановке задача по созданию системы защиты информации, хранимой и обрабатываемой на объекте A_i, $(i=\overline{1,n})$, предполагает оптимизацию по всем элементам

$$M_r(w_i) \subseteq M(w_i),\ r=\overline{1,\sigma} \tag{1.21}$$

и может формализована в следующих вариантах:

1. Минимизировать стоимость обеспечения защиты объекта A_i, $(i=\overline{1,n})$, т.е.

$$C_\Sigma(M)=\sum_{j=1}^{K} C_j(w_i)X_j(w_i) \to \min, \tag{1.22}$$

при ограничениях:

$$\begin{cases} \sum\limits_{j=1}^{K} X_j(w_i) \le K \\ \sum\limits_{j=1}^{K} I_j = C_j(w_i)X_j(w_i) \ge Y_0(w_i), \\ \sum\limits_{j=1}^{K} C_j(w_i)X_j(w_i) \le C_0(w_i) \end{cases} \tag{1.23}$$

где X_j может принимать значения 0 или 1.

2. Максимизировать эффективность системы защиты информации на объекте A

$$Y\left(M(A_i)\right)=Y\left\{P_\Sigma\left(M(A_i)\right),C_\Sigma\left(M(A_i)\right),T_\Sigma\left(M(A_i)\right)\right\} \to \max \tag{1.24}$$

при ограничениях (1.23), где $P_\Sigma\left(M(A_i)\right),C_\Sigma\left(M(A_i)\right),T_\Sigma\left(M(A_i)\right)$ – соответственно суммарные: целевая, стоимостная и временная компоненты показателя эффективности защиты информации на объекте A по всем выбранным механизмам защиты. При этом целевая компонента может быть найдена исходя из следующих соображений:

необходимо минимизировать вероятность взлома всех механизмов, используемых для защиты информации на объекте A, т.е.

$$P(w_i)=1-\prod_{j=1}^{r}\left(1-P_j(w_i)\right)X_j(w_i) \to \min, \tag{1.25}$$

при ограничениях (1.23).

3. Максимизировать стоимость взлома всех механизмов защиты информации, использованных на объекте A_i:

$$C_{B\Sigma} = \sum_{j=1}^{K} C_j(w_i) P_j(w_i) X_j(w_i) \to \max, \qquad (1.26)$$

при ограничениях (1.23), а также

$$\sum_{j=1}^{K} t_j(w_i) P_j(w_j) X_j(w_i) \geq T_0(w_i) \qquad (1.27)$$

$$\sum_{j=1}^{K} C_j(w_i) P_j(w_i) X_j(w_i) \leq C_0(w_i) \qquad (1.28)$$

4. Минимизировать величину ущерба, нанесенного информации в результате взлома всех механизмов защиты объекта Ai:

$$W(w_i) = \sum_{i=1}^{M} C_i \cdot P_{\Pi i} \to \min \qquad (1.29)$$

при ограничениях на стоимость защиты системы объекта, и время, затрачиваемое нарушителем:

$$\begin{cases} C_{\Sigma}(M) = \sum_{i=1}^{K} C_i \leq C_u \\ T_{B\Sigma} = \tau_n \cdot \sum_{i=1}^{M} n_i \leq T_{don} \\ \sum_{i=1}^{M} a_i \leq K \end{cases} \qquad (1.30)$$

Решение задачи в последней постановке выглядит наиболее актуальным, поэтому в дальнейшим будем опираться именно на него.

Выбор совокупности механизмов защиты $m_j \in M$ должен производиться с учетом установления всех возможных каналов и моделей воздействия для каждого конкретного объекта A_i, поэтому в первую очередь необходимо решить задачу разработки адекватных моделей воздействия противника (злоумышленника), а затем уже решать задачи оценки наносимого ущерба, а также способов и средств его снижения (повышения защищенности информации).

ВЫВОДЫ ПО РАЗДЕЛУ

Специфика функционирования ИТС определяется повышенными требованиями к качеству информации, выдаваемой в систему принятия управленческих решений. При этом, как показывает анализ, проведенный в ряде научных работ, степень обеспечения внешнего качества (защищенности) информации в ИТС обуславливается в основном тем, как построена и функционирует СЗИ, как подсистема ИТС. Анализ существа и содержания проблемы защиты информации в ИТС на базе VPN позволил сделать следующие выводы.

1. В настоящий момент для построения VPN используется ряд протоколов, включая IPSec, PPTP, L2TP и т.д. Эти протоколы не шифруют данные, они лишь определяют, как используются алгоритмы шифрования и ряд других условий, необходимых для построения VPN (включая контроль целостности, аутентификацию абонентов и т.д.).

2. Достаточно часто VPN реализуется на базе уже существующего сетевого оборудования, как правило, маршрутизаторов или программно-аппаратных межсетевых экранов. Также существуют и специализированные устройства построения VPN. А раз это обычное устройство, поддерживающее стек TCP/IP, то на него могут быть реализованы атаки, которые могут нарушить как функционирование самого устройства, так и временно взаимодействие защищаемых с их помощью сетей и узлов.

3. Нередко VPN реализуется чисто программными средствами, а программное обеспечение VPN является надстройкой над операционной системой, что нередко и используется злоумышленниками. Поэтому независимо от надежности и защищенности программного обеспечения VPN уязвимости операционной системы могут свести на нет все защитные механизмы VPN.

4. Защищенность информации в ИТС является комплексным свойством и включает по разным источникам от 3-х до 14 частных свойств. Однако, с точки зрения ИТС можно выделить три основных атрибутивных свойства: достовер-

ность, сохранность и конфиденциальность и на них сосредоточить внимание разработчиков СЗИ для ИТС.

5. По ряду степень уязвимости перерабатываемой в ИОС ИТС содержательной информации непрерывно возрастает, что требует постоянного внимания к задачам совершенствования СЗИ. Вместе с тем доказано, что ни один из способов защиты информации, методов, мер, средств и мероприятий не является абсолютно надежным, а максимальный эффект достигается при объединении их всех в единую комплексную СЗИ ИОС ИТС. При этом такая комплексность должна быть: концептуальной, целевой и временной.

6. По совокупности характерных признаков СЗИ ИОС, как подсистема сложной ИТС, сама является сложной системой, и для ее исследования должен использоваться системный подход с его основным инструментом – системным анализом в совокупности с такими важными методами, присущими системному подходу, как метод декомпозиции и метод маргинального подхода. При этом в качестве основной процедуры создания качественной и эффективно используемой СЗИ ИОС ИТС может применяться итерационная процедура, алгоритм которой представлен на рисунке 1.2.

7. Оценка эффективности функционирования СЗИ ИОС ИТС должна включать не только оценку обеспечения физической, логической целостности и несанкционированной модификации, но и оценку предупреждения несанкционированного получения и распределения информации. Поэтому в качестве показателя эффективности функционирования СЗИ ИОС ИТС может быть выбран комплексный показатель вида (1.12), компоненты которого отражают целевую, стоимостную и временную составляющие данного процесса. При этом, для решения конкретных частных задач, рассмотренных в данной работе в качестве показателей защищенности информации выбраны: вероятность взлома i-го средства защиты $P_{пi}$, вероятность взлома всех средств системы защиты – P_{Σ}, среднее время взлома i–го средства защиты – $T_{пi}$, среднее время взлома всех средств СЗИ – T_{Σ}.

Учитывая явно выраженную взаимосвязь целевой и временной составляющих, в работе используется главный показатель – вероятность взлома *i*–го средства защиты за время, не превышающее заданное – $T_з$ – $P_i\,(T \le T_з)$ и, соответственно, - $P_\Sigma(T_\Sigma \le T_з)$. Там, где речь идет об обеспечении защиты информации, хранящейся в нескольких массивах одного ИОС ИТС в качестве показателя используется вероятный ущерб – w_i, наносимый информации, хранящейся в одном массиве, и соответственно, суммарный вероятный ущерб – W_Σ.

8. В зависимости от конкретных условий задачи исследования, формальная постановка задачи может быть выполнена как на достижение минимума вероятности (1.22), максимума стоимости (1.24), так и минимума величины потерь (ущерба) от взлома всех механизмов защиты, используемых в СЗИ (1.29). Критерий выбора СЗИ представлен в виде (1.8).

9. Общая оценка эффективности, созданной или модернизируемой СЗИ ИОС ИТС определяется функционалом полезности (1.5). Записать такой функционал для конкретной СЗИ в настоящее время не представляется возможным, поэтому целесообразно решать общую задачу синтеза СЗИ путем декомпозиции ее на ряд относительно самостоятельных, но взаимосвязанных задач.

10. Важнейшей составной частью функционала (1.5) является неопределенность воздействия нарушителя – М, поэтому в первую очередь необходимо выбрать (разработать) модели воздействия, наиболее адекватно описывающие процесс взаимодействия нарушителя с элементами системы защиты информации ИОС ИТС, и производить дальнейший анализ СЗИ в предположении, что нарушитель стремится нанести информации максимально возможный (с его точки зрения) ущерб, имея априори информацию о СЗИ.

2 РАЗРАБОТКА МОДЕЛЕЙ ВОЗДЕЙСТВИЯ НАРУШИТЕЛЯ

2.1 Анализ известных моделей воздействия

Моделирование является одним из самых мощных средств, как научного познания, так и решения практических задач. Базовым понятием при формировании целей моделирования является модель. Любая модель характеризуется переменными, параметрами и ограничениями (элементами модели). Задать (разработать) любую модель это значит определить пространство (совокупность, множество) параметров, переменных и ограничений с определенными на этом пространстве целями.

Как показано в [21] в группе задач, подлежащих исследованию, исходная информация имеет множественные условия (известна лишь область изменения переменных и неопределенных параметров), последствия принимаемых решений определить точно не представляется возможным, т.е. принятие решения осуществляется в условиях не только неопределенности, но и конфликтности.

В настоящее время, несмотря на большое количество проведенных исследований у нас в стране и особенно за рубежом, единая и общепринятая модель воздействия нарушителя (злоумышленника) на информационные массивы, хранящиеся и обрабатываемые в ИОС ИТС еще не создана [33]. Вместе с тем, совместными усилиями разработан подход к решению этой проблемы, суть которого состоит в создании общей теории защиты (сохранении) какого-либо предмета от несанкционированного доступа (уничтожения, искажения, похищения, размножения) и приложение ее к ИТС с учетом особенностей информации как предмета защиты и самих информационных объектов сети, как объектов ее использования.

Рисунок 2.1 – Классификация моделей защиты информации

В рамках данного подхода разработан, опубликован и используется ряд моделей воздействия. В [98, 110] проведен анализ известных моделей. Вариант их классификации, не претендующий на абсолютную полноту, приведен на рисунке 2.1. Как следует из анализа, одноуровневые и многоуровневые матричные модели являются в большей мере теоретическими и практического применения в оценке СЗИ ИОС ИТС найти не могут, статистические модели также без существенных доработок для целей создания и анализа СЗИ ИТС не применимы. Наиболее близкими по сущности к моделям, разработанным в данной работе, являются логико-вероятностные модели, описанные в [46].

2.1.1 Простая вероятностная модель

Графическое представление такой модели показано на рисунке 2.2.

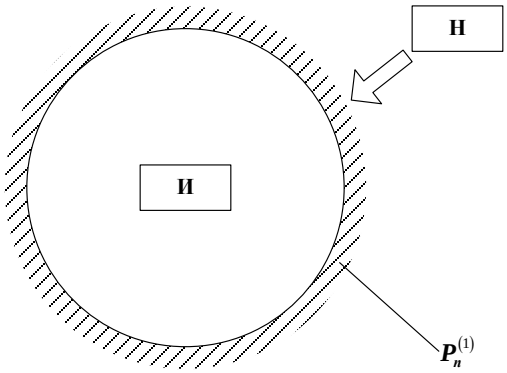


Рисунок 2.2 – Простая вероятностная модель

Используемые ограничения и допущения:

1) нарушитель пытается завладеть информацией, хранящейся за некоторой преградой (защитой), совершая ограниченное k число независимых попыток воздействия;

2) преграда (защита) единственная, замкнутая (круговая), однородная и действует постоянно;

3) система защиты после каждой попытки успевает полностью восстановиться.

В качестве параметров модели выступают: вероятность преодоления защиты с одной попытки - $P_n^{(1)}$ и число попыток k. В качестве переменной - вероятность ее непреодоления $P_{нп}$.

Тогда в соответствии с логико-вероятностным подходом

$$P_{нп}^{(1)} = 1 - P_n^{(1)}, \qquad (2.1)$$

а вероятность непреодоления системы защиты с k попыток

$$P_n^{(k)} = 1 - \left(1 - P_n^{(1)}\right)^k; \; P_{нп}^{(k)} = 1 - P_n^{(k)} = \left(P_{нп}^{(1)}\right)^k \qquad (2.2)$$

Таким образом, совершая требуемое число попыток k^{Tp}, нарушитель может добиться заданной цели даже при высоком уровне защищенности информации.

Пусть требуется вскрыть систему защиты с вероятностью $P_n \geq P_n^{Tp}$. Тогда:

$$1 - P_n^{Tp} = \left(1 - P_n^{(1)}\right)^{k^{\text{Тр}}},$$

$$\ln\left(1 - P_n^{\text{Тр}}\right) = k^{\text{Тр}} \ln\left(1 - P_{\text{п}}^{(1)}\right) \qquad (2.3)$$

$$k^{\text{Тр}} = \frac{\ln\left(1 - P_n^{\text{Тр}}\right)}{\ln\left(1 - P_n^{(1)}\right)}$$

В свою очередь хранитель информации для повышения уровня защищенности может создать несколько эшелонов защиты, что отражается другой моделью.

2.1.2 Простая эшелонированная модель

Графическое представление простой эшелонированной модели защиты информации представлено на рисунке 2.3.

Используемые ограничения и допущения:

1) нарушитель пытается завладеть информацией, хранящейся за *m* эшелонами защиты, совершая ограниченное *k* число независимых попыток воздействия;

2) все эшелоны защиты однородны, круговые и действуют постоянно;

3) вскрытый эшелон защиты не восстанавливается.

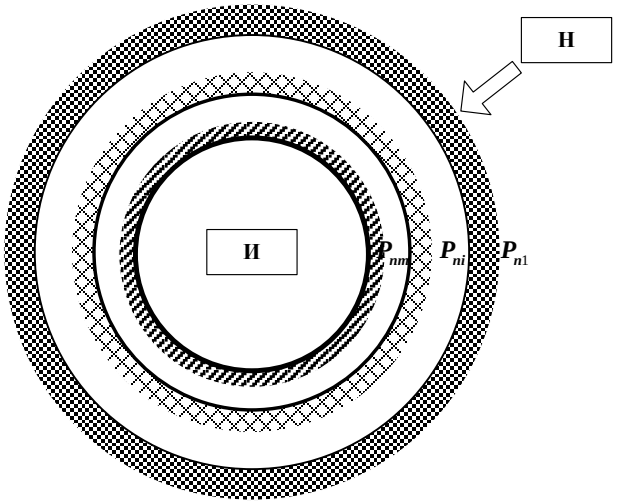


Рисунок 2.3. – Простая эшелонированная модель воздействия нарушителя

В качестве параметров модели выступают:

вероятность преодоления *i*-го эшелона защиты с одной попытки - $P_{ni}^{(1)}$;

число эшелонов защиты - *m*;

число попыток воздействия - *k*.

В качестве переменной - вероятность непреодоления системы защиты $P_{нп_m}^{(k)}$ с *k* попыток.

Тогда, если все эшелоны защиты однородны (имеют одинаковую вероятность преодоления - P_{ni}), а число попыток воздействия равно *k*, то

$$P_{нп_m}^{(k)} = \left(1 - \left(P_{ni}^{(1)}\right)^m\right)^k \qquad (2.4)$$

Отсюда нетрудно решить и обратную задачу. Сколько необходимо иметь эшелонов защиты, чтобы добиться требуемого уровня защищенности инфор-

мации при использовании такой модели? Для этого необходимо лишь проделать следующую последовательность действий:

$$1.\ P_{нп_m}^{(k)} = \left(1 - \left(P_n^{(1)}\right)^m\right)^k,$$

$$2.\ 1 - \left(P_n^{(1)}\right)^m = \sqrt[k]{P_{нп_m}^{(k)}} \qquad (2.5)$$

$$3.\ \left(P_n^{(1)}\right)^m = 1 - \sqrt[k]{P_{нп_m}^{(k)}},$$

$$4.\ m \ln P_n^{(1)} = \ln\left(1 - \sqrt[k]{P_{нп_m}^{(k)}}\right),$$

$$5.\ ]m[= \frac{\ln\left(1 - \sqrt[k]{P_{нп_m}^{(k)}}\right)}{\ln P_n^{(1)}},$$

Знак $]*[$ означает операцию округления в сторону увеличения.

Если эшелоны защиты неоднородны ($P_{n1} \neq P_{n2} \neq ... \neq P_{ni} \neq P_{nm}$), то выражение (2.4) примет вид

$$P_{нп_m}^{(k)} = \left(1 - \left(\prod_{i=1}^{m} P_i\right)\right)^k. \qquad (2.6)$$

Известен [110] и другой подход к созданию моделей воздействия нарушителя на систему преград. Он основывается на свойстве «старения» информации. Следствием этой причины является необходимость решения задачи определения времени $t_н$, после которого информация теряет ценность для тех, кто пытается ее получить.

Решение этой задачи не является сложным, если известны зависимости изменения во времени «стоимости» хранения и «стоимости» получения информации от времени. Так, если «стоимость» хранения информации во времени изменяется по линейному закону $C_u(t) = k_{1t} + b$, а стоимость преодоления системы защиты - по пропорциональной зависимости $C_n(t) = k_{2t}$, найти время $t_н$, после которого взлом защиты становится нецелесообразным, можно как аналитическим, так и графическим путем.

Пусть $k_1 = -0,5; b = 10; k_2 = 2$. Тогда: $C_u(t) = C_n(t)$; $k_{1t} + b = k_{2t}$;

$$k_{2t} - k_{1t} = b;\ t_н = \frac{b}{k_2 - k_1};\ t_н = \frac{10}{2 + 0,5} = 4\,[\text{ед. времени}] \qquad (2.7)$$

Вместе с тем учет «старения» информации приводит к необходимости учета фактора времени и при выборе показателя оценки защищенности, который в данном случае становится главным показателем, т.к. в нем время выступает ограничивающим фактором - $P_{нп}\left(t \le t^{з}\right)$.

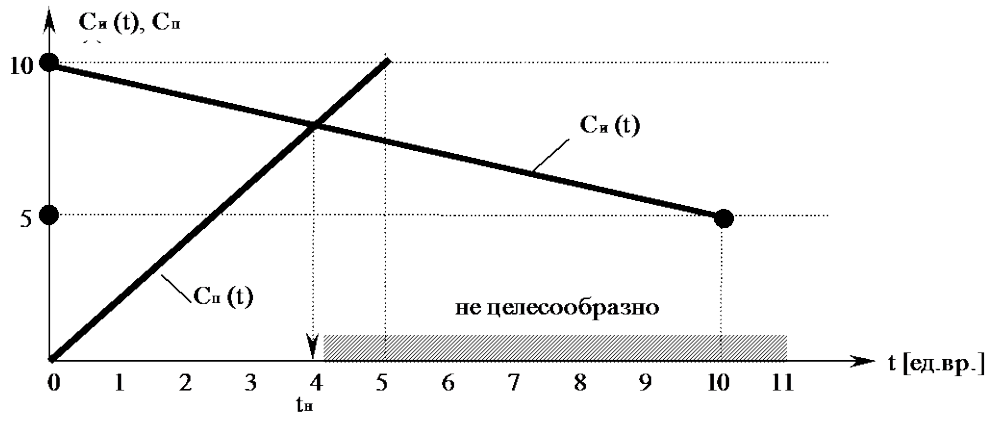


Рисунок 2.4 – Графическое решение задачи

2.1.3 Модель очаговой системы защиты

Ограничения, используемые в моделях 2.1.1 и 2.1.2 являются очень сильными, и в значительной мере не отражают реального построения систем защиты. В первую очередь это обусловлено особенностями распределенных ИТС как объектов использования информации. Одной из таких особенностей является значительные, разнесенные по территории того или иного региона размеры. Следствием этого является большая трудность, а в ряде случаев невозможность создания замкнутой круговой преграды вокруг всей ИТС (ее элементов), и необходимость перехода к очаговой системе преград, имеющей обходные пути (рисунок 2.5).

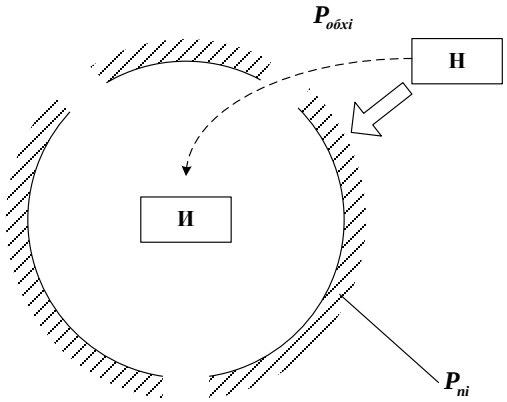


Рисунок 2.5 – Модель очаговой системы защиты

В [46] предлагается для оценки защищенности информации в такой модели использовать следующие выражения:

$P_{нп} = 1$, если $t_{ж} < t_{н}$ и $P_{обх} = 0$;

$$P_{нп} = \left(1 - P_{п}\left(t \le t_{ж}\right)\right); \qquad (2.8)$$

$$P_{нп} = \left(1 - P_{п}\left(t \le t_{ж}\right)\right)\left(1 - P_{обж}\right),$$

где $P_{п}\left(t \le t_{ж}\right) = 0$, если $t_{ж} < t_{н}$;

$P_{п}\left(t \le t_{ж}\right) > 0$, если $t_{ж} > t_{н}$;

$$P_{нп} = \min \begin{cases} 1 - P_{п}\left(t \le t_{ж}\right) \\ 1 - P_{обх} \end{cases},$$

где $t_{ж}$ - время «жизни» информации.

Если обходных путей несколько, то

$$P_{нп} = \min \begin{cases} 1 - P_{п}\left(t \le t_{ж}\right) \\ 1 - P_{обх1} \\ 1 - P_{обх2} \\ \ldots \\ 1 - P_{обхn} \end{cases},$$

где $P_{п}\left(t \le t_{ж}\right)$, например, для взлома системы защиты, основанной только на методе паролирования, рекомендуется находить по выражению [51]

$$P_{п}\left(t \le t_{ж}\right) = \frac{n}{A^{s}}, \qquad (2.9)$$

где n - количество попыток подбора пароля; A - число символов в выбранном алфавите; S - длина пароля.

Эту же задачу, на наш взгляд, можно решить и следующим способом:

1) вероятность преодоления системы преград с одной попытки

$$P_n^{(1)} = P_{пп} \cdot P_n^{(1)} + P_{нпп} - P_{пп} \cdot P_n^{(1)} \cdot P_{нпп}, \quad (2.10)$$

2) вероятность непреодоления с одной попытки

$$P_{нпр}^{(1)} = 1 - P_{пр}^{(1)}, \quad (2.11)$$

3) вероятность преодоления с k попыток

$$P_{пр}^{(k)} = 1 - \left(1 - P_{пр}^{(1)}\right)^k \quad (2.12)$$

4) вероятность непреодоления с k попыток

$$P_{нпр}^{(k)} = 1 - P_{пр}^{(1)} \quad (2.13)$$

где $P_{пр}\left(P_{нпр}\right)$ - соответственно вероятность попадания (непопадания) на очаговую преграду.

Пусть в ИТС установлено десять каналов утечки информации (n=10), четыре из них защищены однородными защитными механизмами (m=4) с вероятностью преодоления с одной попытки $P_n^{(1)} = 0,7$.

Необходимо найти вероятность непреодоления системы защиты с трех независимых попыток - $P_{нпр}^{(3)}$.

1. $P_{пп} = \frac{m}{n} = \frac{4}{10} = 0,4;\ P_{нпп} = 1 - P_{пп} = 0,6$

2. $P_n^{(1)} = P_{пп} \cdot P_n^{(1)} + P_{нпп} - P_{пп} \cdot P_n^{(1)} \cdot P_{нпп} = 0,4 \cdot 0,7 + 0,6 + 0,4 \cdot 0,7 \cdot 0,6 = 0,712$

3. $P_{пр}^{(3)} = 1 - \left(1 - P_{пр}^{(1)}\right)^3 = 1 - 0,288^3 = 0,976$

4. $P_{нпр}^{(3)} = 1 - P_{пр}^{(3)} = 1 - 0,976 = 0,024\,P_н$ (2.14)

Существенным недостатком всех рассмотренных моделей является то, что в них не учитываются следующие важные факторы, характерные практически для всех современных систем защиты:

злоумышленник может перейти к вскрытию очередного эшелона защиты только после того, как ему удалось преодолеть предыдущий;

с течением определенного заданного времени или по решению администратора, вскрытые эшелоны защиты могут восстанавливаться.

Для устранения этих недостатков в данной работе разработан ряд моделей, базирующихся на математический аппарат конечных марковских цепей, которые могут быть использованы на том или ином уровне исследования.

2.2 Разработка аналитической модели воздействия

2.2.1 Простая марковская модель защиты

При разработке модели использованы следующие ограничения:

1) средства защиты различных эшелонов не однородны, попытки преодоления одного и того же средства независимы;

2) преодоление очередного средства возможно только после преодоления предыдущего. Преодоленные средства защиты не восстанавливаются.

Из анализа физической сущности процесса преодоления такой системы преград можно сделать вывод о том, что данный процесс является вероятностным, имеет конечное число дискретных состояний (равное числу преград плюс единица), время преодоления каждой из преград является случайной величиной, в общем случае распределенной по неизвестному (не показательному) закону, т.е. процесс с классической точки зрения не является марковским.

В таких условиях нахождение вероятностно-временных характеристик преодоления системы преград требует привлечения математического аппарата общей теории СМО [39, 41]. Однако, для достижения поставленных в работе целей исследования без особого ущерба для полученных результатов, можно ввести следующие допущения:

1) все события в процессе преодоления преград совершаются в некоторые дискретные моменты времени, именуемые шагами;

2) на длительность шага ограничений не накладывается;

3) переход из одного состояния в другое возможен с определенной вероятностью;

4) вероятность перехода в состояние *j* на шаге *i* зависит только от того, в каком состоянии находится система на шаге (*i-1*) и не зависит от того, каким образом она пришла в это состояние.

В таких предположениях можно исследуемый немарковсий процесс достаточно адекватно заменить вложенной в него конечной марковской цепью, для которой свойство марковости соблюдается только в моменты осуществления переходов из одного состояния в другое [41].

Данный процесс может быть отображен графом состояний и переходов, изображенным на рисунке 2.6.

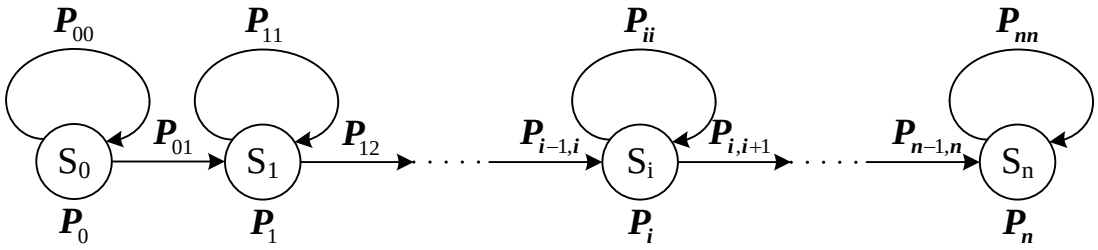


Рисунок 2.6. – Граф состояний и переходов

Состояния, указанные на графе, имеют следующее содержание:

S_0 - нарушитель осуществляет попытку преодоления внешней преграды;

S_1 - нарушитель преодолел внешнюю преграду и осуществляет попытку преодоления второй (с внешней стороны) преграды;

S_i - нарушитель преодолел *i* - ую (с внешней стороны) преграду и осуществляет попытку преодоления (*i+1*)-ой преграды;

S_n - нарушитель преодолел последнюю (внутреннюю) преграду. Это событие является поглощающим.

В качестве вероятностей перехода в графе, изображенном на рис.2.6, выступают вероятности преодоления (непреодоления) той или иной преграды (средства защиты).

Матрица переходных вероятностей для такого процесса примет вид:

$$P_{[n+1,n+1]} = \begin{vmatrix} P_{00} & P_{01} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & P_{11} & P_{12} & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & P_{22} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & P_{ii} & P_{ii+1} & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & P_{i+1i+1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{vmatrix} \qquad (2.15)$$

Основываясь на [41], вероятность преодоления системы защиты за k попыток будет определяться по уравнению Колмогорова - Чепмена

$$P^{(k)}_{\langle n+1\rangle} = P^{(0)}_{\langle n+1\rangle} \cdot P^{k}_{[n+1,n+1]} = P^{(k-1)}_{\langle n+1\rangle} \cdot P_{[n+1,n+1]}, \qquad (2.16)$$

где в качестве вектора исходного состояния принят вектор

$$P^{(0)}_{\langle n+1\rangle} = \langle 1 \quad 0 \quad 0 \quad 0 \quad \dots \quad 0 \rangle \qquad (2.17)$$

Пусть модель системы защиты имеет вид, представленный на рисунке 2.7.

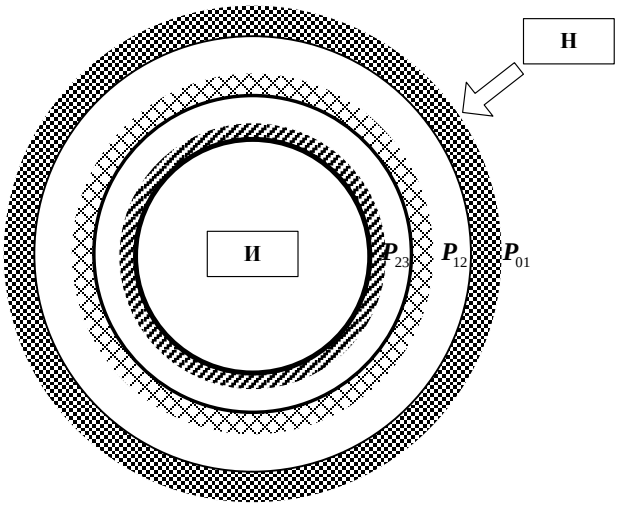


Рисунок 2.7 – Модель системы защиты

Для такой модели системы защиты граф состояний и переходов примет вид, изображенный на рисунке 2.8:

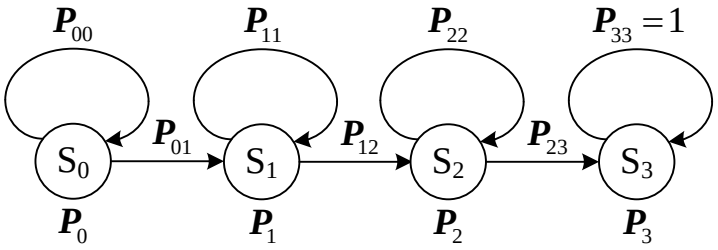


Рисунок 2.8 – Граф состояний и переходов

В общем виде матрица переходных вероятностей будет иметь вид:

$$P_{[4,4]} = \begin{vmatrix} P_{00} & P_{01} & 0 & 0 \\ 0 & P_{11} & P_{12} & 0 \\ 0 & 0 & P_{22} & P_{23} \\ 0 & 0 & 0 & 1 \end{vmatrix} \qquad (2.18)$$

Рассчитаем по (2.16) вероятность взлома системы защиты за *k=3* попытки.

Пусть $P_{01} = 0,7$; $P_{12} = 0,6$; $P_{23} = 0,3$. При таких исходных данных получим матрицу

$$P_{[4,4]} = \begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0 & 0,4 & 0,6 & 0 \\ 0 & 0 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

и вектор исходного состояния $P^{(0)}_{\langle 4 \rangle} = \langle 1 \quad 0 \quad 0 \quad 0 \rangle$.

Тогда

$$P^{(1)}_{\langle 4 \rangle} = P^{(0)}_{\langle 4 \rangle} \cdot P_{[4,4]} = \langle 1 \quad 0 \quad 0 \quad 0 \rangle \times \begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0 & 0,4 & 0,6 & 0 \\ 0 & 0 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix} = \langle 0,3 \quad 0,7 \quad 0 \quad 0 \rangle$$

$$P^{(2)}_{\langle 4 \rangle} = P^{(1)}_{\langle 4 \rangle} \cdot P_{[4,4]} = \langle 0,3 \quad 0,7 \quad 0 \quad 0 \rangle \times \begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0 & 0,4 & 0,6 & 0 \\ 0 & 0 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix} = \langle 0,09 \quad 0,49 \quad 0,42 \quad 0 \rangle$$

$$P^{(3)}_{\langle 4\rangle} = P^{(2)}_{\langle 4\rangle} \cdot P_{[4,4]} = \langle 0,09 \quad 0,49 \quad 0,42 \quad 0 \rangle \times \begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0 & 0,4 & 0,6 & 0 \\ 0 & 0 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix} =$$

$$= \langle 0,027 \quad 0,259 \quad 0,588 \quad 0,126 \rangle$$

Таким образом, после трех попыток взлома вероятность преодоления системы защиты $P^{(3)}_n = 0,126$.

Второй важной особенностью систем защиты информации в современных ИТС является возможность восстановления вскрытых средств защиты либо по времени, либо по действиям администратора. Например, по истечении некоторого наперед заданного интервала времени, меняется имя пользователя, изменяется пароль доступа и т.д. С учетом этого разработан следующий вариант модели.

2.2.2 Марковская модель с восстановлением

Процесс вскрытия системы защиты информации в этой модели отличается от предыдущего тем, что нарушитель, при попытке вскрытия очередного средства защиты обнаруживает, что предыдущие эшелоны (эшелон) восстановлены и ему необходимо приступать к взлому защиты, начиная с первого эшелона. Учитывая тот факт, что вероятности вскрытия средства защиты незначительны (например, нарушитель знает один из миллиона возможных значений пароля), можно считать события воздействий независимыми. Тогда, граф состояний и переходов такого процесса примет вид, изображенный на рисунке 2.9.

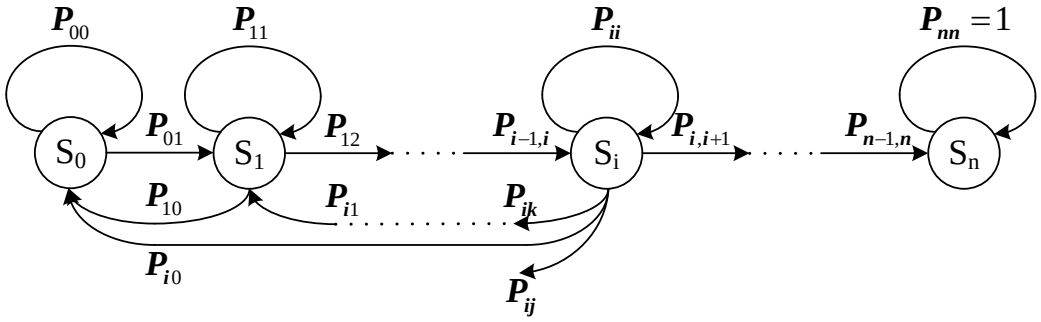


Рисунок 2.9 – Граф состояний и переходов

Дальнейшие расчеты проводятся аналогично тем, что приведены для модели 2.2.1.

Рассчитаем вероятность взлома системы защиты для модели, представленной на рисунке 2.7, значениях вероятностей $P_{01}=0,7$; $P_{12}=0,6$; $P_{23}=0,3$; $P_{10}=0,1$; $P_{11}=0,3$; $P_{20}=P_{21}=0,1$; $P_{22}=0,5$ и при числе попыток взлома $k = 3$.

Изобразим граф состояний и переходов (рисунок 2.10):

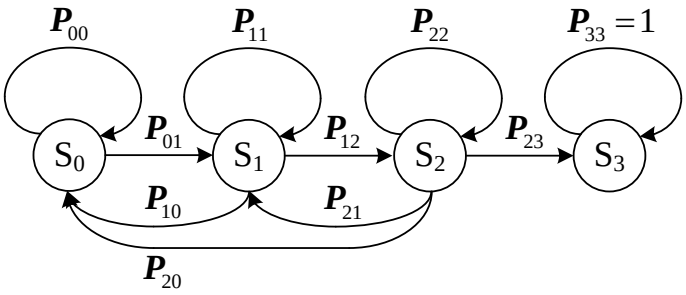


Рисунок 2.10 – Граф состояний и переходов

В дальнейшем методика оценивания вероятности взлома системы защиты останется аналогичной той, что, использована в пункте 2.2.1.

$$P_{[4,4]}=\begin{vmatrix} P_{00} & P_{01} & 0 & 0 \\ P_{10} & P_{11} & P_{12} & 0 \\ P_{20} & P_{21} & P_{22} & P_{23} \\ 0 & 0 & 0 & 1 \end{vmatrix}=\begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0,1 & 0,4 & 0,6 & 0 \\ 0,1 & 0,1 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix}$$

$$P^{(0)}_{\langle 4\rangle}=\langle 1 \quad 0 \quad 0 \quad 0\rangle.$$

$$P^{(1)}_{\langle 4\rangle}=P^{(0)}_{\langle 4\rangle}\cdot P_{[4,4]}=\langle 1 \quad 0 \quad 0 \quad 0\rangle\times\begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0,1 & 0,4 & 0,6 & 0 \\ 0,1 & 0,1 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix}=\langle 0,3 \quad 0,7 \quad 0 \quad 0\rangle$$

$$P^{(2)}_{\langle 4\rangle} = P^{(1)}_{\langle 4\rangle} \cdot P_{[4,4]} = \langle 0,3 \quad 0,7 \quad 0 \quad 0\rangle \times \begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0,1 & 0,4 & 0,6 & 0 \\ 0,1 & 0,1 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix} = \langle 0,16 \quad 0,42 \quad 0,42 \quad 0\rangle$$

$$P^{(3)}_{\langle 4\rangle} = P^{(2)}_{\langle 4\rangle} \cdot P_{[4,4]} = \langle 0,16 \quad 0,42 \quad 0,42 \quad 0\rangle \times \begin{vmatrix} 0,3 & 0,7 & 0 & 0 \\ 0,1 & 0,4 & 0,6 & 0 \\ 0,1 & 0,1 & 0,7 & 0,3 \\ 0 & 0 & 0 & 1 \end{vmatrix} =$$

$$= \langle 0,132 \quad 0,28 \quad 0,462 \quad 0,126\rangle$$

Таким образом, после k=3 попыток воздействия, система защиты (рисунок 2.7) при исходных данных (2.19) будет преодолена с вероятностью $P^{(3)}_n = 0,126$.

2.2.3 Марковская модель очаговой системы защиты

Для распределенных ИТС, где невозможно построить круговую систему защиты (полностью перекрыть все возможные каналы воздействия), разработана марковская модель очаговой системы защиты в нескольких модификациях.

Для разработки марковской модели воздействия нарушителя на систему защиты, состоящую из системы очаговых преград, воспользуемся методом индукции.

Вариант 1. Система защиты информации имеет вид, изображенный на рисунке 2.11.

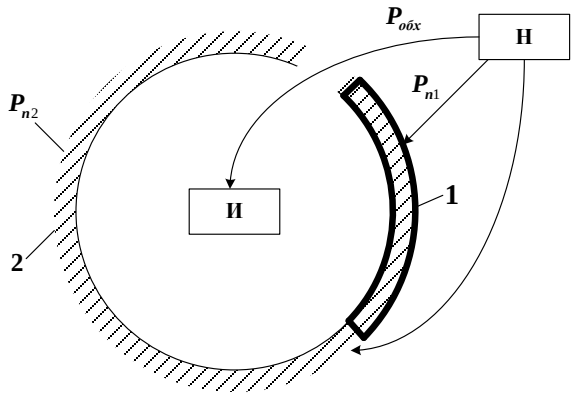


Рисунок 2.11 – Модель очаговой системы защиты

Исходные данные, ограничения и допущения:

1) система защиты имеет три канала воздействия;

2) два канала защищены неоднородными средствами защиты с вероятностями преодоления с одной попытки - P_{n1} и P_{n2} ;

3) вероятности попадания на каналы защиты в одной попытке воздействия соответственно равны - $P_{пп1}$ и $P_{пп2}$, вероятность попадания в данной попытке на незащищенный канал $P_{обх}$;

4) при попадании на незащищенный канал нарушитель преодолевает систему защиты с вероятностью, равной 1;

5) попытки воздействия являются независимыми, преодоленные средства защиты не восстанавливаются.

Формализуем возможные состояния системы при воздействии нарушителя:

S_0 - нарушитель совершает попытку преодоления системы защиты;

S_1 - нарушитель при совершении попытки преодоления системы защиты попал на защищенный канал 1;

S_2 - нарушитель при совершении попытки преодоления системы защиты попал на защищенный канал 2;

S_3 - нарушитель преодолел систему защиты.

Граф и матрица состояний и переходов для такой системы примут вид:

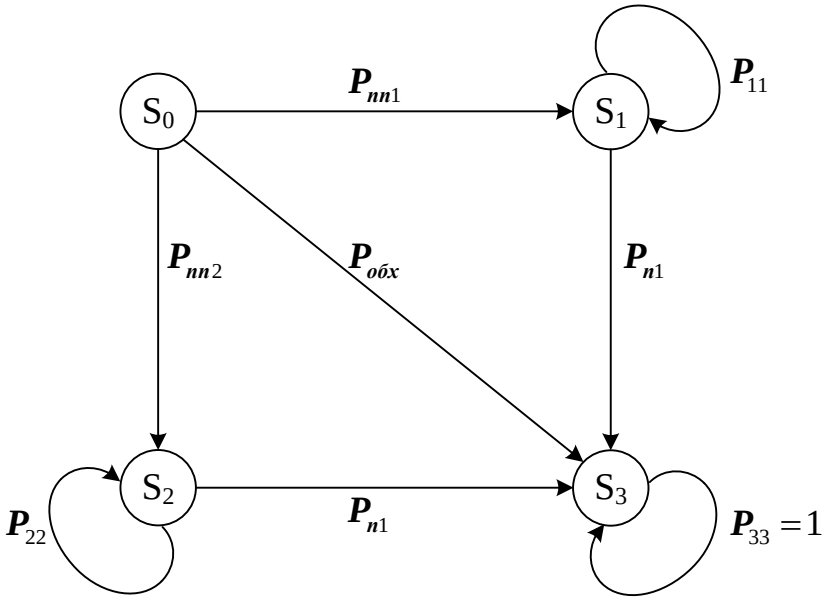


Рисунок 2.12 – Граф состояний и переходов

$$P_{[4,4]} = \begin{vmatrix} 0 & P_{пп1} & P_{пп2} & P_{обх} \\ 0 & (1-P_{п1}) & 0 & P_{п1} \\ 0 & 0 & (1-P_{п2}) & P_{п2} \\ 0 & 0 & 0 & 1 \end{vmatrix} \qquad (2.20)$$

Вариант 2. Граф и матрица состояний и переходов для модели системы защиты представленной на рисунке 2.13 будут иметь аналогичный вид, за исключением того, что элемент матрицы P_{03} вычисляется как сумма вероятностей $P_{03} = P_{обх} = P_{обх1} + P_{обх2}$. Такая запись всегда будет математически корректна, т.к. матрица состояний и переходов является стохастической.

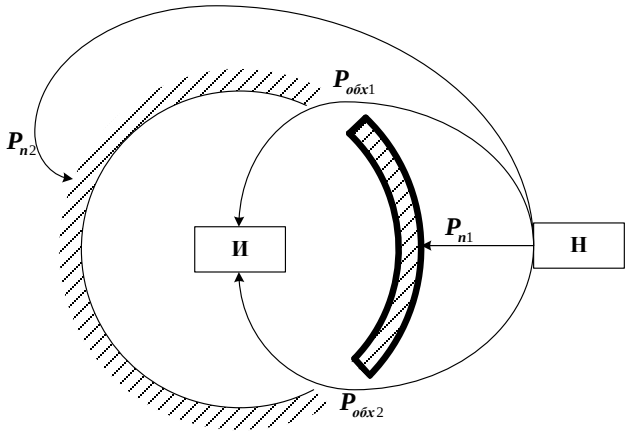


Рисунок 2.13 –- Модель системы защиты информации

Вариант 3. Система защиты имеет шесть каналов воздействия, три из которых защищены неоднородными средствами защиты, три остались не защищенными (рисунок 2.14).

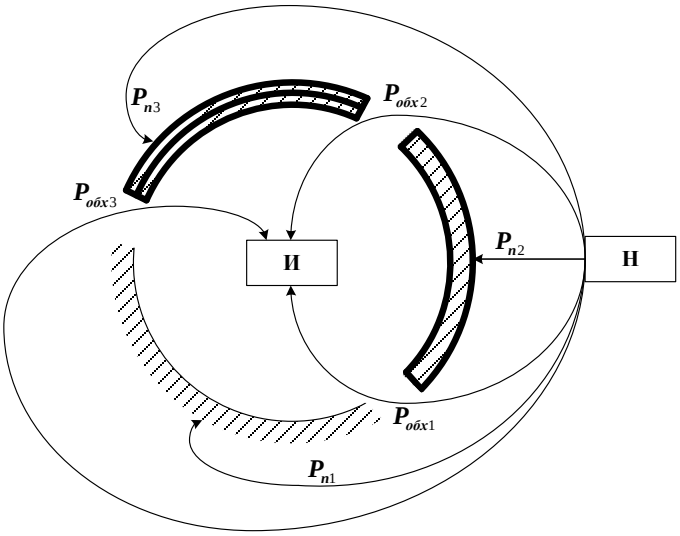


Рисунок 2.14 – Модель системы защиты информации

Тогда по аналогии с вариантами 1 и 2 граф и матрица состояний и переходов примут вид:

$$P_{[5,5]} = \begin{vmatrix} 0 & P_{пп1} & P_{пп2} & P_{пп3} & \left(P_{обх1} + P_{обх2} + P_{обх3}\right) \\ 0 & \left(1 - P_{пп1}\right) & 0 & 0 & P_{n1} \\ 0 & 0 & \left(1 - P_{n2}\right) & 0 & P_{n2} \\ 0 & 0 & 0 & \left(1 - P_{n3}\right) & P_{n3} \\ 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

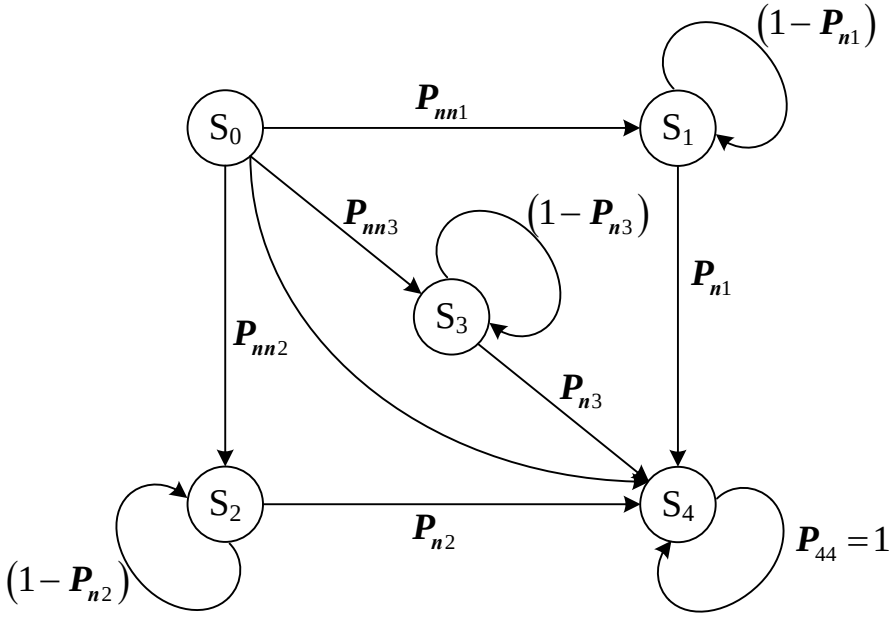


Рисунок 2.15 – Граф состояний и переходов

Воспользовавшись методом индукции, представим граф и матрицу состояний и переходов для общего случая

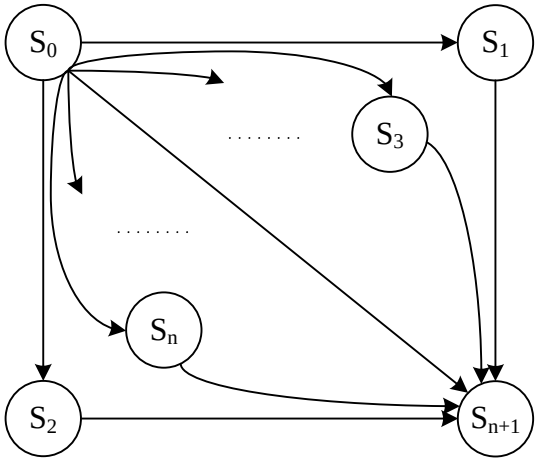


Рисунок 2.16 – Граф состояний и переходов

$$P_{[n+2,n+2]}=\begin{vmatrix} 0 & P_{nn1} & \dots & P_{nn3} & \left(P_{обх1}+P_{обх2}+\dots+P_{обхк}\right) \\ 0 & \left(1-P_{nn1}\right) & \dots & 0 & P_{n1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \left(1-P_{n3}\right) & P_{n3} \\ 0 & 0 & \dots & \dots & 1 \end{vmatrix} \quad (2.21)$$

В остальном методика оценки вероятности преодоления остается аналогичной той, что рассмотрена в пункте 2.2.1.

2.3 Разработка имитационной модели воздействия

Марковские модели являются универсальным инструментом исследования систем. Однако, требование экспоненциального распределения времени нахождения в том или ином состоянии существенно ограничивает область их корректного применения. Поэтому в данной работе, наряду с моделями, рассмотренными в пунктах 2.2.1, 2.2.2, 2.2.3, разработана имитационная модель воздействия нарушителя, представляющая собой численный метод статистического исследования процесса взлома системы защиты информации. Модель построена на сочетании принципов особых состояний и узловых точек [18]. Ввиду того, что события, соответствующие взлому (не взлому) того или иного устройства защиты в данной попытке являются вероятностными, а процесс взлома реализуется как правило методом подбора или случайного угадывания, в модели используется совокупность случайных чисел с квазиравномерным законом распределения в интервале [0,1].

2.3.1 Разработка алгоритмического описания процесса

Целью имитации является оценка возможных последствий взаимодействия воздействий нарушителя и системы защиты в условиях, наиболее адекватных исследуемому процессу.

Построение математической модели включает описание параметров и переменных, их взаимосвязи в общем алгоритме функционирования системы. Модель представлена в виде алгоритмического описания моделируемого процесса (рисунок 2.17).

Перед запуском процесса имитационного моделирования производится ввод исходных данных (блоки 1-4):

количество уровней защиты;

количество экспериментов (опытов);

характеристика каждого уровня защиты – вероятность преодоления, количество незаметных попыток проникновения сквозь средства защиты и количество проходов до восстановления средств защиты.

В блоке 5 осуществляется инициализация переменных, в которых будут накапливаться статистические данные по результатам экспериментов. Блоки 6 и 7 предназначены для динамического выделения памяти под хранение статистических данных соответственно за все попытки воздействия по каждому уровню и количество случаев "вскрытия" защиты по каждому уровню.

Для отслеживания времени, затрачиваемого на имитационное моделирование в блоке 8 предусмотрен запуск секундомера, отмечающего время с точностью до 1 с.

С блока 9 начинается цикл с предусловием, производящий с помощью декрементного счетчика заданное в блоке 2 количество экспериментов.

Блок 10 предназначен для подготовки исходных данных для текущего эксперимента.

Начиная с блока 11 производится моделирование воздействия нарушителя на всю систему защиты в целом. Если количество попыток воздействия нарушителя закончилось, то управление передается на блоки 12 – 14, где производится статистическая обработка результатов за текущий эксперимент и управление возвращается на блок 9 для проведения следующего эксперимента.

Если нарушитель использовал не все попытки воздействия на систему защиты информации, то в блоке 15 производится проверка преодоления первого уровня защиты. Если он был преодолен, тогда в блоке 16 инкрементируется счетчик проходов, а в блоках 17 – 18 производится проверка количества проходов нарушителя через "вскрытые" уровни защиты. При превышении заданного в исходных данных количества проходов для i-го уровня производится восстановление защиты *i*-го уровня. Тем самым имитируется обнаружение события нарушения защиты лицом, ответственными за обеспечение безопасности информации в системе.

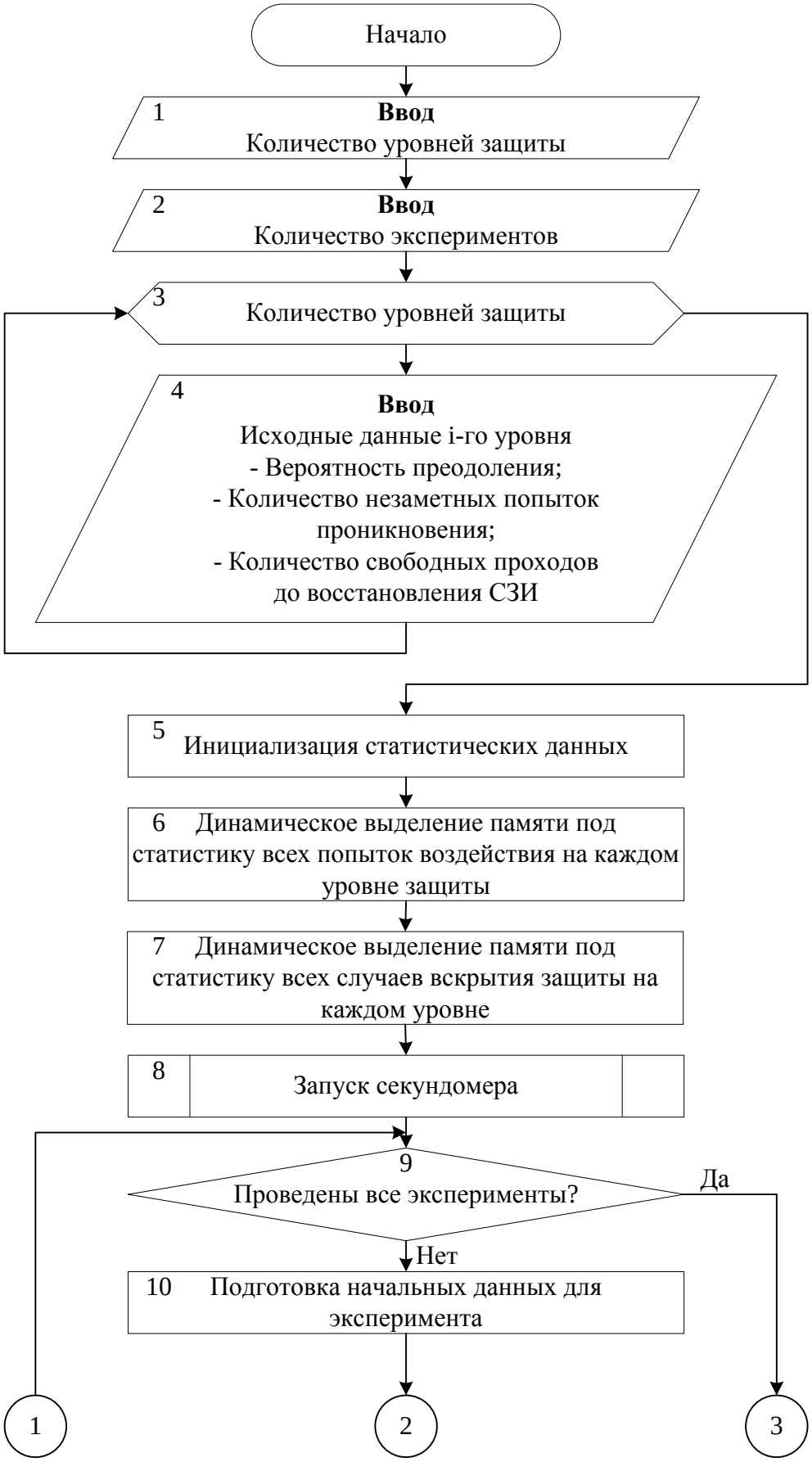


Рисунок 2.17 – Схема алгоритма имитационной модели (начало)

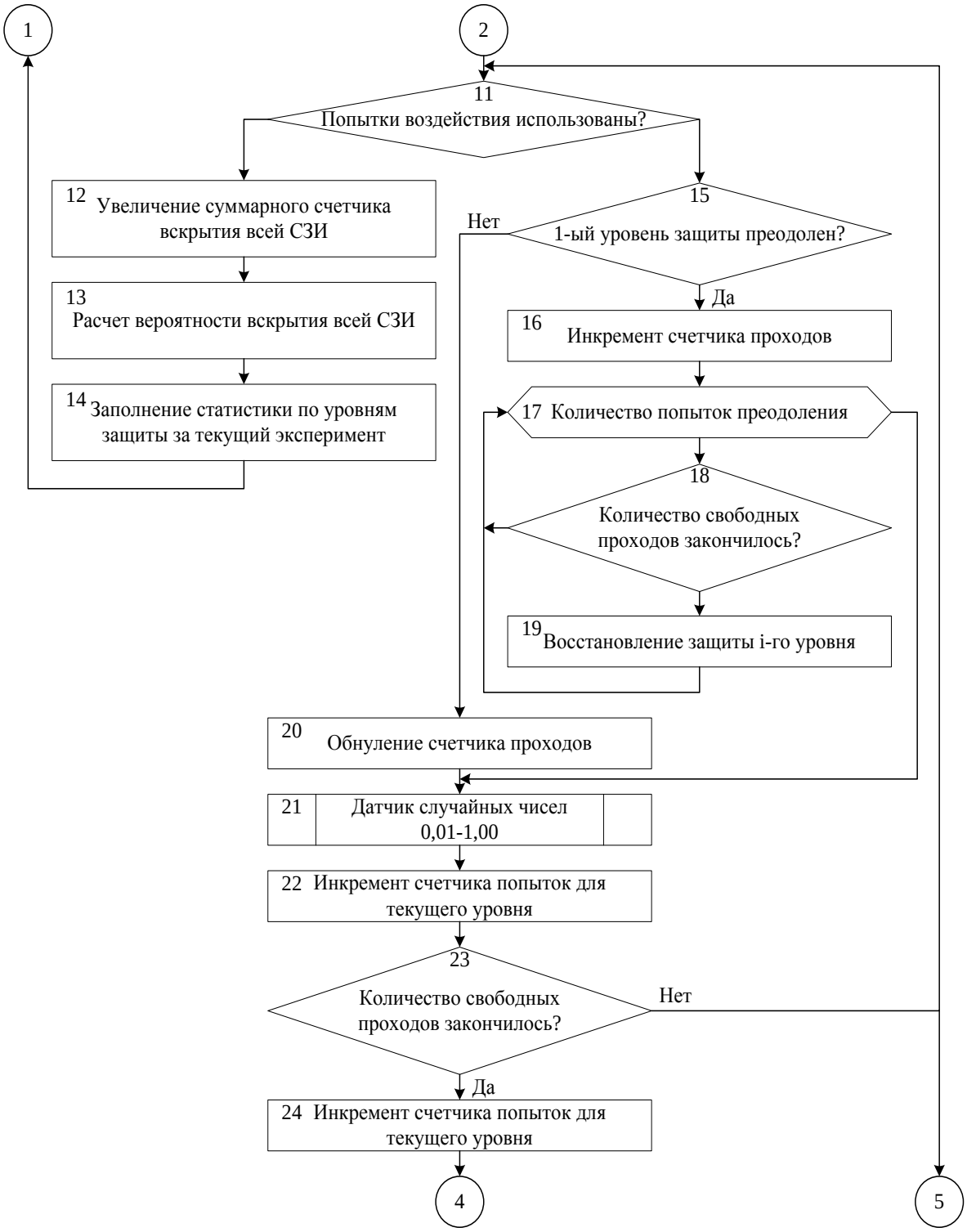


Рисунок 2.17 – Схема алгоритма имитационной модели (продолжение)

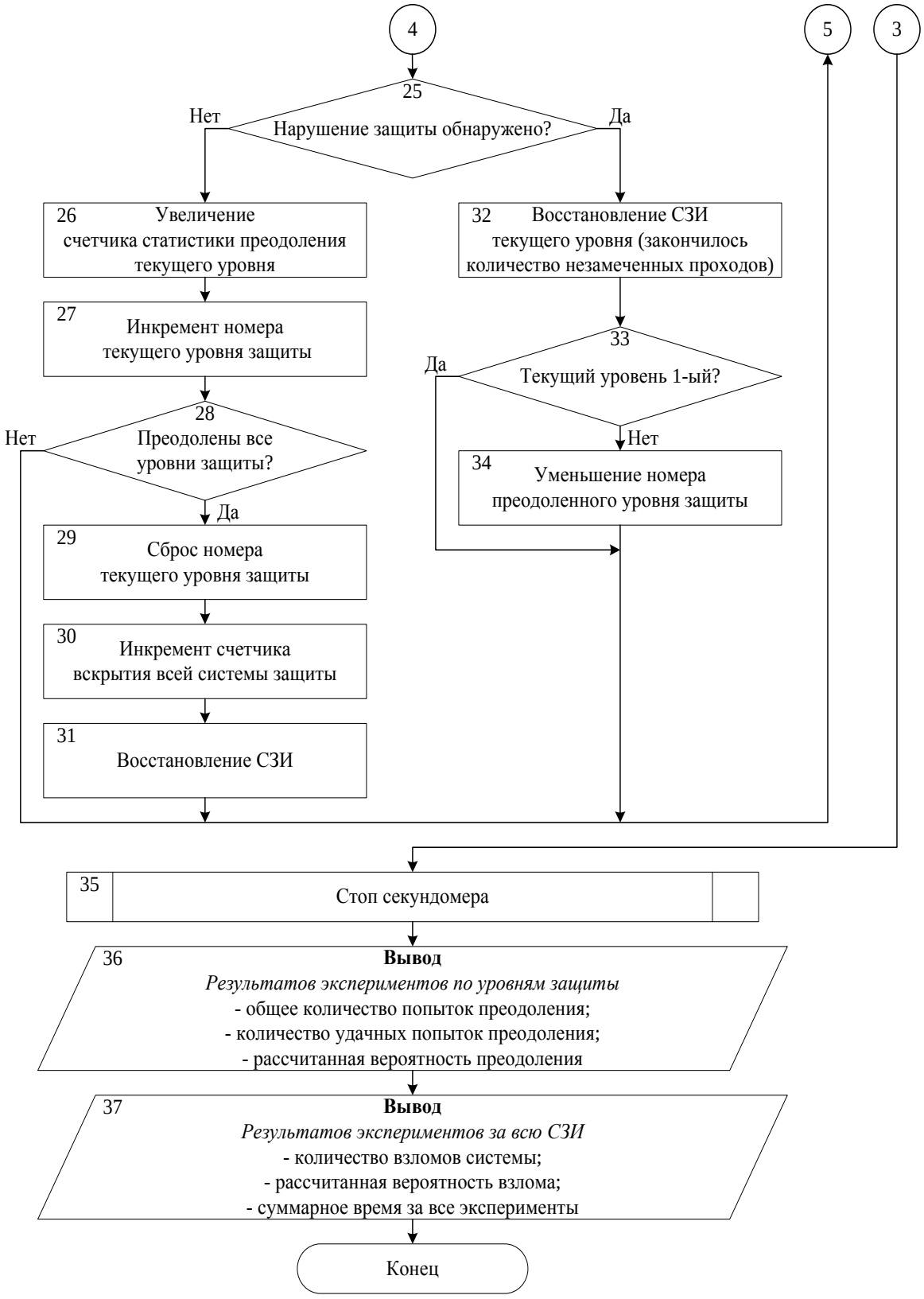


Рисунок 2.17 – Схема алгоритма имитационной модели (окончание)

В блоке 21 получается случайное число, распределенное по равномерному закону в диапазоне 0,01 – 1. Блок 22 увеличивает счетчик попыток преодо-

ления защиты текущего уровня. В блоке 23 полученное псевдослучайное число сравнивается с вероятностью преодоления средства защиты текущего уровня и, если полученное число меньше заданной вероятности преодоления уровня, то уровень защиты считается преодоленным, и блок 24 увеличивает счетчик удачных попыток преодоления текущего уровня защиты. Если защита текущего уровня не преодолена, то управление возвращается на блок 11.

В блоке 25 имитируется изменение параметров средств защиты предыдущего уровня с течением времени. Например, окончание действия пароля, кода доступа и т.д., используемого для проникновения сквозь уровень защиты.

Если параметры средств защиты предыдущего уровня не изменились, то текущий уровень защиты считается преодоленным, в блоке 26 увеличивается счетчик количества случаев преодоления для данного уровня и в блоке 27 инкрементируется номер уровня защиты; тем самым имитируется переход злоумышленника к следующему уровню защиты.

Блок 28 проверяет, не является ли "вскрытый" уровень защиты последним, тем самым осуществляется проверка преодоления всей СЗИ в целом. Если произошло "вскрытие" всей СЗИ, то в блоках 29 – 31 производится запоминание этого события для последующей статистической обработки и восстановление исходного состояния системы.

Если изменение параметров системы защиты предыдущего уровня (блок 25) произошло, то производится восстановление защиты предыдущего уровня (декремент номера преодоленного уровня защиты). Тем самым злоумышленник "отбрасывается" на предыдущий уровень защиты.

По окончании заданного количества экспериментов останавливается секундомер (блок 35), производится статистическая обработка данных, полученных за все эксперименты и на экран выводятся результаты моделирования:

1) по уровням защиты: общее количество попыток воздействия; количество удачных (для нарушителя) попыток преодоления уровня защиты; рассчитанная вероятность преодоления.

2) за всю систему защиты: количество "взломов" системы; рассчитанная вероятность "взлома"; суммарное время на моделирование.

2.3.2 Программная реализация модели

Программная реализация процесса имитационного моделирования системы защиты написана на языке C++. Общий вид основного экрана ПС изображен на рисунке 2.18

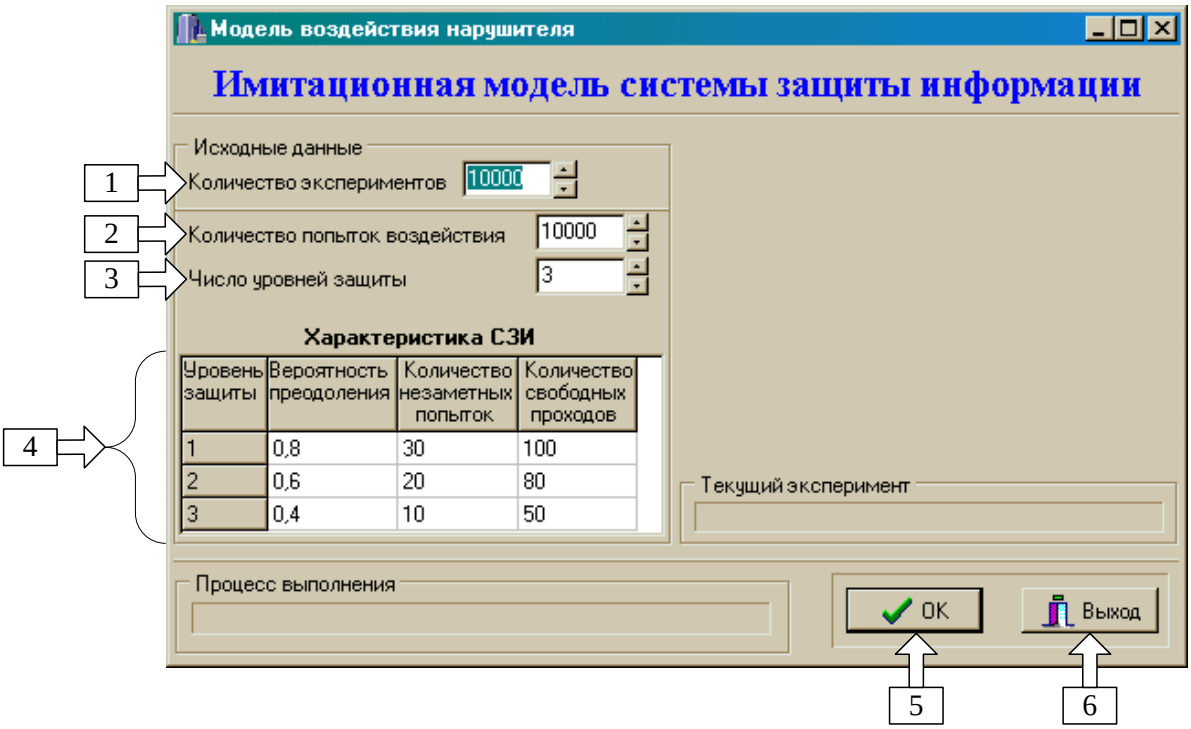


Рисунок 2.18 – Основной экран ПС имитационно модели

Процесс имитационного моделирования начинается с ввода исходных данных. Указывается количество экспериментов (1). Вводится количество попыток воздействия (2) на всю СЗИ, данная величина определяет, сколько попыток преодоления системы защиты может предпринять злоумышленник.

В общем случае она определяется стоимостью одной попытки и стоимостью охраняемой информации, либо последствий ее разрушения (модифика-

ции). Данная величина характеризует возможности злоумышленника по воздействию на СЗИ.

Количество уровней защиты (3) определяет, является ли система защиты эшелонированной (количество уровней > 1) и сколько уровней образуют систему защиты в целом.

Каждый уровень характеризуется своими исходными данными (4).

К ним относятся:

вероятность преодоления защиты уровня. Эта характеристика получается по специальным методикам для конкретного оборудования в результате сертификационных испытаний средств защиты, составляющих данный уровень;

количество свободных проходов. Характеристика, определяющая период изменения (восстановления) параметров средств защиты, составляющих данный уровень. Она задает количество проходов через преодоленный уровень защиты до момента, когда истечет срок действия данных, найденных злоумышленником, позволяющих ему проникать через данный уровень защиты (например, истек срок действия пароля, идентификатора, ключа защиты и т.д.);

количество незаметных проходов. Эта характеристика определяет субъективную сторону уровня защиты и характеризует наличие специальной службы безопасности информации, а также качество ее работы. Введенное число задает количество проходов через уровень защиты, которые может совершить злоумышленник до момента, когда представитель службы безопасности сети обнаружит факт «вскрытия» защиты уровня и изменяет его параметры.

Запуск имитационного моделирования производится нажатием кнопки «ОК» (5). Протекание процесса моделирования показывается двумя полосовыми индикаторами 7 и 8 рисунка 2.19. Сегментированный индикатор (7) отражает процесс моделирования в текущем эксперименте, а сплошной индикатор (8) – за все эксперименты.

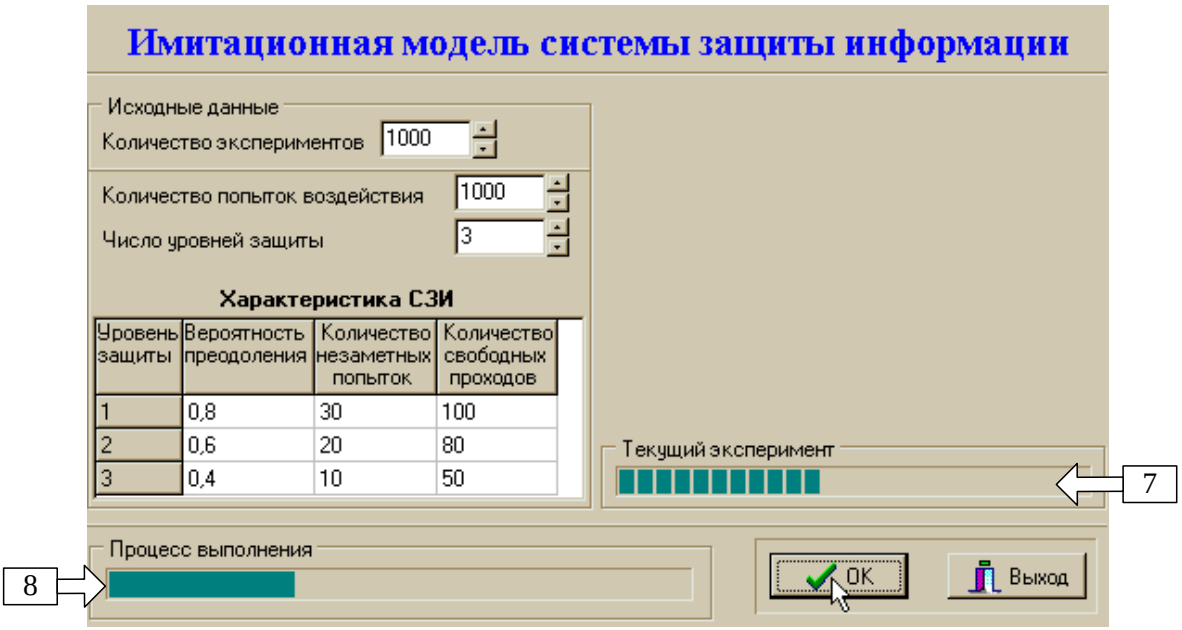


Рисунок 2.19 – Экран протекания процесса имитационного моделирования

По окончании процесса имитационного моделирования (индикатор 8 достигает правой границы), на правую часть основного окна выводятся результаты моделирования (рисунок 2.20).

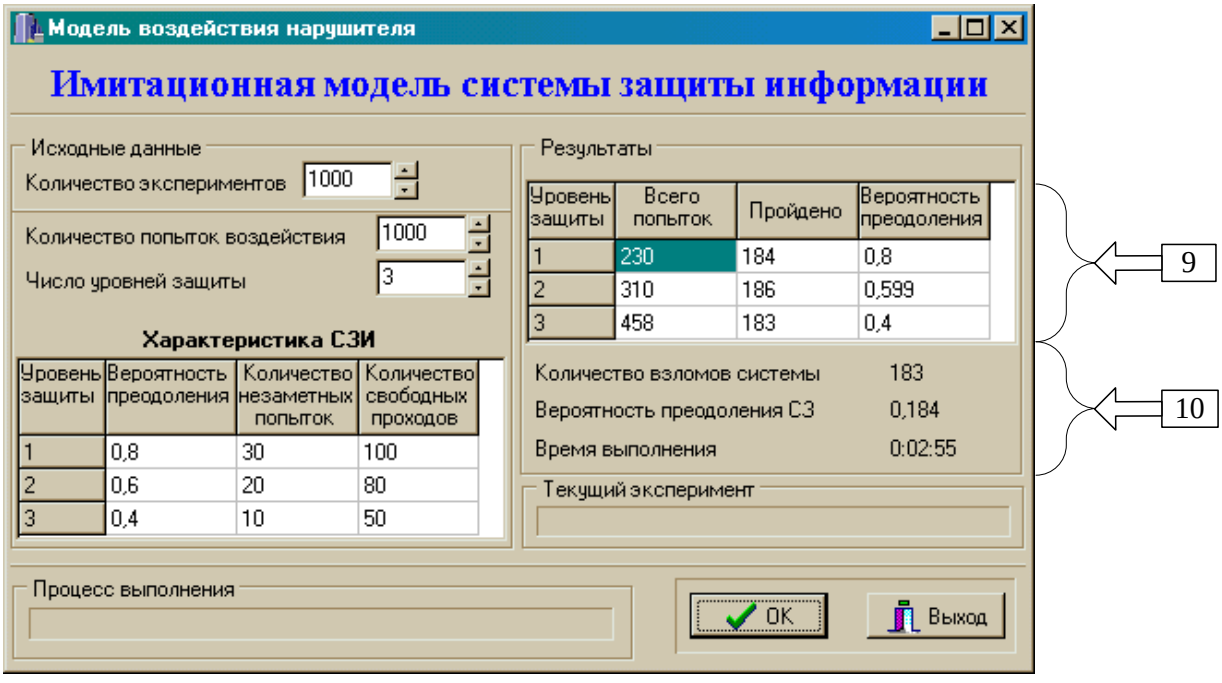


Рисунок 2.20 – Экран результатов имитационного моделирования

Результаты разделяются на две части: по уровням защиты и за всю СЗИ в целом. Для каждого уровня выводится количество попыток, предпринятых злоумышленником для «вскрытия» защиты уровня и сколько из них увенчались

для него успехом. В результате рассчитывается вероятность преодоления защиты данного уровня.

Основным результатом является общее количество попыток, предпринятых злоумышленником для «вскрытия» всей СЗИ и количество случаев преодоления всех уровней защиты. На основании этих данных рассчитывается вероятность преодоления всей системы защиты целиком.

Для оценки временных характеристик имитационного моделирования выводится время, затраченное компьютером на этот процесс.

Для выхода из программы моделирования и возвращения в операционную систему предназначена кнопка «Выход» (6) (рисунок 2.18).

2.3.3 Оценка статистической точности результатов моделирования

Для количественной оценки репрезентативности полученных результатов воспользуемся выборочным методом, как наиболее распространенным в статистике методом не сплошного наблюдения. Основным достоинством данного метода является то, что он позволяет при относительно небольшой выборке из генеральной совокупности (обычно 5…10%, реже 15…25%) получить с требуемой достоверностью численные значения таких важных показателей, как относительная величина альтернативного признака (например, частота проявления исследуемого признака) – ω и средняя величина количественного признака (выборочная средняя – x).

Частота ω будем определять из отношения числа воздействий, при которых СЗИ оказалась невскрытой – m к общему числу испытаний – n:

$$\omega = \frac{m}{n} \tag{2.22}$$

В связи с тем, что изучаемые статистикой признаки варьируются, то состав единиц, попавших в выборку, может не совпасть (по изучаемым признакам) с их составом в генеральной совокупности. Отсюда значения ω и x могут отличаться от значений этих характеристик в генеральной совокупности – P и

X. Возможные расхождения между значениями характеристик выборки и генеральной совокупности измеряются средней ошибкой выборки – μ, характеризующей достоверность полученных результатов. В [22, 114] доказано, что значения средней ошибки выборки определяются по формуле:

$$\mu = \sqrt{\frac{\sigma_0^2}{n}}. \qquad (2,23)$$

Формула (2.23) предполагает, что известна генеральная дисперсия σ_0^2, что не является достоверным событием при проведении статистического моделирования. Вместе с тем в статистике доказано следующее соотношение между дисперсиями в генеральной и выборочной совокупностях:

$$\sigma_0^2 = \sigma^2\left(\frac{n}{n-1}\right) \qquad (2.24)$$

Тогда, подставив (2.24) в (2.23) при большом *n* получаем приближенное значение

$$\mu \approx \sqrt{\frac{\sigma^2}{n}} \qquad (2.25)$$

При этом для показателя доли альтернативного признака дисперсия в выборке определяется по формуле

$$\sigma_\omega^2 = \omega(1-\omega). \qquad (2.26)$$

Однако, необходимо иметь ввиду, что формула (2.25) выведена при условии проведения так называемого повторного отбора (при проведении независимых испытаний). Поскольку при бесповоротном отборе численность генеральной совокупности *N* в ходе выборки сокращается, то в формулу для расчета средней ошибки выборки включают дополнительный множитель и формула средней ошибки выборки принимает вид:

$$\mu \approx \sqrt{\frac{\sigma^2}{n}\left(1-\frac{n}{N}\right)} \qquad (2.27)$$

Так как при решении данной задачи испытания являются независимыми (число *N* от реализации к реализации не меняется), то будем использовать вы-

ражение (2.25). тогда доля исходов испытаний, когда СЗИ окажется невзломанной, будет находится в пределах:

$$p - \mu_\omega \le \omega \le p + \mu_\omega \qquad (2.28)$$

т.е. характеристика искомой доли в генеральной совокупности – p, будет отличаться от характеристики доли в выборке – ω на величину средней ошибки выборки – μ, но лишь с определенной степенью вероятности. В статистике доказано, что эта вероятность составляет 0,6827. Там же доказано, что вероятность суждений можно повысить, если расширить пределы отклонений, приняв в качестве меры среднюю ошибку выборки μ, умноженную на t. Данное произведение называется предельной ошибкой выборки и обозначается

$$\Delta_B = t\mu_\omega \qquad (2.29)$$

При $t=2$ вероятность суждения достигает 0,9545, при $t=3$ - *0,9973*. В общем случае доли альтернативного признака в генеральной совокупности и выборке связаны между собой соотношением

$$p = \pm t\mu_\omega \qquad (2.30)$$

Множитель t называется коэффициентом доверия. Он выбирается в зависимости от того, с какой доверительной вероятностью необходимо гарантировать результаты выборочного исследования. Выбор t осуществим, используя таблицы, полученные А.М. Ляпуновым по функции вида

$$F_{(t)} = \frac{1}{\sqrt{2\pi}} \int_{-t}^{+t} e^{-\frac{t^2}{2}} dt \qquad (2.31)$$

Выписка из этой таблицы для приемлемых значений t приведена в таблице 2.1.

Таблица 2.1 – Выписка из таблицы Ляпунова

Кратность ошибки t	Вероятность $F_{(t)}$	Кратность ошибки t	Вероятность $F_{(t)}$
0,0	0,0000	2,0	0,9545
0,1	0,0797	2,5	0,9876
0,5	0,3829	2,6	0,9907
1,0	0,6827	3,0	0,9973
1,5	0,8664	4,0	0,999937

Из (2.25) следует, что средняя ошибка выборки μ обратно пропорциональна $\sqrt{n}$, т.е. при увеличении численности выборки, например в 4 раза, оцениваемый показатель ошибки уменьшится в 2 раза, поэтому необходимую численность выборки определяют как некоторый компромисс между требуемыми точностью и оперативностью расчетов. Так как при решении данной задачи оперативность решения не является критичным показателем, предъявим более высокие требования к точности расчетов.

Определение необходимой точности выборки основывается на формуле предельной ошибки выборки. Подставив (2.26) в (2.23), для определения доли альтернативного признака получим

$$\Delta_{\omega}^{2} = t^{2}\frac{\omega(1-\omega)}{n} \tag{2.32}$$

откуда

$$n = \frac{t^{2}\omega(1-\omega)}{\Delta_{\omega}^{2}} \tag{2.33}$$

Таким образом, пусть событие A – факт не преодоления многоуровневой СЗИ с заданного числа попыток воздействия. Тогда отношение

$$P_{B}(A) = \frac{m}{n} \tag{2.34}$$

будет являться частотою возникновения события A в выборке n. Она естественно может не совпадать с вероятностью

$$P(A) = \frac{m_{\Gamma}}{n} \tag{2.35}$$

полученной по генеральной совокупности N испытаний.

Из общей теории статистики известно, что существуют понятия:

малой выборки - $4 < n < 20$;

средней выборки - $20 < n < 100$;

большой выборки - $n > 100$.

При применении малой выборки для определения средней ошибки μ пользуемся таблицами, полученными по распределению Стьюдента. Однако,

если сравнить значения вероятностей в таблицах Стьюдента и функции (2.31), то нетрудно заметить, что уже при *n=20* и числе степеней свободы *t=3* расхождения в значениях вероятностей невелики. При решении данной задачи особых ограничений на объем выборки не накладывается, поэтому выберем число *n* более 100 и тогда при определении средней ошибки μ можно использовать нормальное распределение.

При этом

$$P\left(\left|P_B(A)-P(A)\right|-\Delta_B\right)=\alpha \qquad (2.36)$$

где α доверительная вероятность.

Если выбрать $\alpha=0,95$, $t=2$, тогда вероятность P=0,9545.

Зададимся предельной ошибкой $\Delta_B \le 0,01$, при этом из (2.29) μ=0,005, т.е. с вероятностью 0,9545.

$$\left|P_B(A)-P(A)\right|=0,005$$

При $\omega=0,995$ и $\sigma^2=\omega(1-\omega)$, в соответствии с (2.33),

$$n=\frac{\sigma^2}{\mu^2}=\frac{0,004975}{0,000025}=199$$

Таким образом, при проведении *n=200* испытаний и более, средняя ошибка репрезентативности с вероятностью 0,9545 не превысит 0,005.

Варьируя между оперативностью и точностью выберем *n=1000*. При этом с вероятностью 0,9545 средняя ошибка репрезентативности не превысит

$$\mu=\sqrt{\frac{\sigma^2}{n}}=0,00016$$

Кроме того, при $n \ge 1000$ с некоторой степенью приближенности данный процесс может считаться стационарным и эргодическим. Из этого следует, что обработка и анализ данных, полученных при моделировании, может осуществляться традиционными методами математической статистики (усреднением полученных в каждой реализации результатов).

Результаты исследования процесса "взлома" системы защиты, приведенной на рисунке 2.7, с исходными данными таблицы 2.2 представлены в таблице 2.3.

Таблица 2.2 – Исходные данные системы защиты

Количество попыток воздействия – 1000			
Уровень защиты	Вероятность преодоления уровня	Количество незаметных попыток проникновения	Количество свободных проходов через "взломанный" уровень
1	0,8	30	100
2	0,6	20	80
3	0,4	10	50

Таблица 2.3 – Результаты исследования системы защиты

Уровень защиты	Количество попыток «вскрытия» защиты уровня	Количество «взломов» защиты уровня	Вероятность преодоления
1	230	184	0,8
2	312	186	0,6
3	458	183	0,4
Количество "взломов" всей системы защиты – 184			
Вероятность преодоления системы защиты – 0,184			
Время выполнения – 0:02:55			

ВЫВОДЫ ПО РАЗДЕЛУ

Исследование систем защиты информации в ИОС сложных ИТС требует разработки моделей воздействия нарушителя (злоумышленника), адекватно описывающих наиболее существенные состояния и связи процесса защиты информации и степени их влияния на выбранные показатели.

Вместе с тем, анализ известных моделей воздействия и возможности их применения для исследования СЗИ ИОС ИТС позволяет сделать следующие выводы.

1. В настоящее время, несмотря на большое количество проведенных исследований у нас в стране и, особенно за рубежом, единая и общепринятая модель воздействия ещё не создана.

2. Одноуровневые и многоуровневые матричные модели носят в основном теоретический характер и практического применения без существенных доработок найти не могут.

3. Значительная часть статистических моделей предполагает исследование влияния возможных вариантов воздействия на стоимостные характеристики систем защиты информации конкретных ИОС и ИТС в целом. Данный класс моделей основывается на методики оценки экономической целесообразности и не может быть напрямую использован при исследовании СЗИ ИОС ИТС.

4. Наиболее близким по сущности к поставленной в данной работе задаче является класс моделей, базирующихся на логико-вероятностный подход. Однако, существенным недостатком данного класса моделей является то, что они не учитывают динамику изменения состояний системы защиты в процессе воздействия («взлом» отдельных эшелонов защиты и восстановление их по истечение определенного установленного времени или по действиям администраторов службы безопасности).

5. Этих недостатков лишены модели, разработанные в данной работе. Математическую основу данного класса моделей составляет аппарат теории

марковских цепей. Разработанные модели более адекватно описывают процесс защиты информации, так как позволяют учитывать следующие обстоятельства:

злоумышленник может перейти к вскрытию очередного эшелона защиты только после того, как ему удалось преодолеть предыдущие («простая марковская модель защиты» - п.2.2.1);

вскрытый эшелон защиты восстанавливается по истечении некоторого указанного времени или при обнаружении вскрытия оперативным персоналом службы безопасности информации ИТС («марковская модель с восстановлением» - п.2.2.2).

6. Важной особенностью распределенных ИТС является принципиальная невозможность создания замкнутых (круговых) систем защиты, обеспечивающих закрытие всех возможных каналов воздействия. Для исследования таких СЗИ в динамике разработана «марковская модель воздействия на очаговую систему защиты» - п.2.2.3.

7. Исследование СЗИ со значительным числом эшелонов защиты с помощью марковских моделей встречает серьезные затруднения в связи с необходимостью пошагового оперирования с матрицами большой размерности. В связи с этим в работе разработана имитационная статистическая модель, построенная на сочетании особых состояний и узловых точек (п. 2.3). исследования, проведенные в работе данной модели показали, что с её помощью можно получить требуемую точность вычислений за приемлемое время, а реализованный в модели человеко-машинный интерфейс достаточно прост, удобен в работе и позволяет использовать данную модель в методике оптимизации размещения средств защиты по каналам воздействия. Правильность разработки модели подтверждена сходимостью ее результатов с результатами математического моделирования с помощью марковских моделей при одинаковых исходных данных.

8. Результаты моделирования СЗИ ИОС ИТС с помощью разработанных моделей показали, что полученные результаты отличаются от известных (полученных по ранее использовавшимся моделям) в сторону увеличения вероятности преодоления на 17…21 %, что еще раз подчеркивает необходимость совершенствования СЗИ в существующей и создаваемых ИТС управленческого типа.

3 РАЗРАБОТКА МЕТОДИКИ ОПТИМАЛЬНОГО РАЗМЕЩЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОБЪЕКТАХ ИТС

3.1 Постановка задачи

В разделе 2 данной диссертационной работы разработаны модели воздействия на один субъект информации (например, массив) ИОС ИТС. Вместе с тем, на ИОС ИТС хранится, обрабатывается и используется, как правило, достаточно большое количество массивов, содержащих информацию разной важности.

Пусть на некотором объекте *A* хранится *M* субъектов (массивов) информации. Каждый массив S_j, $j=\overline{1,M}$ (рисунок 3.1) оценивается коэффициентом относительной важности (стоимости) хранимой информации - C_j, $j=\overline{1,M}$ и характеризуется внутренней защищенностью, основывающейся на установленных административных правилах и особенностях аппаратного и программного построения. Следует отметить, что $\sum C_j = 1$. То есть, относительный ущерб характеризует часть номинальной стоимости ущерба от вскрытия всех объектов. Злоумышленник (хакер, крекер) стремится получить доступ к информации, хранящейся на ИОС ИТС в составе массивов, с целью ее уничтожения, копирования, модификации и т.д., характеризующийся нанесением ущерба хранимой информации. Вероятный ущерб, наносимый информации, хранящейся в *i*-м, будем обозначать w_j, $j=\overline{1,M}$.

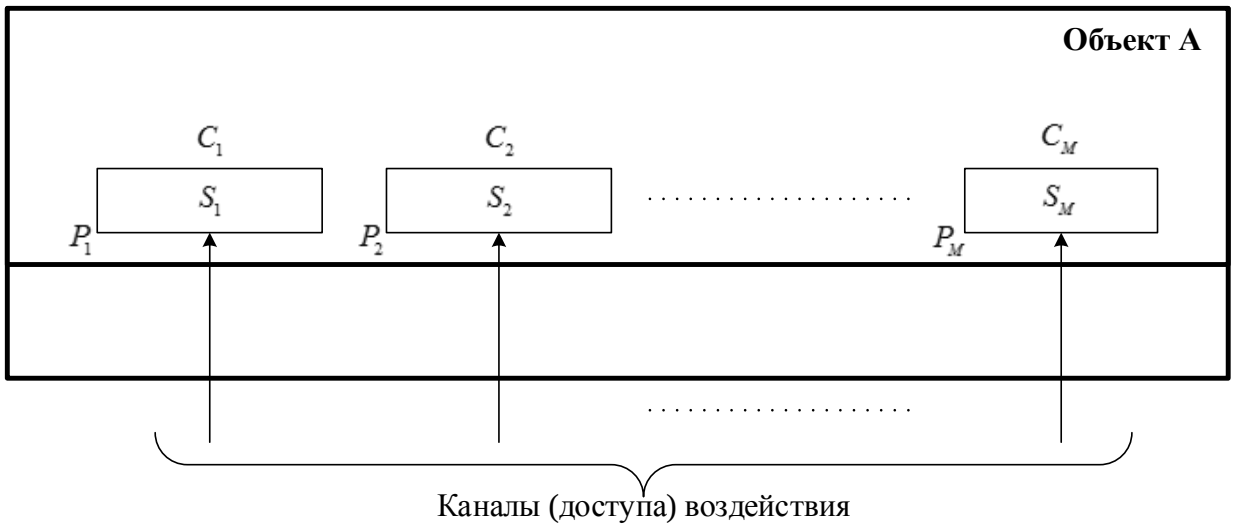


Рисунок 3.1 – Объект, хранящий массивы информации

Как показано в (1.4) с учетом важности хранимой и обрабатываемой информации показатель эффективности СЗИ может быть представлен как ущерб, наносимый массиву информации при получении к нему несанкционированного доступа

$$w_i = C_i P_{\Pi i}, \tag{3.1}$$

а суммарный вероятный ущерб, наносимый M массивам информации, как

$$W = \sum_{i=1}^{M} w_i \tag{3.2}$$

В распоряжении злоумышленника имеется ограниченное количество N попыток воздействия, с помощью которых он может физически или логически разрушить, исказить, модифицировать и т.д. каждый массив одним средством с вероятностью P_j, $j = \overline{1,M}$, причем

$$N = \sum_{j=1}^{M} n_j, \tag{3.3}$$

где n_j - количество попыток воздействия на массив S_j;

Тогда, в соответствии с логико-вероятностным подходом, вероятный ущерб, наносимый информации, хранимой в массиве S_j с одной попытки воздействия может быть найден из выражения:

$$w_j = C_j \left[1 - \left(1 - P_j\right)\right], \tag{3.4}$$

а с n_j попыток

$$w_j\left[n_j\right] = C_j\left[1-\left(1-P_j\right)^{n_j}\right] \tag{3.5}$$

С учетом (3.4), (3.5) выражение (3.2) примет сепарабельный аддитивный вид

$$W\left[N\right] = \sum_{j=1}^{M} C_j\left[1-\left(1-P_j\right)^{n_j}\right] \tag{3.6}$$

Естественно полагать, что противник стремится нанести хранимой информации максимально возможный, с его точки зрения, ущерб. В [21] показано, что суммарный вероятный ущерб W будет являться функцией не только от C_j, P_j и n_j, но и от распределения числа попыток $<n>$ по массивам хранимой информации, основывающегося на знании противником векторов $<C_j>$, $<P_j>$, и в следствие выпуклости функции (3.4), (3.5), всегда имеется некоторое распределение $<n^*>$, при котором $W[n^*]$ будет максимально.

Тогда, с точки зрения злоумышленника, задача нахождения максимального ущерба, наносимого информации, хранящейся на объекте А, может быть поставлена следующим образом:

при заданных C_j, P_j, M, найти $<n^*>$, для которого $W[n^*] \underset{\{N\}}{\rightarrow} \max$, при ограничении:

$$N = \sum_{j=1}^{M} n_j \,. \tag{3.7}$$

В свою очередь хранитель информации, стремясь уменьшить ущерб, наносимый информационным массивам ИОС ИТС до допустимой величины Y_{TP} создает систему защиты, перекрывая возможные каналы воздействия некоторым набором A средств защиты (рисунок 3.2).

Злоумышленник, получив априори информацию о количестве (А), размещении $<a>$ и характеристиках $<q>$ средств защиты, решает задачу (3.7), с учетом изменившейся ситуации. Формально новая задача может быть поставлена следующим образом:

найти такой план распределения попыток воздействия $<n^*>$, для которого

$\underset{\{N,A\}}{И[n^*, a]} \to \max$, при ограничениях

$$\sum_{j=1}^{M} n_j = N; \quad \sum_{j=1}^{M} a_j = A. \tag{3.8}$$

Дальнейшее снижение ущерба может быть достигнуто как минимум тремя путями:

1) увеличением числа средств защиты. При этом не должно нарушаться условие $C_A \le \sum_{j=1}^{M} C_j$,

где C_A - стоимость средств защиты;

2) модернизацией (заменой) установленных на объекте средств защиты (совершенствованием их характеристик - g). Эта возможность также ограничена общей стоимостью средств защиты;

3) оптимальным размещением имеющихся средств защиты по каналам воздействия.

В условиях финансовых ограничений и высокой стоимости существующих средств защиты третий путь является наиболее привлекательным.

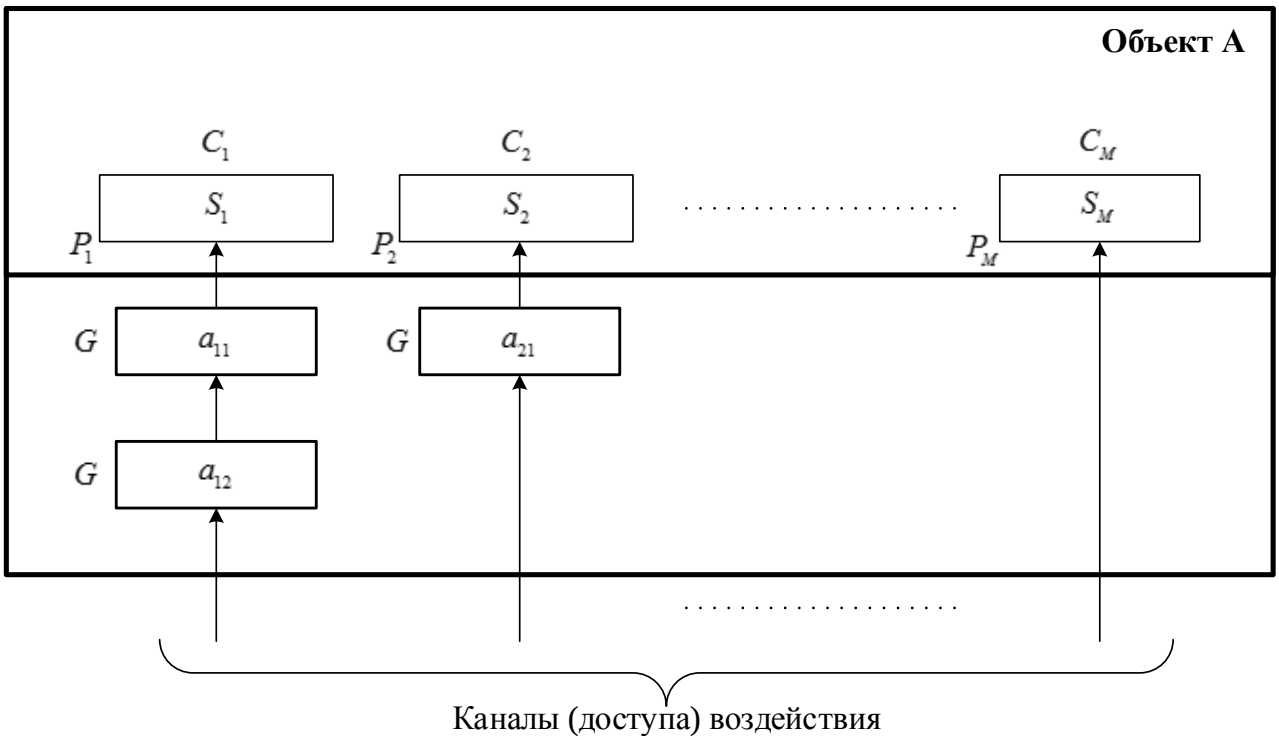


Рисунок 3.2 – Объект с созданной системой защиты

С учетом этого, с точки зрения хранителя информации, задача может быть поставлена следующим образом:

при заданных C_j, P_j, и M, найти такой план распределения средств защиты $<a^*>$, при оптимальном плане распределения попыток воздействия злоумышленника $<n^*>$, для которого суммарный вероятный ущерб $W[a^*,n^*]$ был бы минимальным, т.е.:

найти $<a^*>$, при $<n^*>$,

для которых $\underset{\{A;N\}}{W^*}[a^*, n^*] \to \min$, при

$$\sum_{j=1}^{M} n_j^* = N; \quad \sum_{j=1}^{M} a_j^* = A. \tag{3.9}$$

Такая задача относится к комбинаторным и при большой размерности обладает высокой сложностью. Поэтому, для ее решения целесообразно использовать итерационную процедуру, базирующуюся на системном подходе, обобщенный алгоритм которой представлен на рисунке 3.3.

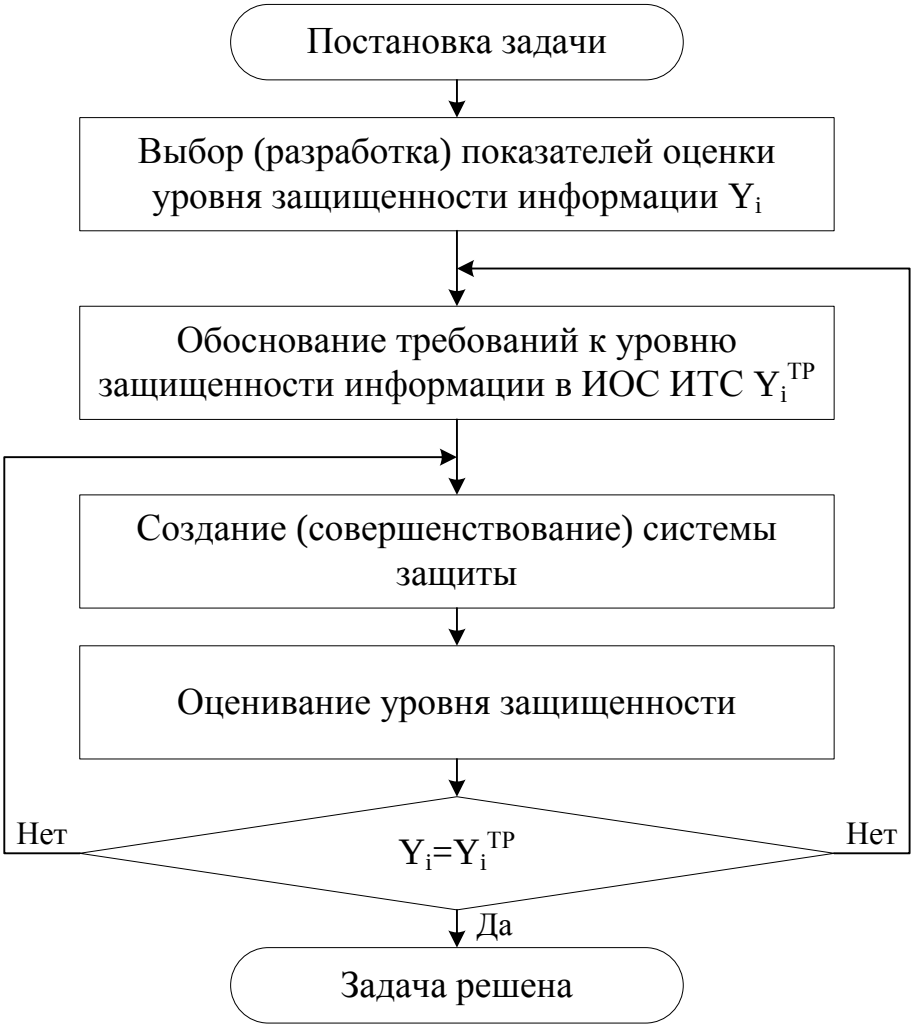


Рисунок 3.3 – Общий подход к достижению требуемого уровня защиты ИОС

Содержание блоков 1 и 2 является самостоятельной научной задачей, в рамках данной диссертационной работы разработана методика, реализующая содержание блоков 3 и 4. Основные этапы методики представлены на рисунке 3.4 и рассматриваются в п. 3.2-3.5.

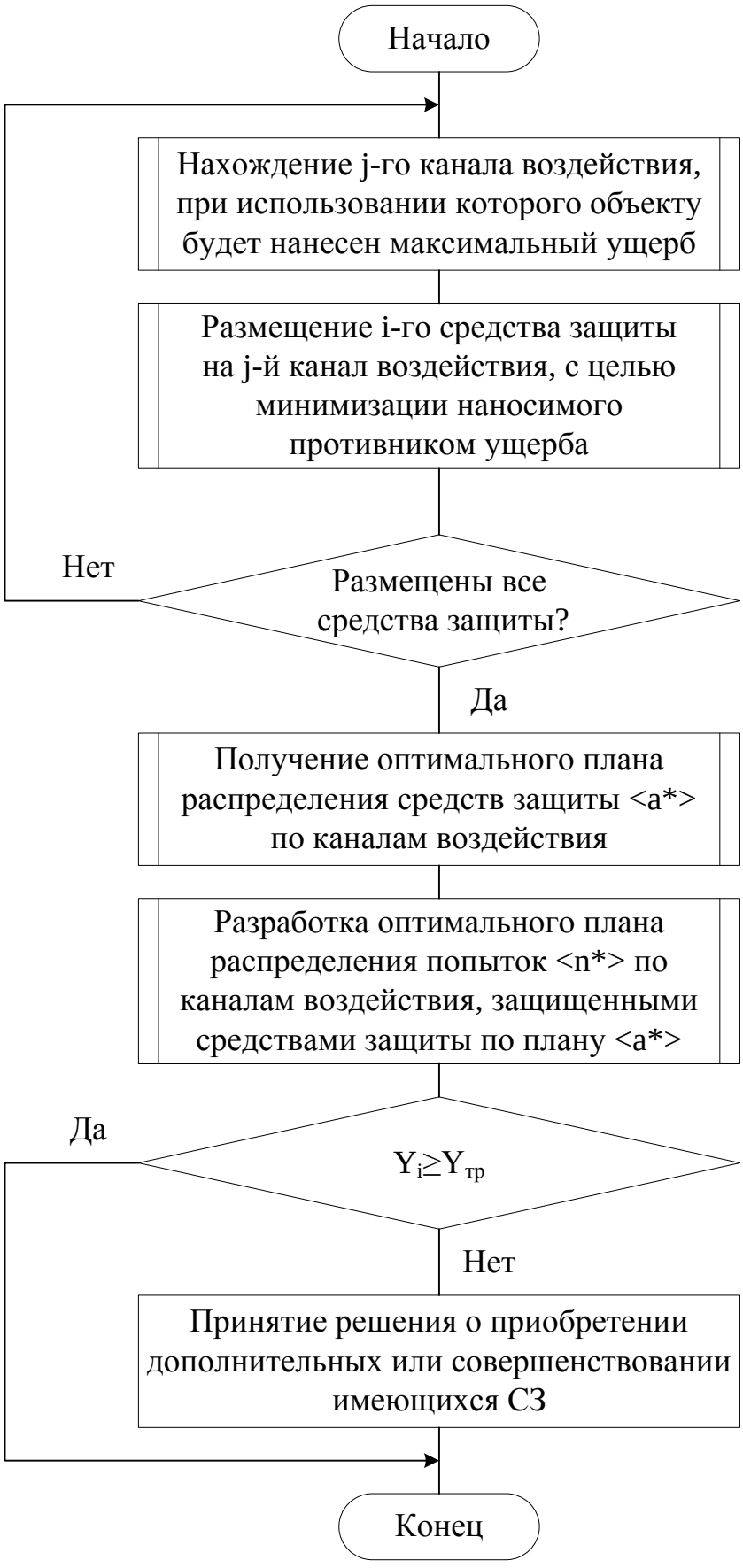


Рисунок 3.4 – Основные этапы методики оптимизации размещения средств защиты информации

3.2 Оценка ущерба, наносимого массивам информации, хранящимся на ИОС

3.2.1 Оценка ущерба на объекте без средств защиты

Проведенные исследования [53, 55, 69] показывают, что целевая функция частных ущербов (3.1, 3.4, 3.5) в значительной части практических задач оценивания эффективности применения СЗИ, является функцией целочисленного аргумента, а её огибающая – монотонной и выпуклой, огибающая функции суммарного вероятного ущерба (3.6) в силу теоремы 3.1 [1, 14] – монотонной выпуклой аддитивной сепарабельной. Для таких функций справедливы все теоремы выпуклого программирования, в том числе и лемма 1 (Гибса), позволяющая достаточно оперативно отыскивать искомое распределение.

Вместе с тем, как показано в [53], в силу особенностей функционирования СЗИ (наличия борьбы антагонизмов), применить напрямую лемму Гибса для решения поставленной задачи не представляется возможным. С учетом этого в диссертационной работе найдено решение данной задачи в виде пошаговой оптимизационной процедуры, алгоритм которой представлен на рисунке 3.5.

Алгоритм реализован в интегрированной системе научных и математических расчетов Mathcad. Покажем применение алгоритма на конкретном примере.

1. Ввод исходных данных (блок 1).

Исходные данные для исследуемого объекта приведены в таблице 3.1.

Таблица 3.1 – Исходные данные объекта защиты

Количество защищаемых массивов информации и их стоимость	M=4 (2600 у.е.)			
	S_1	S_2	S_3	S_4
Относительная важность (C_j)	0,23	0,15	0,27	0,35
Вероятность поражения (P_j)	0.3	0.5	0.2	0.1
Количество попыток воздействия	N=10			

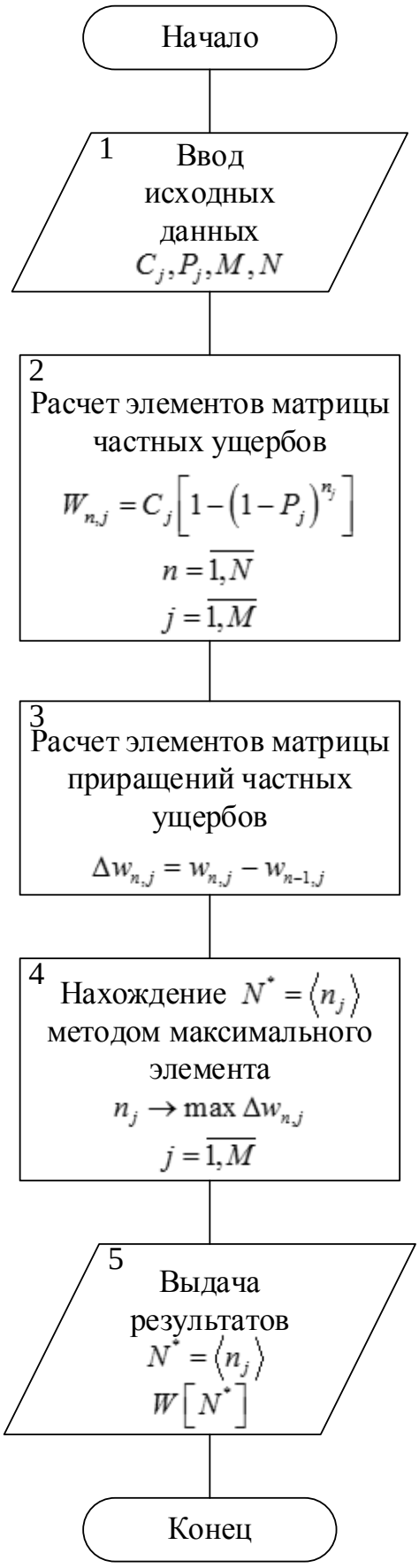


Рисунок 3.5 – Схема алгоритма оценки ущерба, наносимого информации и, хранящейся на объекте без средств защиты

2. Расчет матрицы частных ущербов (блок 2).

Таблица 3.2 – Матрица частных ущербов от воздействия

$n\backslash w$	w_1	w_2	w_3	w_4
1	180	200	140	90
2	306	300	252	172
3	394	350	342	243
4	456	375	413	310
5	499	388	470	369
6	529	394	517	422
7	551	397	553	470
8	565	398	583	513
9	576	399	606	551
10	583	399	624	586

3. Расчет элементов матрицы приращений частных ущербов (блок 3)

Таблица 3.3

$n\backslash \Delta w$	Δw_1	Δw_2	Δw_3	Δw_4
1	180	200	140	90
2	126	100	112	81
3	88,2	50	89,6	72,9
4	61,74	25	71,68	65,61

4. Нахождение оптимального (с точки зрения злоумышленника) распределения попытки воздействия (таблица 3.3)

$$N^* = \langle 3,2,3,2 \rangle.$$

5. Вычисление суммарного вероятного ущерба, наносимого злоумышленником, при использовании оптимального распределения попыток воздействия (таблица 3.2)

$$W = 1206,8 \ (0,464).$$

3.2.2 Оценка ущерба на объекте со средствами защиты

Создавая на исследуемом объекте А (ИОС ИТС) систему защиты информации, в дополнение к п.3.2.1, вводим следующие исходные данные и допущения. Каждый массив S_j может быть защищен некоторым количеством внешних однородных, универсальных средств защиты a_j, причем $\sum_{j=1}^{M} a_j = A$.

Любое средство защиты a_j может быть преодолено однородными и универсальными средствами воздействия злоумышленника с одной попытки с вероятностью G. С учетом этих дополнений, вероятный ущерб, наносимый информации, хранимой в массиве S_j, закрытом a_j числом средств круговой системы защиты, с одной попытки воздействия может быть найден из выражения

$$w_j\left[a_j\right] = C_j \cdot \left(G^{a_j} \cdot P_j\right), \tag{3.10}$$

а с n независимых попыток

$$w_j\left[a_j, n_j\right] = C_j \cdot \left[1 - \left(1 - \left(G^{a_j} \cdot P_j\right)\right)^{n_j}\right], \tag{3.11}$$

Тогда выражение (3.6) примет вид:

$$W\left[A, N\right] = \sum_{j=1}^{M} C_j \cdot \left[1 - \left(1 - \left(G^{a_j} \cdot P_j\right)\right)^{n_j}\right], \tag{3.12}$$

При применении моделей, разработанных в п.п. 2.2, 2.3, значения $w_j\left[a_j, n_j\right]$ в (3.11), будут вычисляться как результат моделирования, т.е. $w_j\left[a_j, n_j\right] = RES(M)$. Схема алгоритма решения задачи (3.9) с учетом (3.12) представлена на рисунке 3.6.

Покажем применение алгоритма при исходных данных, приведенных в таблице 3.1, с учетом дополнительных исходных данных по средствам защиты (таблица 3.4).

Рисунок 3.6 – Схема алгоритма оценки ущерба, наносимого информации, на объекте с установленными средствами защиты

1. Ввод исходных данных (блок 1).

Таблица 3.4 – Исходные данные объекта защиты

Количество средств защиты	A=4
Вероятность преодоления	G=0,4
Размещение средств защиты	<a>=<0,2,1,1>

2. Расчет элементов матрицы частных ущербов (блок 2)

Таблица 3.5 – Матрица частных ущербов объекта защиты

$n\backslash w$	w_1	w_2	w_3	w_4
1	180	32	56	36
2	306	61,440	107,52	70,56
3	394,2	88,52	154,92	103,74
4	455,94	113,44	198,52	135,59
5	499	136	239	166
6	529	157	276	196

3. Расчет элементов матрицы приращений частных ущербов (блок 3)

Таблица 3.6 – Значения матрицы приращений ущерба

$n\backslash \Delta w$	Δw_1	Δw_2	Δw_3	Δw_4
1	180	32	56	36
2	126	2,44	51,52	34,56
3	88,2	27,085	47,398	33,178
4	61,74	24,918	43,607	31,851
5	43,218	22,925	40,118	30,576
6	21,177	19,403	33,956	28,179

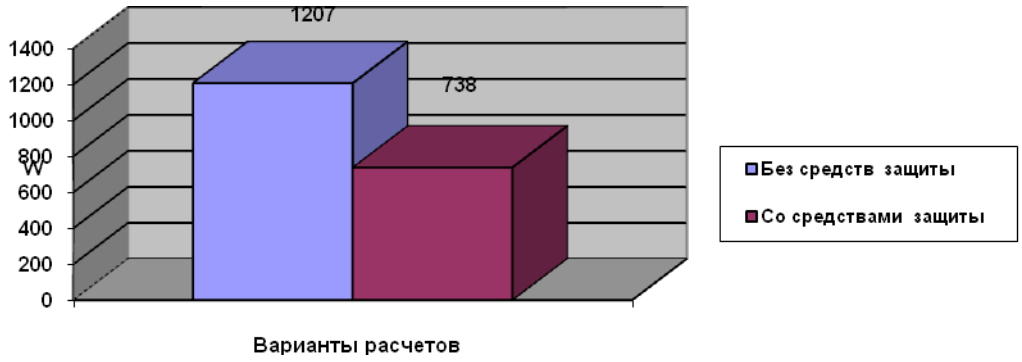
4. Нахождение оптимального, с точки зрения злоумышленника, распределения попыток воздействия (табл. 3.6):

$$n^* = \langle 5,0,5,0 \rangle$$

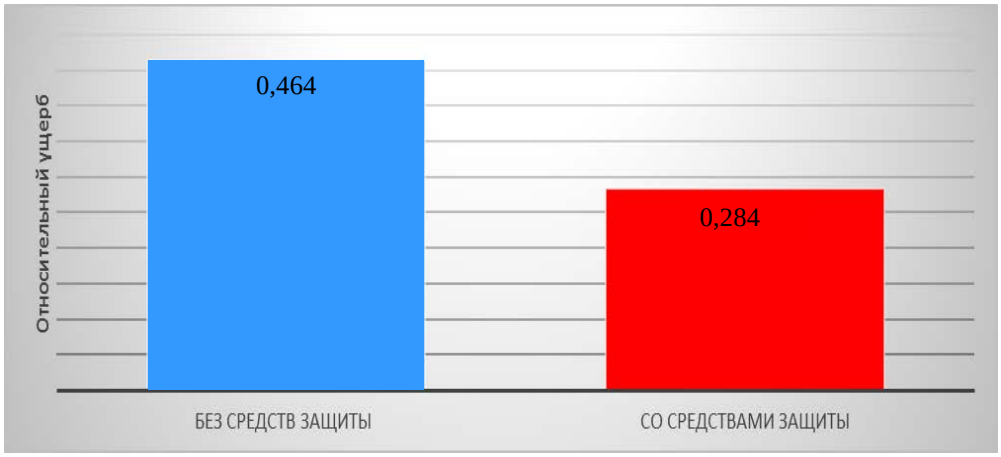
5. Вычисление суммарного вероятного ущерба, наносимого злоумышленником, при использовании оптимального распределения попыток воздействия (таблица 3.5)

$$W\left[n^*, a\right] = 737 \quad (0.284),$$

Сравнительные результаты расчетов для примеров п. 3.2.1 и п. 3.2.2 при одинаковых исходных данных по объекту защиты показаны на рисунке 3.7.



а)



б)

Рисунок 3.7 – Сравнительные результаты расчетов а) абсолютный ущерб, б) относительный ущерб

3.3 Методика оптимизации размещения средств защиты информации на ИОС

Результаты расчетов, полученные в п. 3.2.1 и п.3.2.2, наглядно демонстрируют возможности ущерба при применении специальных средств защиты.

Однако, характер изменения огибающих функций частных ущербов и их сепарабельной функции (рисунок 3.8), а также линейность ограничений, позво-

ляют сделать предположение, что добиться снижения ущерба, наносимого массивам информации, можно не только экстенсивным путем (увеличением числа и улучшением характеристик средств защиты), но и оптимизацией их размещения по каналам воздействия. Это предположение подтверждается результатами расчетов, выполненных методом полного перебора для исходных данных п. 3.2.1, 3.2.2 при всех возможных вариантах размещения средств защиты и приведенных на рисунке 3.9.

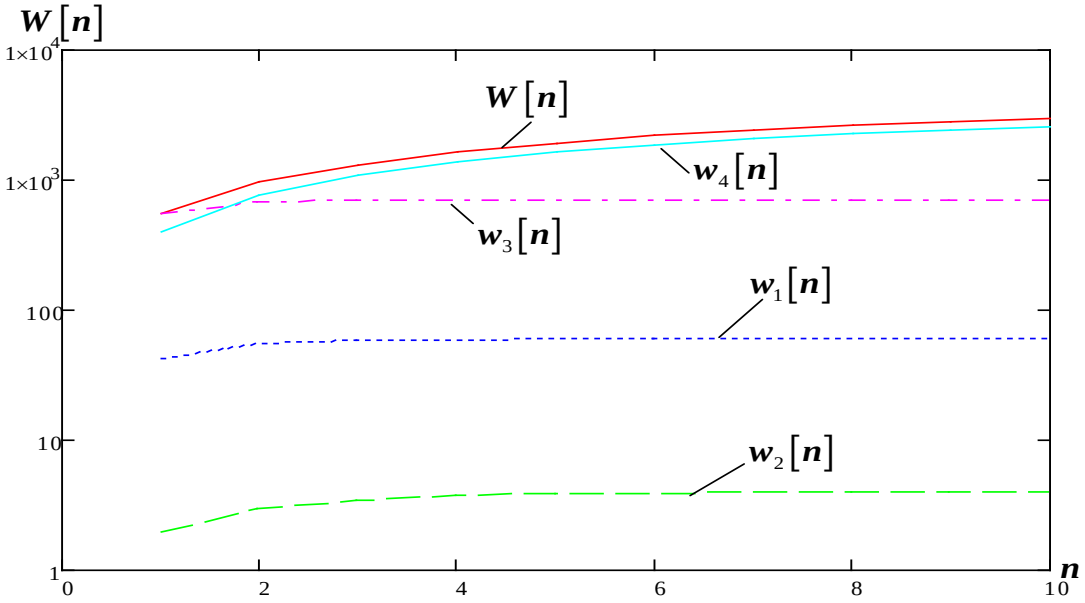


Рисунок 3.8 – Зависимость частных w_j и суммарного W вероятных ущербов от количества попыток воздействия n

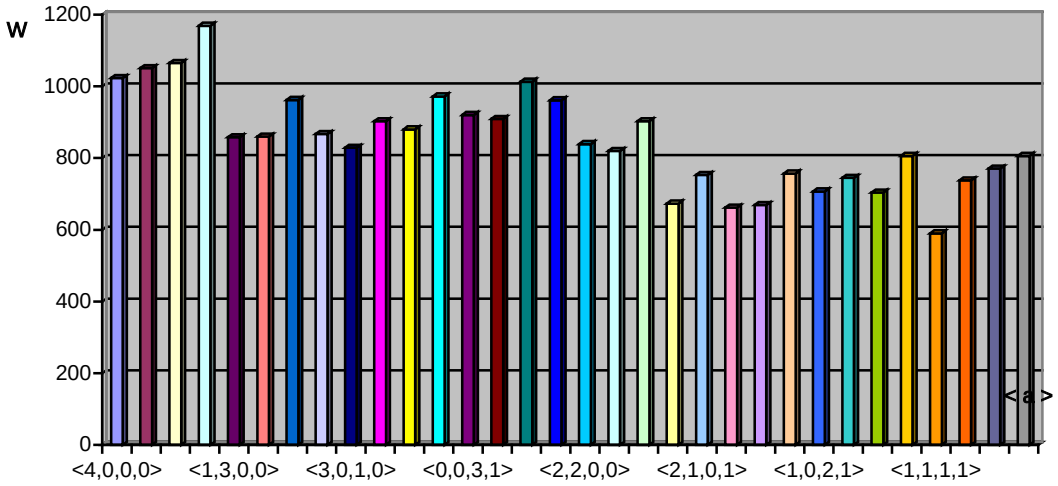


Рисунок 3.9 – Результаты расчетов методом полного перебора

Из анализа результатов (рисунок 3.9) следует, что величина ущерба W в зависимости от варианта размещения средств защиты при использованных исходных данных колеблется в пределах от 1169 (для <a> = <0,0,0,4>) до 590 (для <a> = <1,1,1,1>).

Таким образом, есть все основания полагать, что путем оптимизации размещения средств защиты по возможным (потенциальным) каналам воздействия, можно получить значительный (примерно в два раза) выигрыш в снижении ущерба, наносимого информации в хранимых массивах. При этом необходимо иметь ввиду, что средства защиты могут быть: однородными, для которых ($g_1=g_2=\ldots=g_i=\ldots=g_n=G$), и неоднородными ($g_1\neq g_2\neq\ldots\neq g_i\neq\ldots\neq g_n$). В свою очередь, и те, и другие могут быть: универсальными (размещаются на любой канал воздействия) и не универсальными (могут быть установлены только на определенный канал воздействия).

В связи с этим и при больших значениях M, A и N решение задачи (3.9) методом полного перебора становится весьма затруднительным и приводит к огромным затратам, что и обусловило разработку данной методики, имеющей четыре варианта: для всех сочетаний однородных и неоднородных, универсальных и не универсальных средств защиты информации.

3.3.1 Средства защиты универсальные и однородные

Данный вариант методики приведен на рисунке 3.10. Основу алгоритма составляет последовательность действий, описанная в п. 3.2.2. Покажем содержание варианта методики на контрольном примере.

1. Ввод исходных данных.

Исходные данные для исследуемого объекта А приведены в таблице 3.7. Ввиду того, что средства защиты однородные и универсальные, они имеют одинаковые характеристики ($g_1=g_2=g_3=g_4$) и могут быть размещены на любой канал воздействия, что отмечено в таблице 3.7 знаком √.

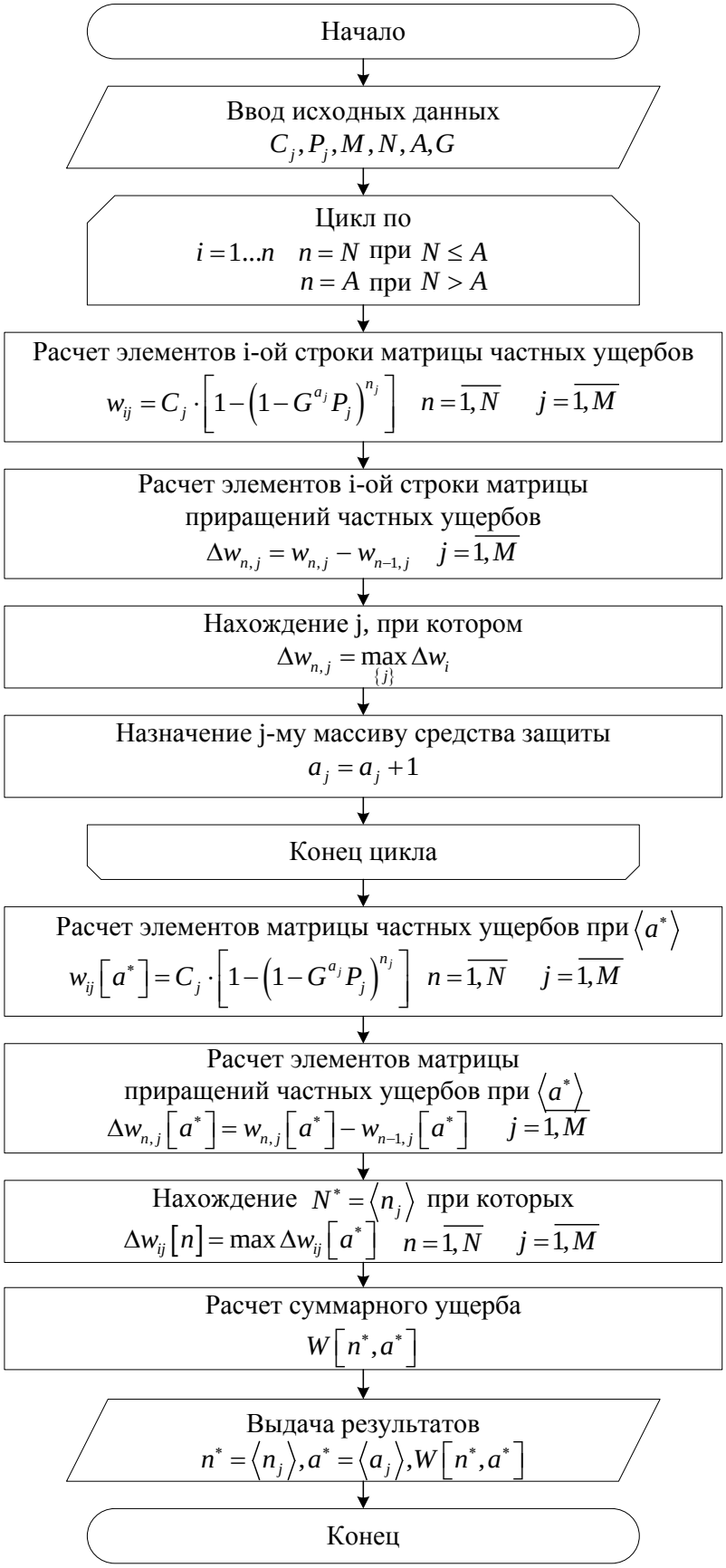


Рисунок 3.10 – Вариант методики оптимизации размещения универсальных и однородных средств защиты

Таблица 3.7 – Исходные данные объекта защиты

Количество защищаемых массивов информации	M=4			
	S_1	S_2	S_3	S_4
Относительная важность (C_j)	0,0126 (60)	8,396e-4 (4)	0,147 (700)	0,84 (4000)
Вероятность поражения (P_j)	0,7	0,5	0,8	0,1
Количество средств защиты	A=4			
Тип средств защиты	Однородные			
Вероятность преодоления	G=0,4			
Вариант установки	Универсальные			
Возможность установки на каналы воздействия	√	√	√	√
Количество попыток воздействия	N=10			

2. Расчет элементов первой строки матрицы частных ущербов по выражению (3.19) (блок 3).

№ попытки воздействия	Каналы воздействия			
	1	2	3	4
1	42	2	90	64

3. Расчет элементов первой строки матрица приращений ущербов по выражению $\Delta w_{n,j} = w_{n,j} - w_{n-1,j} \quad j = \overline{1,M}$ (блок 4).

№ попытки воздействия	Каналы воздействия			
	1	2	3	4
1	42	2	90	64

4. Расчет элементов первой строки матрицы частных ущербов по выражению (3.19) (блок 3).

№ попытки воздействия	Каналы воздействия			
	1	2	3	4
1	42	2	90	64

5. Расчет элементов первой строки матрица приращений ущербов по выражению $\Delta w_{n,j} = w_{n,j} - w_{n-1,j} \quad j = \overline{1,M}$ (блок 4).

№ попытки воздействия	Каналы воздействия			
	1	2	3	4
1	42	2	90	64

6. Нахождение канала воздействия на информационные массивы, при котором прирост ущерба на данном шаге максимален (блок 5).

№ попытки воздействия	Каналы воздействия			
	1	2	3	4
1	42	2	90	64

7. Размещение средства защиты на найденный канал воздействия (блок 6).

	Каналы воздействия			
	1	2	3	4
Размещение СЗИ				

8. Повторение п. 2 - 5 до распределения всех средств защиты (получение <*a**>).

	W			
	1	2	3	4
1	42	2	90	64
2	55	3	168	127
3	58	4	236	189
4	60	4	295	250
5	60	4	347	310
6	60	4	392	369
7	60	4	432	427
8	60	4	466	484
9	60	4	496	540
10	60	4	522	596

ΔW			
1	2	3	4
42	2	90	64
12,6	1	78,131	62,976
3,78	0,5	68,13	61,968
1,134	0,25	59,41	60,977
0,34	0,125	51,805	60,001
0,102	0,063	45,174	59,041
0,034	0,031	39,392	58,097
0,009	0,016	34,350	57,167
0,003	0,008	29,953	56,252
0,001	0,004	26,119	55,352

9. Получение <n^*> в соответствии с п.3.2.2.

$$<n^*> = <0,0,4,6>$$

10. Расчет суммарного вероятного ущерба, наносимого объекту защиты, защищенному специальными средствами, расставленными по плану <a^*> в соответствии с оптимальным, для злоумышленника, планом воздействия <n^*>.

$$W[n^*,a^*] = 664$$

Таким образом, система защиты на некотором абстрактном объекте для исходных данных табл. 3.7 примет вид, показанный на рисунке 3.11.

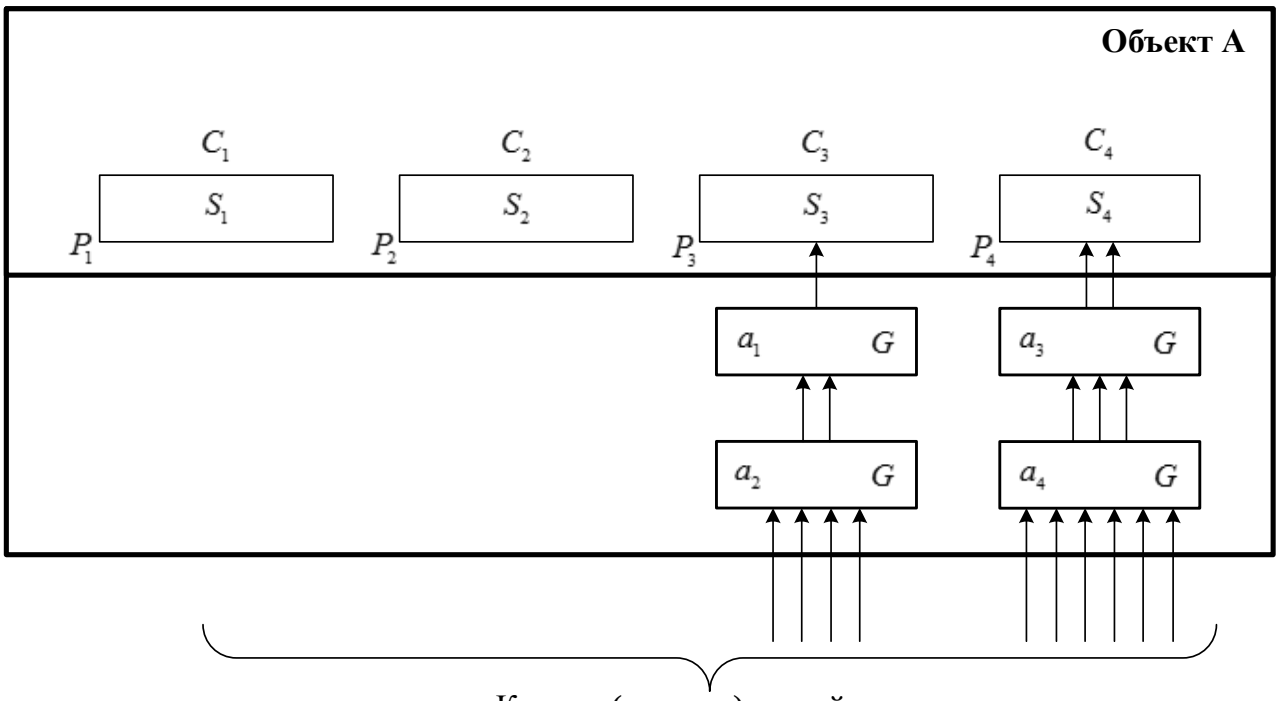


Рисунок 3.11 – Система защиты объекта с оптимально размещенными однородными и универсальными средствами защиты

3.3.2 Средства защиты универсальные и неоднородные

Данный вариант методики в форме алгоритма приведен на рисунке 3.12.

Учитывая, что в этом варианте используются средства защиты различных типов, то $g_1 \neq g_2 \neq g_3 \neq ... \neq g_i$.

Рисунок 3.12 – Вариант методики оптимизации размещения универсальных и неоднородных средств защиты

При этом для *i*-го канала воздействия

$$G^{(i)} = \prod_{i=1}^{l} g_i \tag{3.13}$$

и выражение (3.12) примет вид:

$$W\left[A,N\right] = \sum_{j=1}^{M} C_j \cdot \left[1 - \left(1 - \left[\prod_{i=1}^{l} g_i^{k_{i,j}}\right] \cdot P_j\right)^{n_j}\right] \tag{3.14}$$

где:

l – количество типов средств защиты;

g_i – вероятность преодоления средства защиты i-го типа;

$k_{i,j}$ – количество средств защиты i-го типа на j-м канале воздействия.

В связи с этим в алгоритм, рассмотренный в п. 3.3.1, добавлена процедура начальной сортировки массива имеющихся средств защиты по возрастанию вероятности их преодоления. Кроме этого изменено содержание блока 6 (рисунок 3.10) размещения средств защиты по каналам воздействия с учетом приоритетного размещения средств с наименьшей вероятностью преодоления.

Результат размещения средств защиты будет представлять собой не вектор, а матрицу оптимального размещения

$$\left|A\right| = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1M} \\ a_{21} & a_{22} & \ldots & a_{2M} \\ \ldots & \ldots & \ldots & \ldots \\ a_{L1} & a_{L2} & \ldots & a_{LM} \end{vmatrix}, \tag{3.15}$$

где M – количество каналов воздействия;

L – количество типов средств защиты.

В остальном последовательность действий по распределению универсальных и неоднородных средств защиты соответствует процедуре, описанной в п. 3.3.1. Для исходных данных таблицы 3.7 с учетом дополнений таблицы 3.8

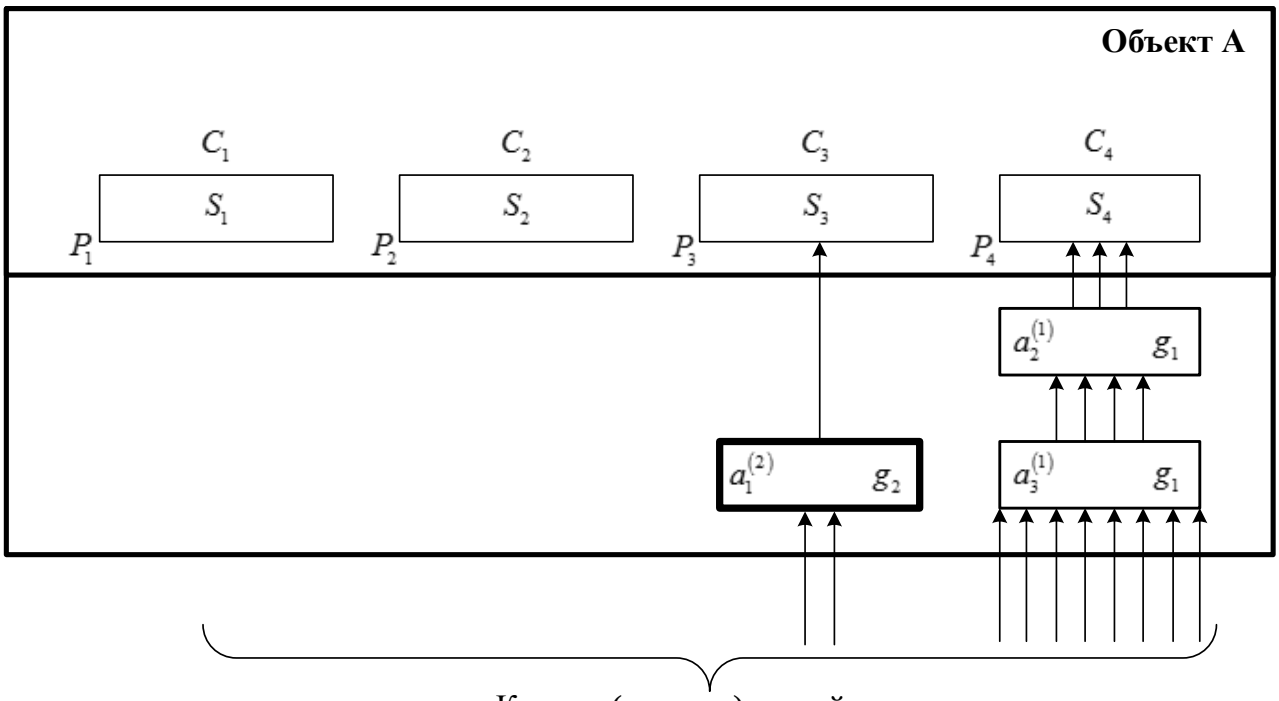


Рисунок 3.13 – Система защиты объекта с оптимально размещенными неоднородными и универсальными средствами защиты

Таблица 3.8 – Дополнительные исходные данные объекта защиты

Тип средств защиты	Неоднородные	
Количество типов средств защиты	*L = 2*	
Тип средства защиты	**1**	**2**
Вероятность преодоления	0,6	0,4
Количество	2	1

получены следующие результаты:

|a*| =	Тип средств защиты	Каналы воздействия			
		1	**2**	**3**	**4**
	1	0	0	0	2
	2	0	0	1	0

При <*n**> = <0, 0, 2, 8> - *W*[*n**,*a**] = 1393 и система защиты на исследуемом объекте А примет вид, показанный на рисунке 3.13.

3.3.3 Средства защиты не универсальные и однородные

Учитывая, что используемые в данном варианте средства защиты не являются универсальными, то в дополнение к исходным данным п. 3.3.1 необходимо добавить дополнительные ограничения – вектор-строку:

$$U = \langle u_1, u_1, ..., u_M \rangle, \tag{3.16}$$

элементы которого $u_j = \begin{cases} 0 \\ 1 \end{cases} j = \overline{1, M}$ в зависимости от возможности (невозможности) размещения средства защиты на *j*-й канал воздействия.

Так как средства защиты в данном варианте методики однородны, то целевая функция остается в виде (3.11). Вариант методики в форме алгоритма приведен на рисунке 3.14.

В отличие от варианта (рисунок 3.10) в исходные данные добавлено ограничение (3.16) и изменено содержание блока 6: перед размещением i-го средства защиты на j-й канал воздействия осуществляется проверка возможности использования его для закрытия данного канала ($u_j=1$). В остальном последовательность действий по распределению однородных и не универсальных средств защиты соответствует описанному в п. 3.3.1. При этом, для исходных данных таблицы 3.7 с учетом дополнения (таблица 3.9) получены следующие результаты: <*a**>=<0,0,0,4>, <*n**>=<2,0,3,5>, *W[n*,a*]=800*.

Таблица 3.9 – Дополнительные исходные данные объекта защиты

	Каналы воздействия			
Возможность установки по каналам воздействия	1	2	3	4
	1	0	0	1

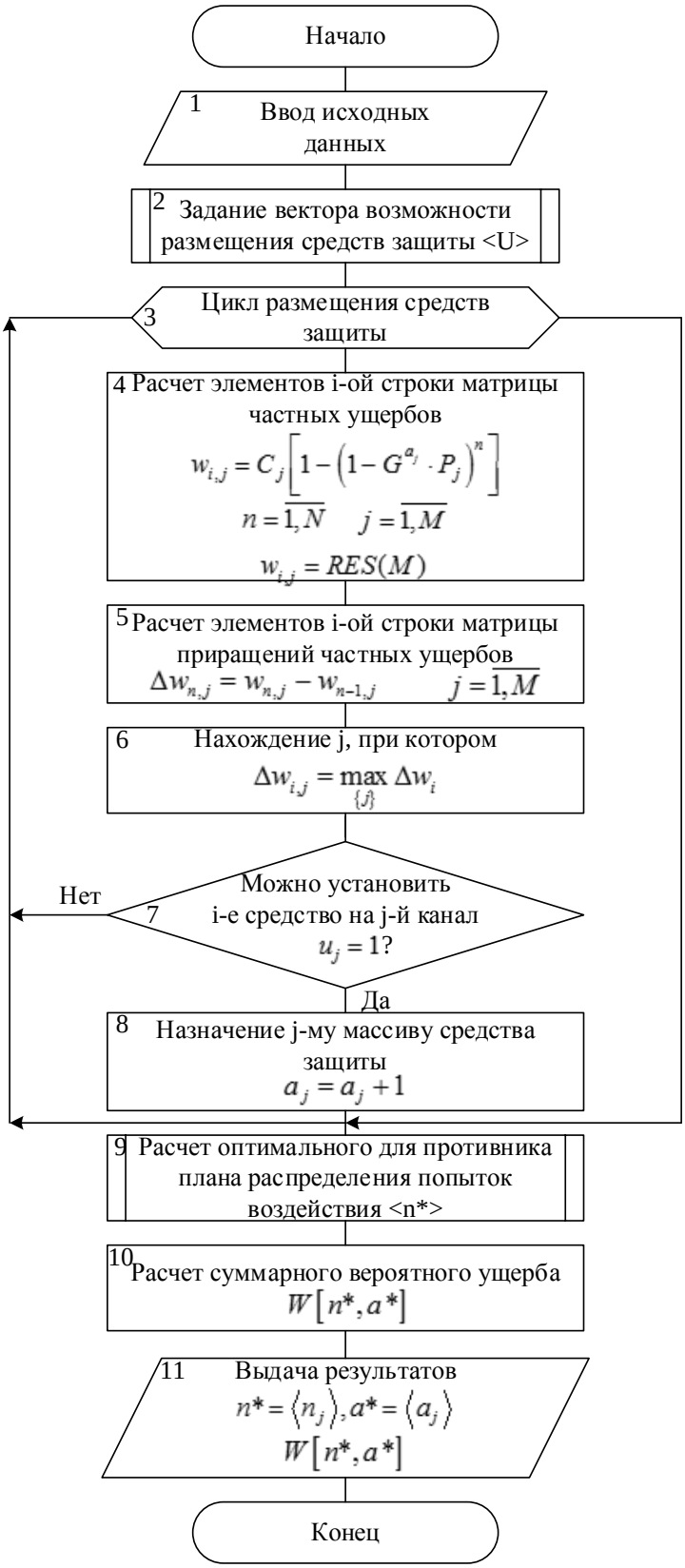


Рисунок 3.14 – Вариант методики оптимизации размещения не универсальных и однородных средств защиты

Таким образом, система защиты на исследуемом объекте А примет вид, показанный на рисунке 3.15.

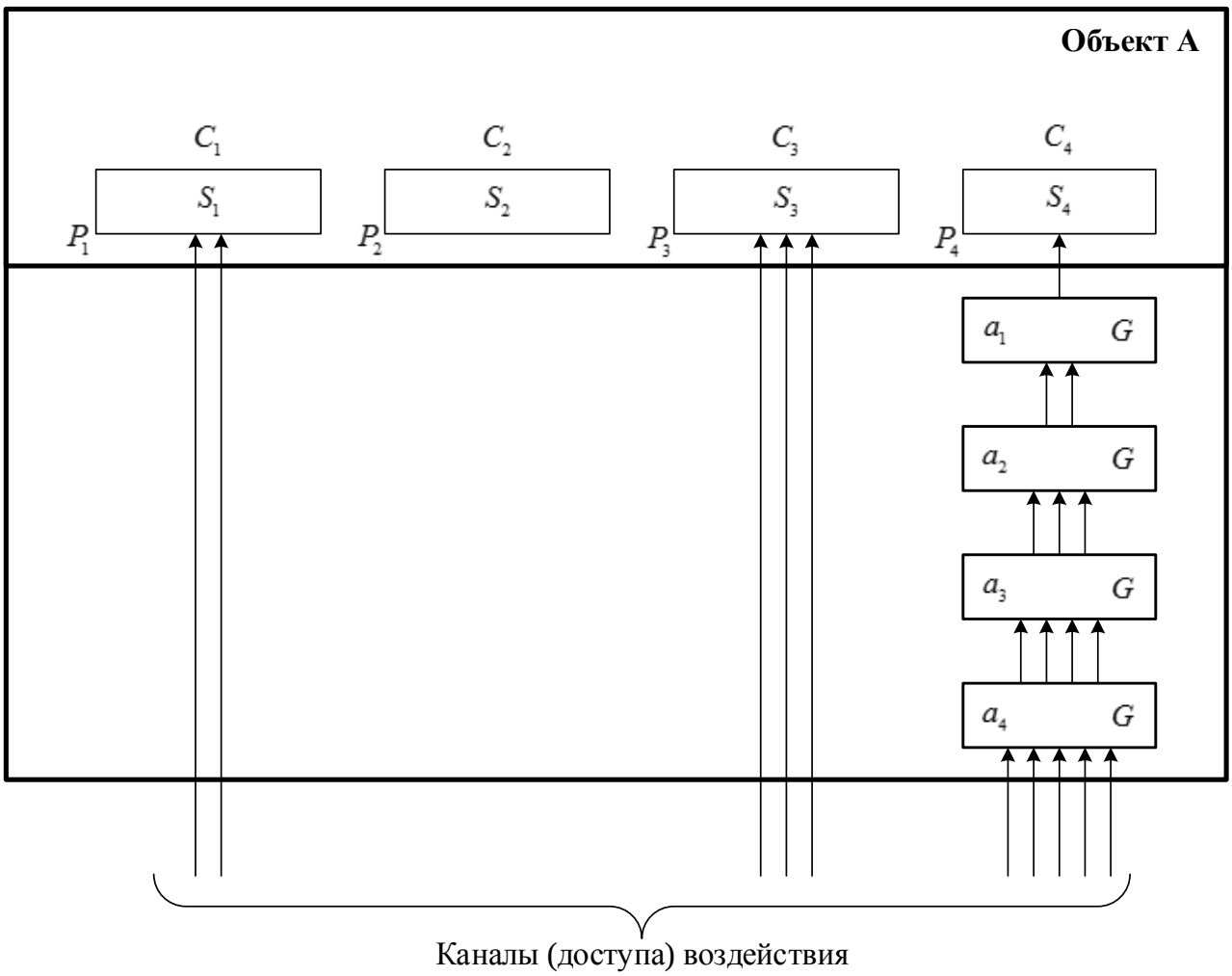


Рисунок 3.15 – Система защиты объекта с оптимально размещенными не универсальными и однородными средствами защиты

3.3.4 Средства защиты неоднородные и не универсальные

Учитывая, что используемые в данном варианте средства защиты не являются ни универсальными, ни однородными, в качестве дополнительных данных выступает совокупность ограничений (3.15) и изменений (3.13), (3.14), в результате которых вектор-строка (3.16) преобразуется в матрицу:

$$|U_1| = \begin{vmatrix} u_{11} & u_{12} & \dots & u_{1M} \\ u_{21} & u_{22} & \dots & u_{2M} \\ \dots & \dots & \dots & \dots \\ u_{L1} & u_{L2} & \dots & u_{LM} \end{vmatrix} \qquad (3.17)$$

где $u_{ij} = \begin{cases} 0 \\ 1 \end{cases} i = \overline{1,L},\ j = \overline{1,M}$.

Так как средства защиты в данном варианте методики неоднородны, то в качестве целевой функции будет выступать выражение (3.14). Вариант методики в форме алгоритма приведен на рисунке 3.16.

В отличие от варианта (рисунок 3.12), в исходные данные добавлено следующее: ограничение (3.17), процедура получения матрицы приоритетов расстановки средств защиты по каналам воздействия (блок 4) и изменено содержание блока 8: перед размещением средства защиты *i*-го типа на *j*-й канал воздействия осуществляется проверка возможности использования его для закрытия данного канала ($u_{ij}=1$). Если такая возможность отсутствует ($u_{ij}=0$), выбирается следующий по приоритету (с наименьшей вероятностью преодоления) тип средств защиты.

Таблица 3.10 – распределение СЗИ по объектам защиты

Возможность установки по каналам воздействия	Тип средств защиты	Каналы воздействия			
		1	2	3	4
	1	0	1	0	1
	2	0	0	0	1

В остальном последовательность действий по распределению неоднородных и не универсальных средств защиты соответствует описанному в п.3.3.2, 3.3.3.

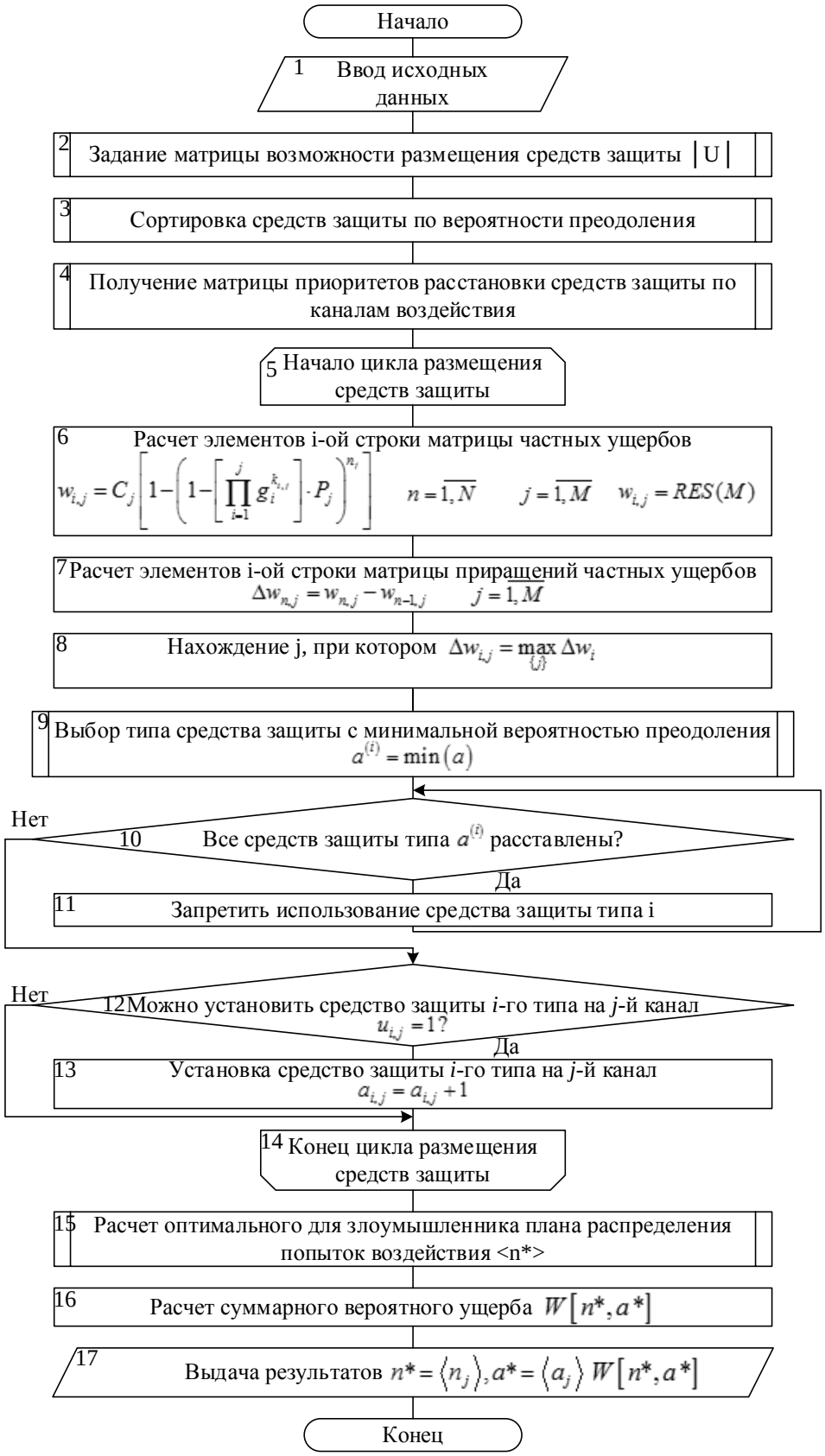


Рисунок 3.16 – Вариант методики оптимизации размещения не универсальных и неоднородных средств защиты

Для исходных данных таблицы 3.7 с учетом дополнения таблицы 3.8 и таблицы 3.10 получены следующие результаты:

$\lvert n^* \rvert =$	Тип средств защиты	Каналы воздействия			
		1	2	3	4
	1	0	0	0	2
	2	0	0	0	1

При $<n^*>=<0,0,2,8>$, $<a^*>=<0,0,0,4>$, $W[n^*,a^*]=1110$.

Таким образом, система защиты на исследуемом объекте примет вид, показанный на рисунке 3.17.

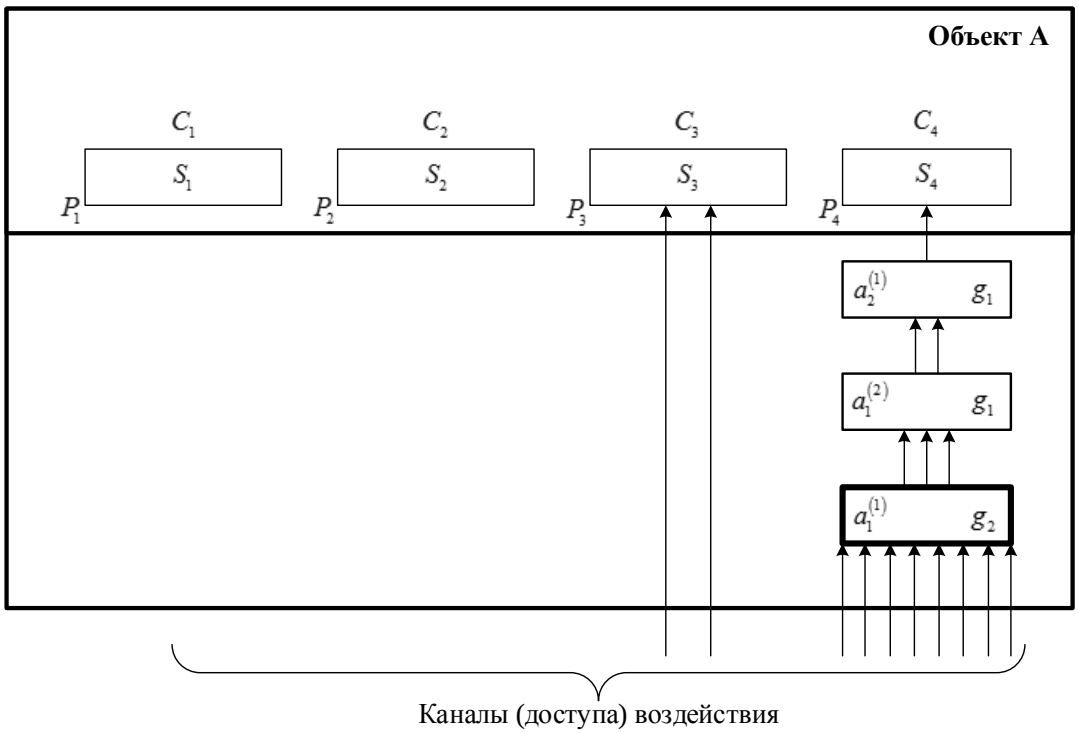


Рисунок 3.17 – Система защиты информации с оптимально размещенным и неоднородными и не универсальными средствами защиты

Обобщая все варианты, представим методику оптимизации размещения средств защиты на ИОС ИТС в виде, изображенном на рисунке 3.18.

Формальность процессов оптимизации размещения средств защиты на объекте хранения информации позволяет, а возрастающая в зависимости от качества хранимых массивов, средств защиты, их характеристик, числа попыток

воздействия и т.д., сложность расчетов, настоятельно требуют перехода от ручных методов расчета к их программной реализации.

Рисунок 3.18 – Методика оптимизации размещения средств защиты на ИОС

3.4 Программная реализация разработанной методики

Разработанная методика может быть использована на двух этапах:

1) *при отсутствии средств защиты* – для оценки необходимости их приобретения, расчета требуемого количества, выбора характеристик и последующего размещения;

2) *при наличии некоторого набора средств защиты* – для оценки необходимости совершенствования существующих систем защиты путем оптимизации их размещения.

Таким образом, при выполнении обоих этапов возникает проблема выбо-

ра. При этом принципиальным является решение вопроса о том – с чем сравнивать полученные оценочные результаты:

1) с результатами оценки при отсутствии средств защиты для оценки целесообразности их приобретения;

2) с результатами оценки существующей системы – для определения целесообразности совершенствования системы защиты;

3) с требуемыми значениями выбранных показателей защищенности;

4) с результатами оценки варианта размещения, выбранного методом:

экспертных оценок ("умозаключительным" методом);

тривиальным методом (равномерным размещением средств защиты без учета характеристик хранимых массивов.

Исходя из этого, к разрабатываемому программному средству должны быть предъявлены следующие требования [44, 45]:

1) результаты работы программного средства должны иметь количественное представление выбранных показателей (вектор-строку ($<a>$) или матрицу($|\ a\ |$) размещения средств защиты по каналам воздействия, вектор оптимального распределения попыток воздействия $< n^* >$, значение величины суммарного вероятного ущерба – $W[n,a]$);

2) возможность осуществления сравнительного анализа результатов оценки (без средств защиты, с их тривиальным, умозаключительным и оптимальным размещением);

3) программное средство должно выдавать графическое представление целевых функций в зависимости от количества попыток воздействия – N;

4) программное средство должно позволять оптимально распределять однородные, неоднородные, универсальные, не универсальные средства защиты и их комбинации.

В соответствии с этими требованиями и рекомендациями разработано программное средство, позволяющее автоматизировано решать задачу оптимального размещения средств защиты. Данное средство создано на основе разработанной методики оптимизации размещения средств защиты и включает ва-

рианты, изображенные на рисунках 3.10, 3.12, 3.14 и 3.16. Оно создано на языке C++ в среде визуального программирования C++.

Основной экран разработанного программного средства представлен на рисунке 3.19.

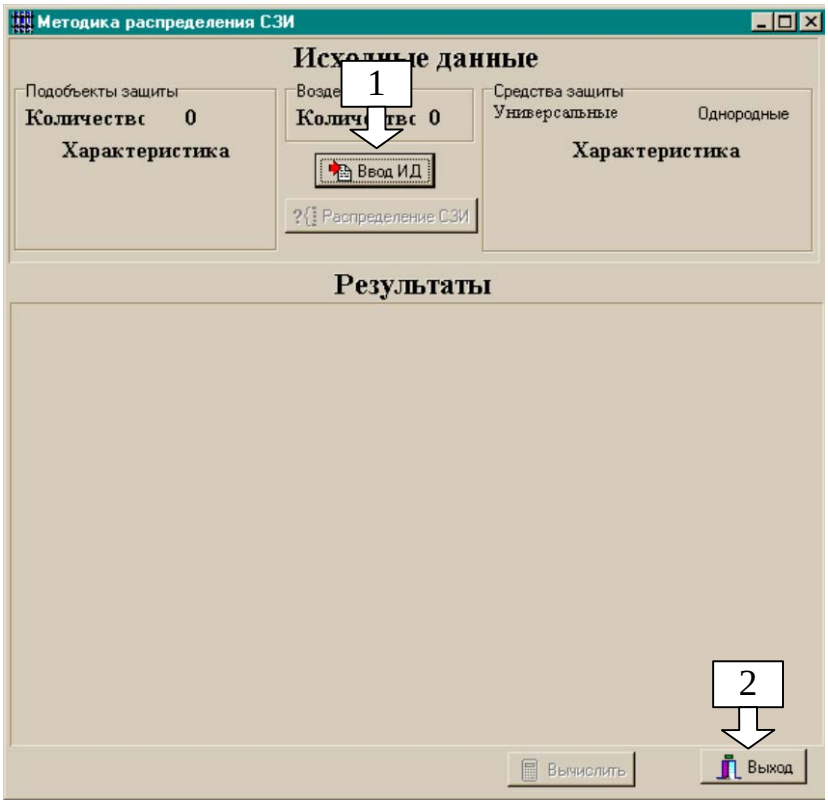


Рисунок 3.19 – Основной экран программного средства оптимизации размещения средств защиты

Для ввода исходных данных предназначена кнопка "Ввод ИД" (1). При ее нажатии открывается окно ввода исходных данных (рисунок 3.20). Ввод исходных данных предусматривает задание начальных значений для защищаемых информационных массивов (3), специальных средств защиты, установленных (либо предполагаемых для установки) на объекте защиты (4), и количества попыток воздействия, которые может предпринять противник (5).

В качестве исходных данных, описывающих защищаемые информационные массивы выступают:

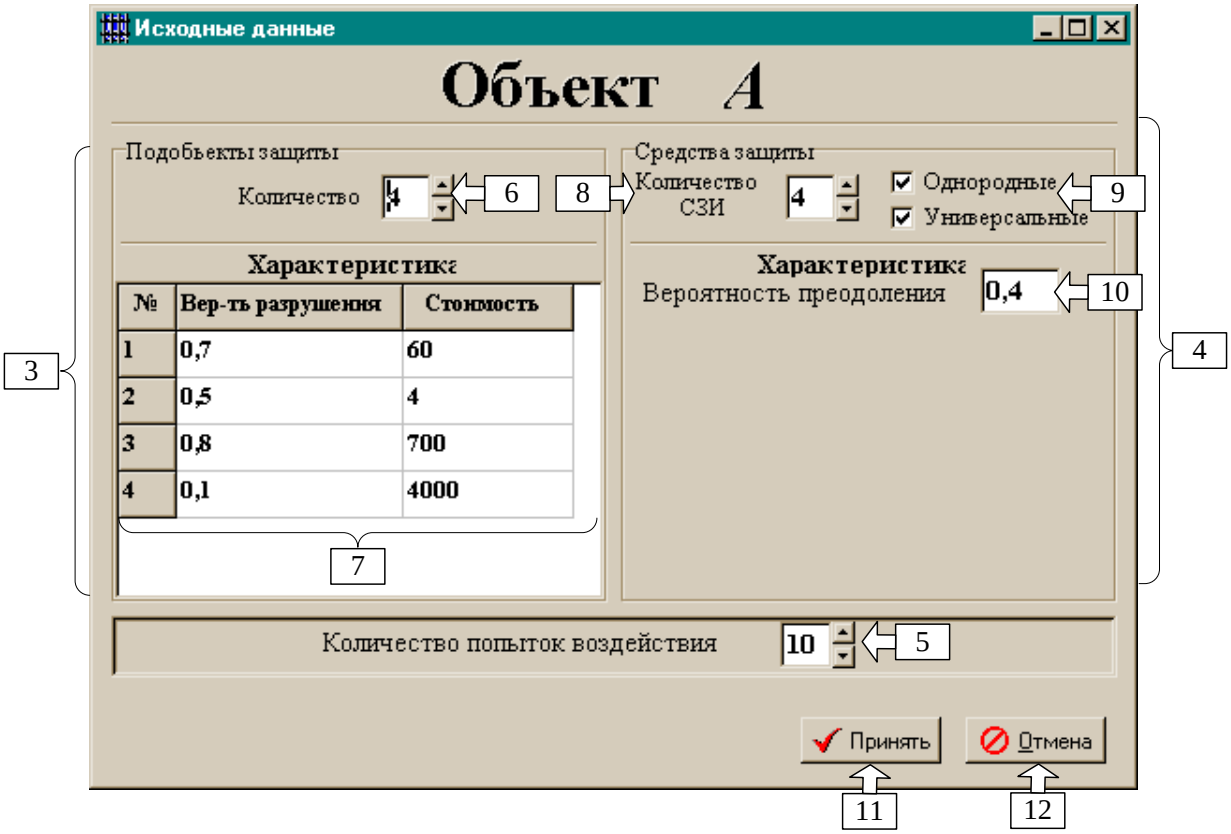


Рисунок 3.20 – Окно ввода исходных данных

1) количество массивов, подлежащих защите (6);

2) характеристики каждого массива (P_j , C_j) сведенные в таблицу (7).

Основным исходным данным, описывающим средства защиты, является вид средств защиты, который может принимать значения:

а) однородные и универсальные; б) неоднородные и универсальные;

в) однородные и не универсальные; г) неоднородные и не универсальные.

Вид задается независимыми переключателями (9). При установленном переключателе средствам назначается соответствующий вид, при сброшенном переключателе противоположный.

Рассмотрим работу программного средства при использовании однородных и универсальных средств защиты. Для подтверждения введенных данных и возвращения в основное окно программы предназначена кнопка "Принять"(11), для отказа от них – кнопка "Отмена" (12).

После задания исходных данных они отображаются в верхней части основного окна программы рисунка 3.21.

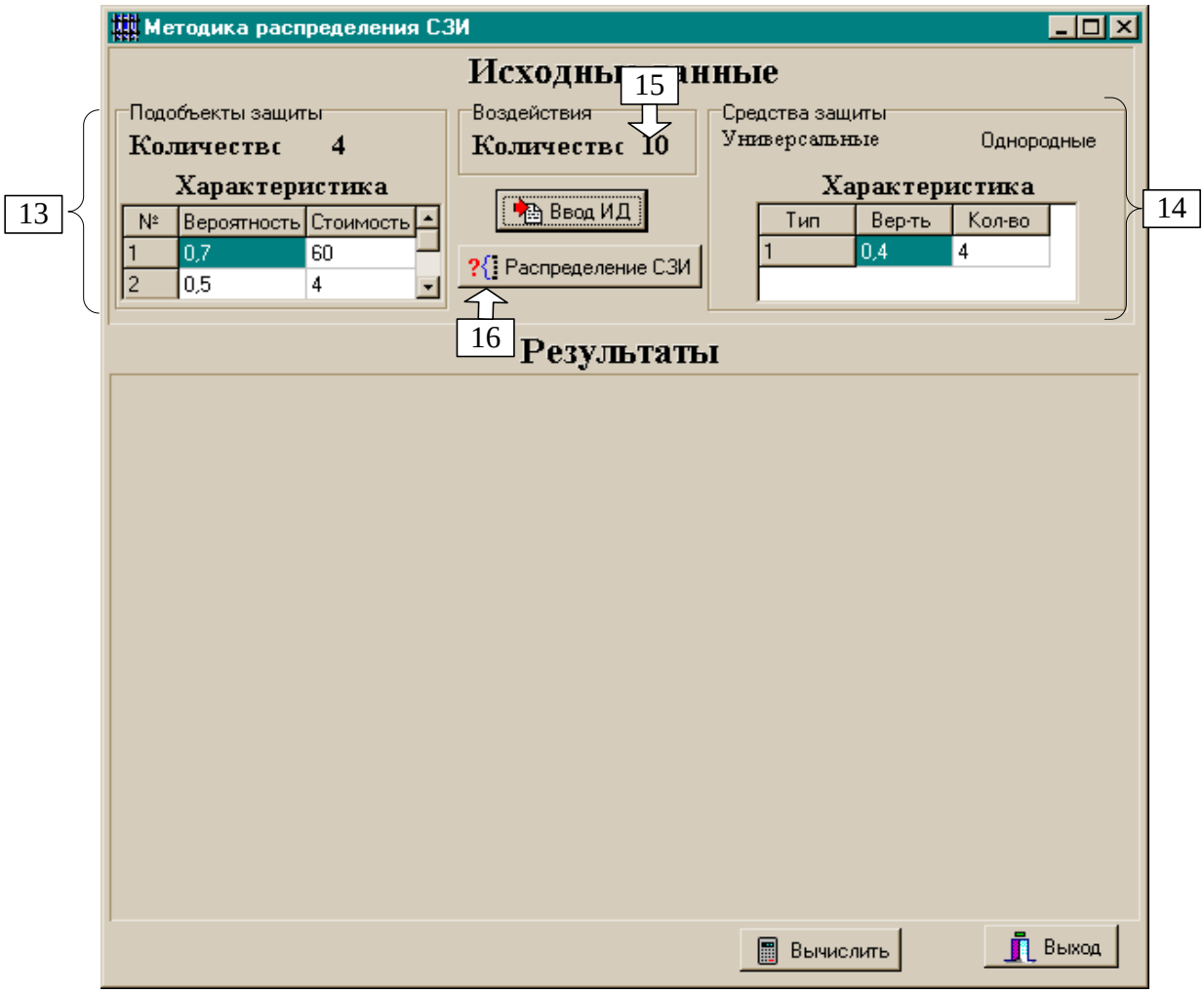


Рисунок 3.21 – Основной экран программы с заданными исходными данными при использовании однородных и универсальных средств защиты

После ввода исходных данных, необходимо перейти к следующему этапу – "умозаключительному" распределению средств защиты по каналам воздействия (нажать кнопку "Распределение СЗИ" (16)). Внешний вид экрана данного этапа представлен на рисунке 3.22.

Распределение производится путем указания количества средств защиты, устанавливаемых на каждый канал воздействия (18). Если программное средство используется для проверки целесообразности совершенствования существующей системы защиты, тогда вводится действительное размещение средств защиты на объекте, в противном случае (система защиты только созда-

ется) указывается их предполагаемое размещение, полученное путем экспертных оценок (опорный вариант).

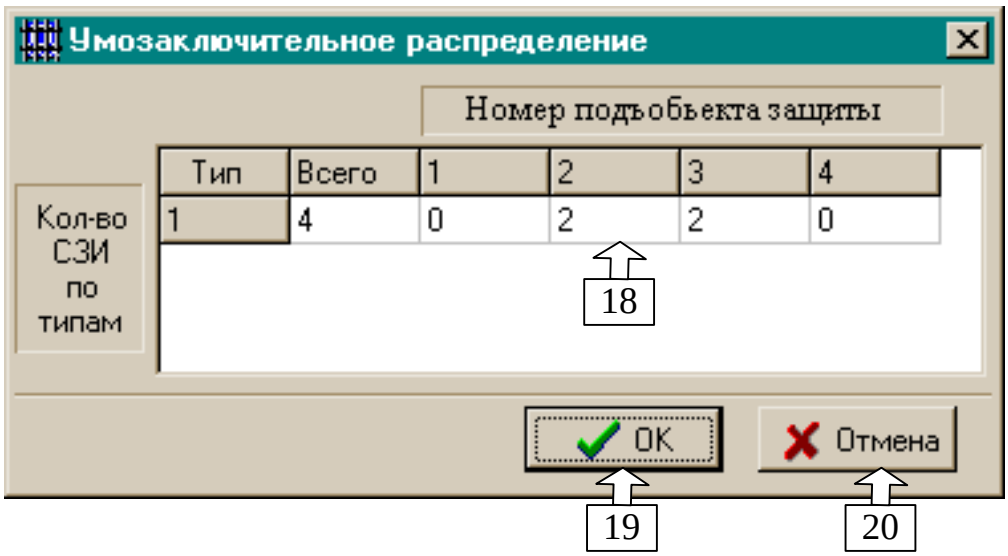


Рисунок 3.22 – Экран "умозаключительного" распределения однородных и универсальных средств защиты.

Подтверждение введенных данных осуществляется нажатием кнопки "ОК" (19), для отмены предназначена кнопка с соответствующим названием (20).

На этом этапы подготовки данных заканчиваются, и по нажатию кнопки "Вычислить" (17) (рисунок 3.21), производится запуск расчетов. Сравнительные результаты расчетов выводятся в нижней части основного экрана (рисунок 3.23).

В качестве результатов выступают данные, полученные в процессе расчетов при воздействии противника на информационные массивы, хранящиеся на объекте без средств защиты и с системой защиты, в которой средства защиты расположены по тривиальному, "умозаключительному" и оптимальному (рассчитанному по разработанной методике) плану распределения. В зависимости от выбранной закладки (23), (24), (25), результаты могут быть представлены в трех вариантах:

1) обобщенные (рисунок 3.23). В данном варианте представлены сравнительные результаты суммарного вероятного ущерба, наносимого объекту защиты в числовом виде (21) и в виде диаграмм (22).

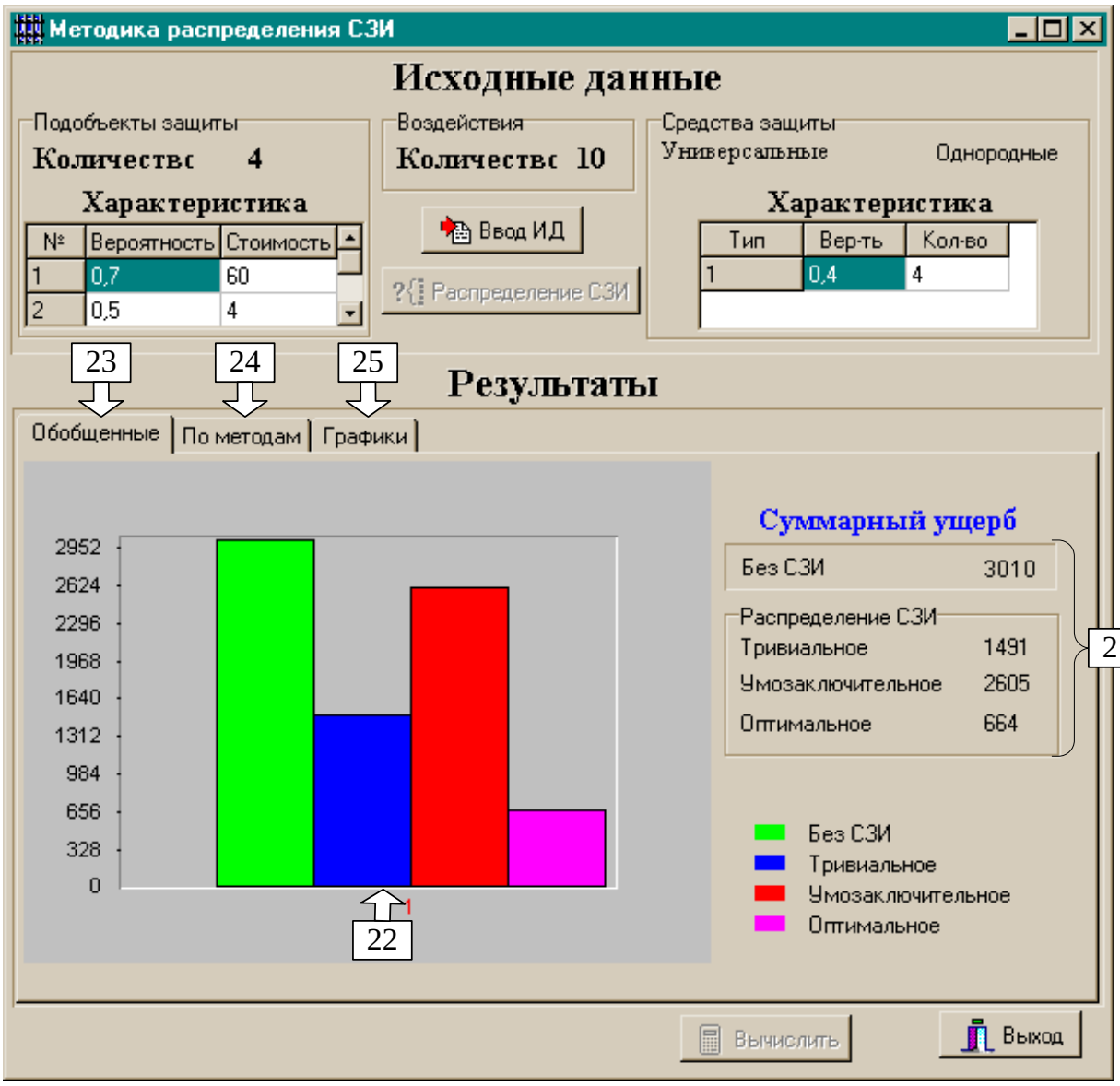


Рисунок 3.23 – Основной экран программного средства с результатами расчетов

2) по методам распределения средств защиты (рисунок 3.24). В данном варианте представлены полные результаты расчетов по каждому из методов распределения средств защиты. Указывается план распределения средств защиты <*a*> (27), оптимальный план распределения попыток воздействия противника <*n**> при данном варианте размещения средств защиты (29), матрицы частных ущербов (28) и приращений частных ущербов (30). Выбор метода размещения средств защиты, по которому выводятся данные, осуществляется с помощью зависимого переключателя "Метод" (26).

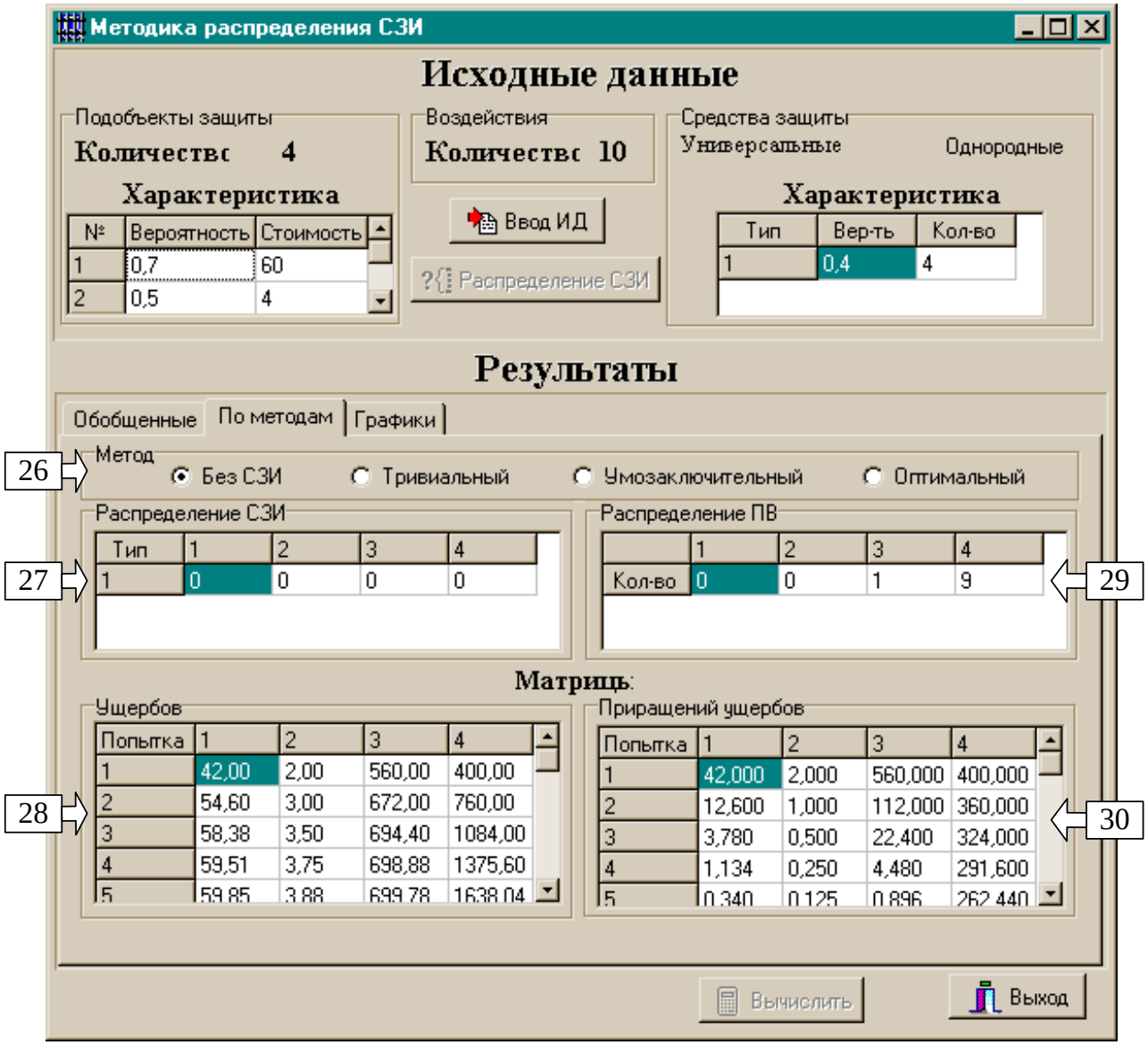


Рисунок 3.24 – Результаты расчетов по методам распределения средств защиты

3) по графическим представлениям функций суммарного ущерба, наносимого объекту защиты в зависимости от попыток воздействия (рисунок 3.25).

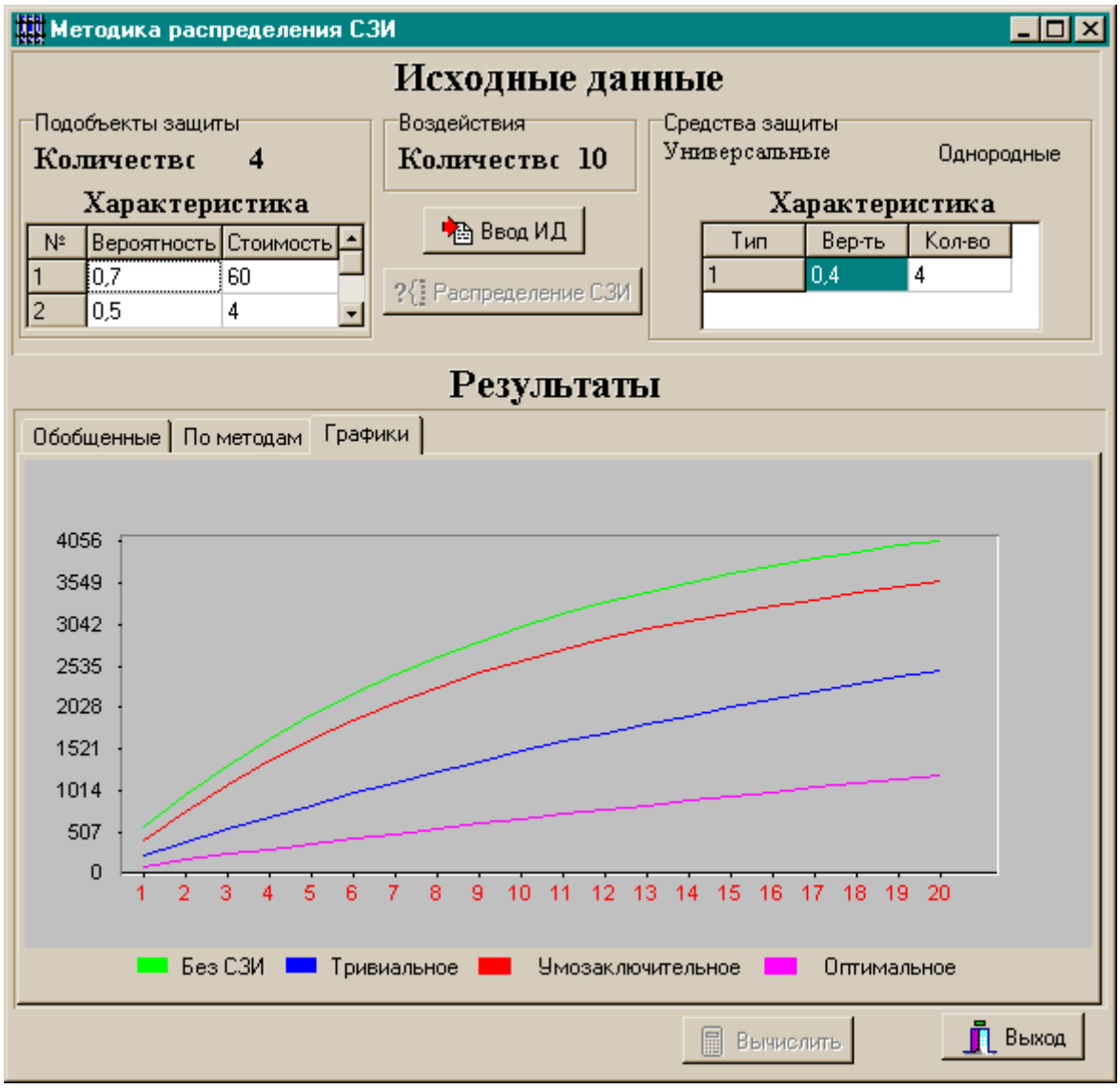


Рисунок 3.25 – Графическое представление функций суммарного вероятного ущерба, наносимого объекту защиты

В связи с особенностями применения неоднородных и универсальных средств защиты, рассмотренных в п. 3.3.2, работа программного средства оптимизации размещения средств защиты изменится.

Внешний вид экрана ввода исходных данных при использовании неоднородных и универсальных средств защиты примет вид, показанный на рисунке 3.26.

Вместо ввода количества средств защиты (8) рисунке 3.20, указывается количество типов средств защиты (31), а для ввода их характеристик используется таблица (32), для реализации дополнения (3.21) п.3.3.2.

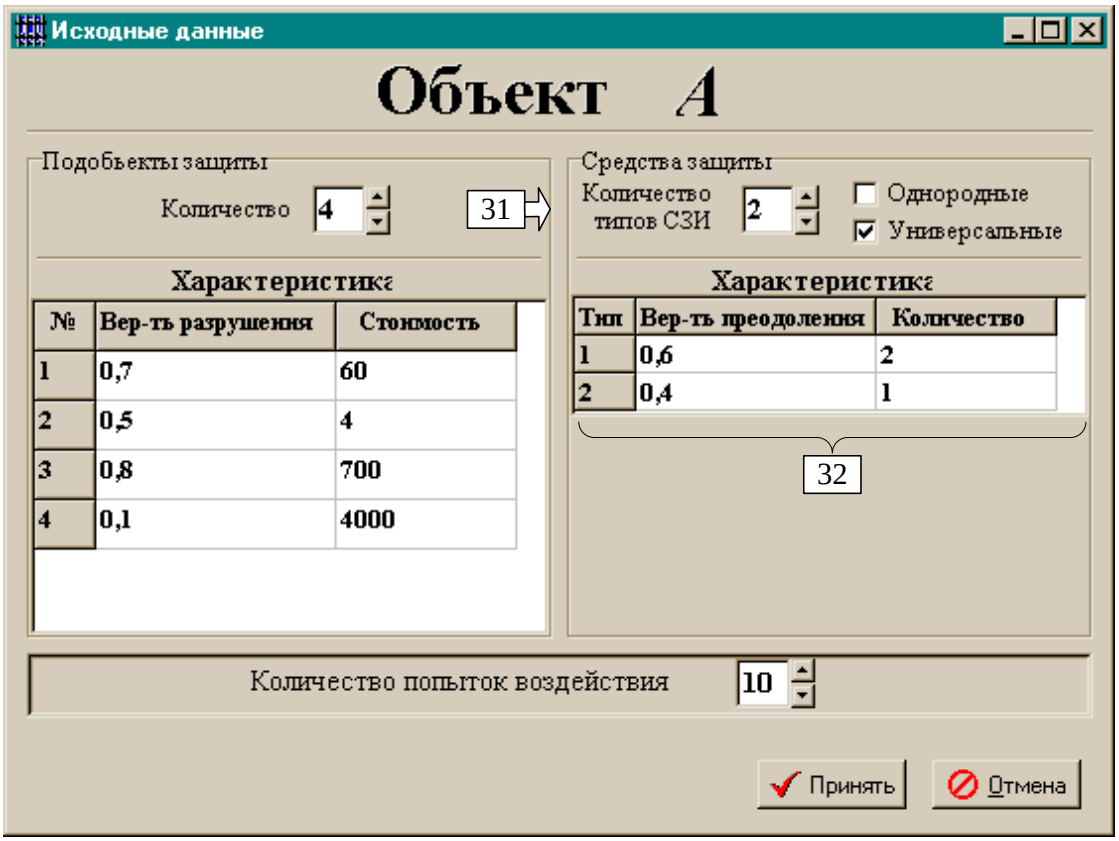


Рисунок 3.26 – Ввод исходных данных для неоднородных и универсальных средств защиты

В связи с появлением различных типов средств защиты претерпел изменение и этап "умозаключительного" распределения. Внешний вид экрана этого этапа для неоднородных и универсальных средств защиты представлен на рисунке 3.27.

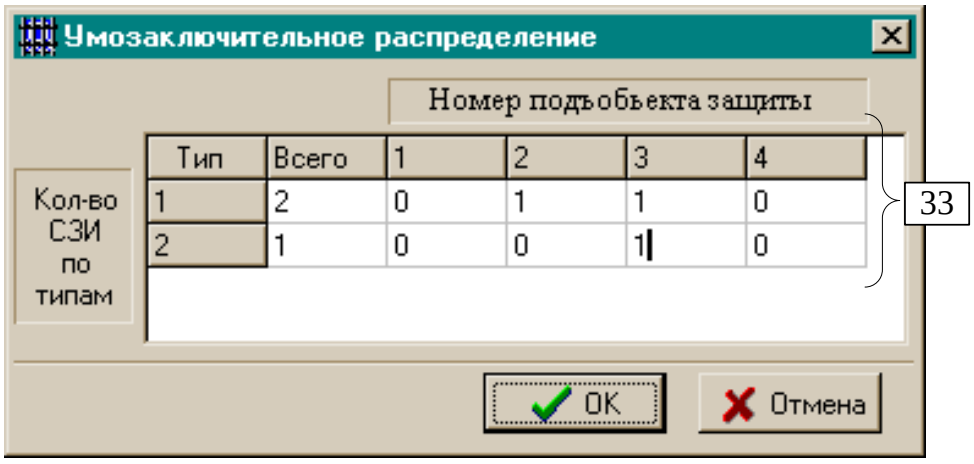


Рисунок 3.27 – "Умозаключительное" распределение неоднородных и универсальных средств защиты

Ввод матрицы (3.15) осуществляется с помощью таблицы (33). В связи с этим изменяется и вид основного экрана (рисунок 3.28), где характеристики средств защиты сведены в таблицу (34).

Принимая во внимание (3.15), результаты распределения неоднородных средств защиты также представляются в виде таблицы (35) рисунок 3.28.

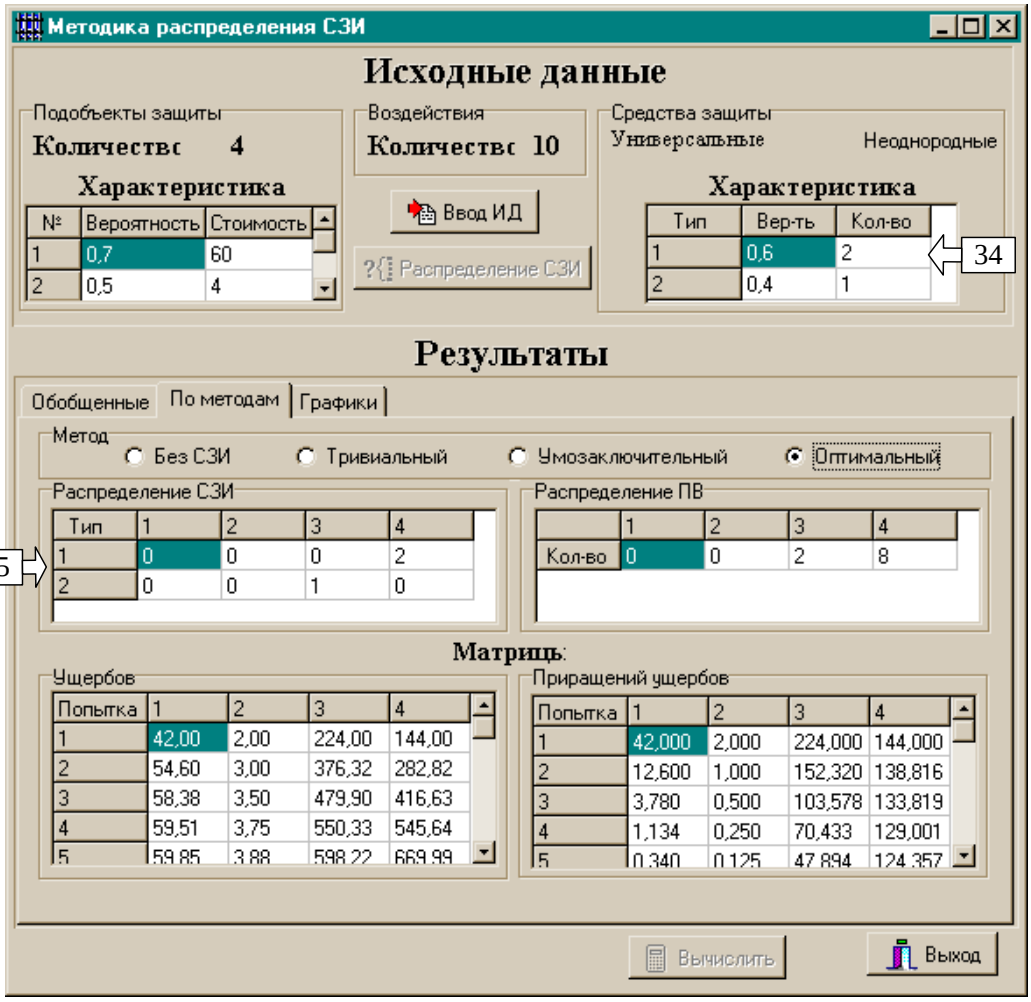


Рисунок 3.28 – Вид основного экрана при использовании неоднородных средств защиты

Применение не универсальных средств защиты, рассмотренных в п. 3.3.3 также приводит к необходимости внесения изменений в работу программного средства оптимизации размещения средств защиты.

Внешний вид экрана ввода исходных данных при использовании однородных не универсальных средств защиты примет вид, показанный на рисунок 3.29.

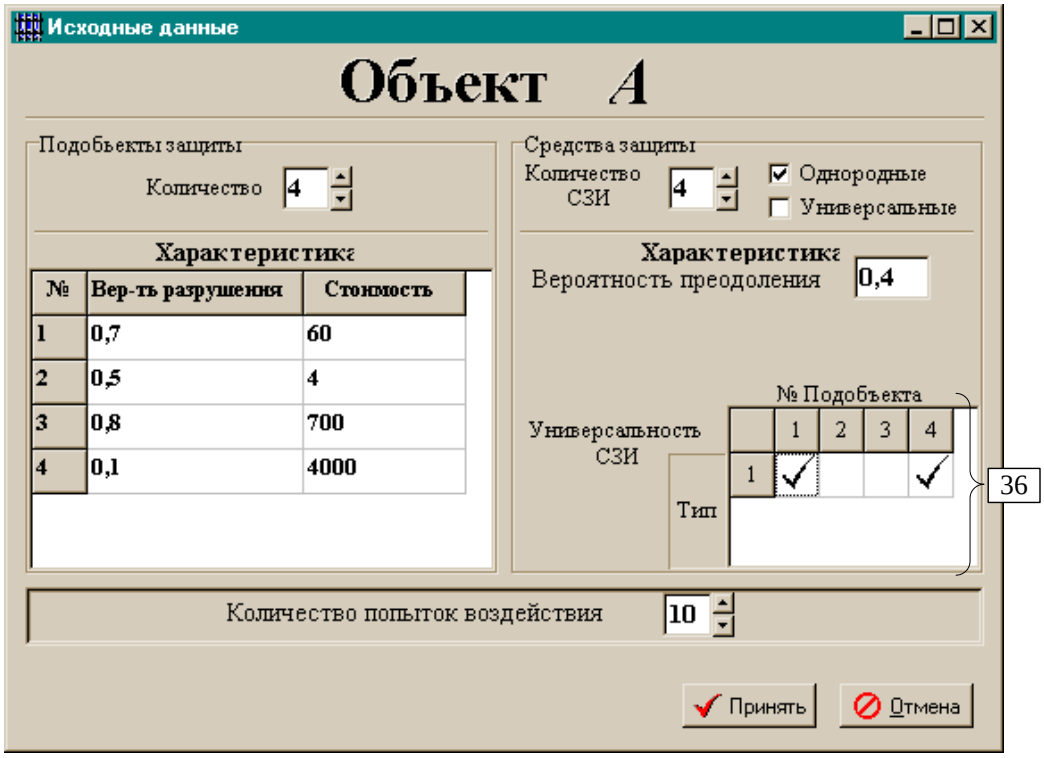


Рисунок 3.29 – Ввод исходных данных для однородных и не универсальных средств защиты

Для реализации ограничения (3.23) добавлена схема, показывающая возможность установки средства защиты на различные каналы воздействия (35). Знак (√) показывает возможность установки данного средства на указанный канал, его отсутствие – невозможность. В связи с этим требует изменения и процедура "умозаключительного" распределения средств защиты. Вид экрана этой процедуры для не универсальных средств защиты показан на рисунке 3.30.

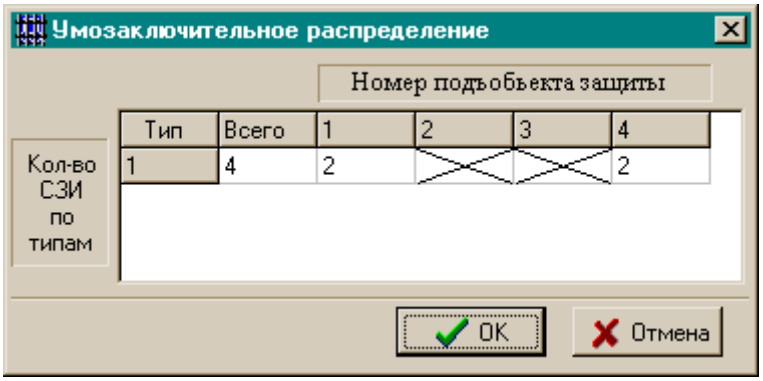


Рисунок 3.30 – "Умозаключительное" распределение однородных и не универсальных средств защиты

Перечеркнутые ячейки показывают те каналы воздействия, на которых размещение средств защиты невозможно.

Применение комбинации неоднородных и не универсальных средств защиты приводит к необходимости сочетания возможностей рисунков 3.26 и 3.29 для ввода исходных данных. Внешний вид экрана ввода исходных данных при использовании неоднородных и не универсальных средств защиты приведен на рисунке 3.31. При этом процедура "умозаключительного" распределения средств защиты примет вид, показанный на рисунке 3.32.

Рисунок 3.31 – Ввод исходных данных при использовании неоднородных и не универсальных средств защиты

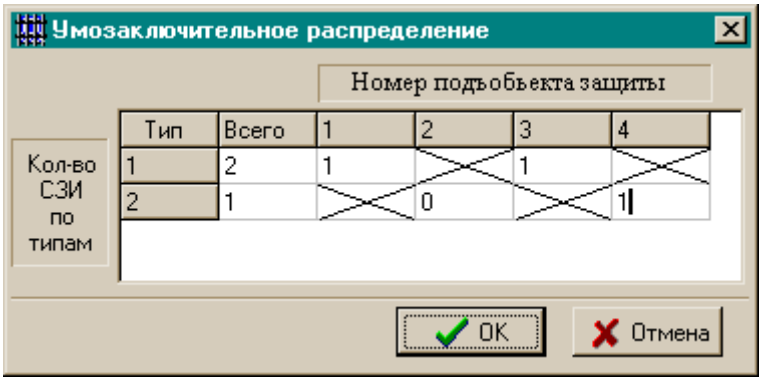


Рисунок 3.32 – "Умозаключительное" распределение неоднородных и не универсальных средств защиты

3.5 Проверка работоспособности программного средства и достоверности полученных результатов

Для проверки работоспособности разработанного программного средства и достоверности полученных результатов решена задача оптимизации размещения средств защиты в локальной информационной сети, содержащей хранилища конфиденциальной информации при исходных данных, использованных в п. 3.3.1... 3.3.4. в качестве СЗИ предполагается аппаратно-программный комплекс шифрования «Континент» и программно-аппаратное средство ЗИ «Соболь». Полученные результаты (рисунки 3.33-3.36) (W, $< a >$, $< a^* >$, $< n^* >$, $| a |$, $| a^* |$) сведены в таблицах 3.11-3.14 и представлены в виде диаграмм (для W) на рисунках 3.37- 3.41.

Таблица 3.11 – Средства защиты однородные и универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключительный	Оптимальный
W	3010	1491	1341	664
$< a >(< a^* >)$	<0,0,0,0>	<1,1,1,1>	<0,0,3,1>	<0,0,2,2>
$< n^* >$	<0,0,1,9>	<0,0,2,8>	<0,0,0,10>	<0,0,4,6>

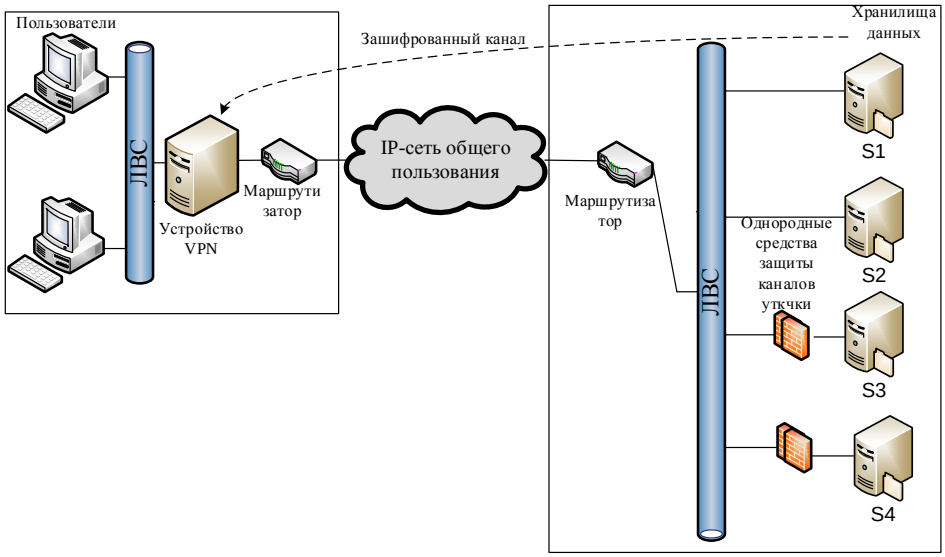


Рисунок 3.33 – Вариант защиты информации в VPN сети однородными универсальными средствами

Таблица 3.12 – Средства защиты неоднородные и универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключи-тельный	Оптималь-ный
W	3010	2674	1341	664
$\lvert a \rvert (\lvert a^* \rvert)$	$\begin{vmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{vmatrix}$	$\begin{vmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{vmatrix}$	$\begin{vmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{vmatrix}$	$\begin{vmatrix} 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 \end{vmatrix}$
$< n^* >$	<0,0,1,9>	<0,0,2,8>	<0,0,2,8>	<0,0,2,8>

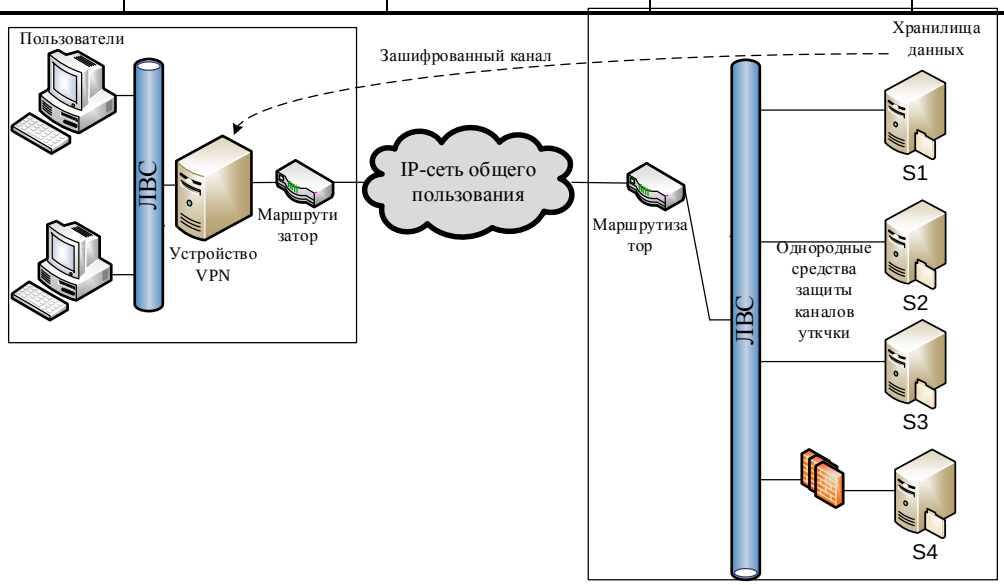


Рисунок 3.34 – Вариант защиты информации в VPN сети неоднородными универсальными средствами

Таблица 3.13 – Средства защиты однородные и не универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключи-тельный	Оптималь-ный
W	3010	1156	872	800
$< a >(< a^* >)$	<0,0,0,0>	<2,0,0,2>	<1,0,0,3>	<0,0,0,4>
$< n^* >$	<0,0,1,9>	<0,0,2,8>	<0,0,2,8>	<2,0,3,5>

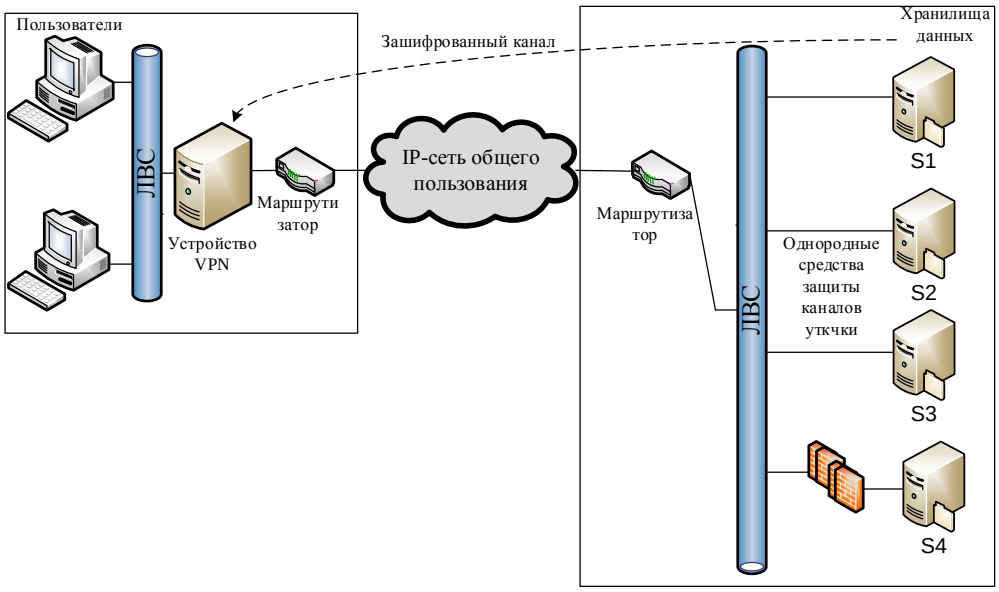


Рисунок 3.35 – Вариант защиты информации в VPN сети однородными не универсальными средствами

Таблица 3.14 – Средства защиты неоднородные и не универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключительный	Оптимальный
W	3010	1378	1110	1110
$\|a\|(\|a^*\|)$	$\begin{vmatrix}0&0&0&0\\0&0&0&0\end{vmatrix}$	$\begin{vmatrix}0&1&0&1\\0&0&0&1\end{vmatrix}$	$\begin{vmatrix}0&0&0&2\\0&0&0&1\end{vmatrix}$	$\begin{vmatrix}0&0&0&2\\0&0&0&1\end{vmatrix}$
$< n^* >$	<0,0,1,9>	<0,0,2,8>	<0,0,2,8>	<0,0,2,8>

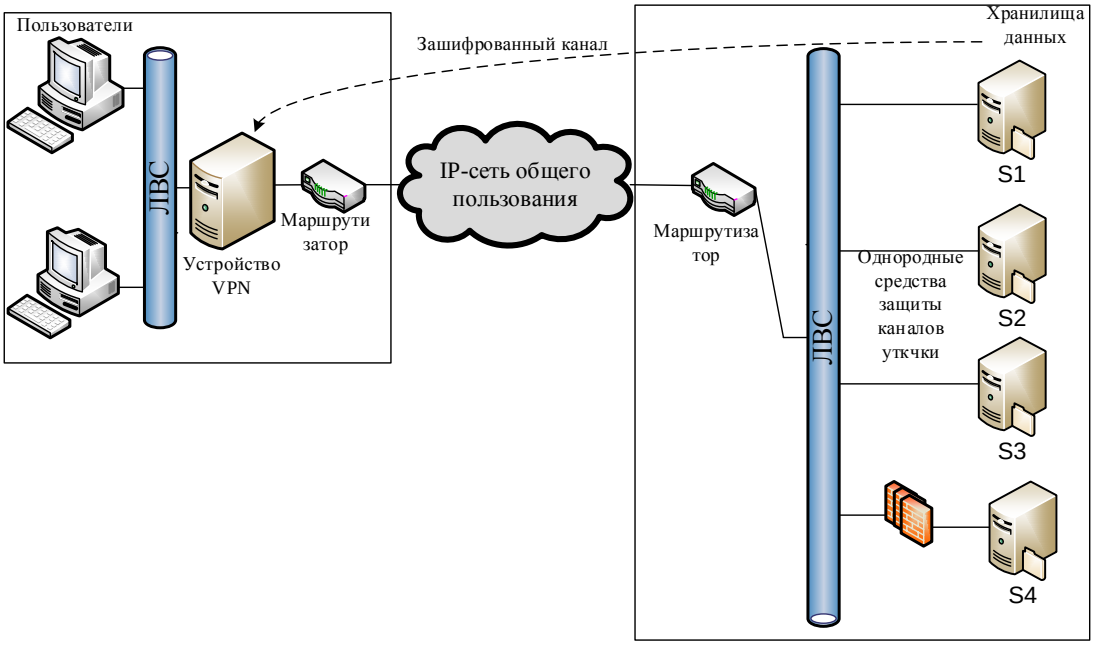


Рисунок 3.36 – Вариант защиты информации в VPN сети неоднородными и не универсальными средствами

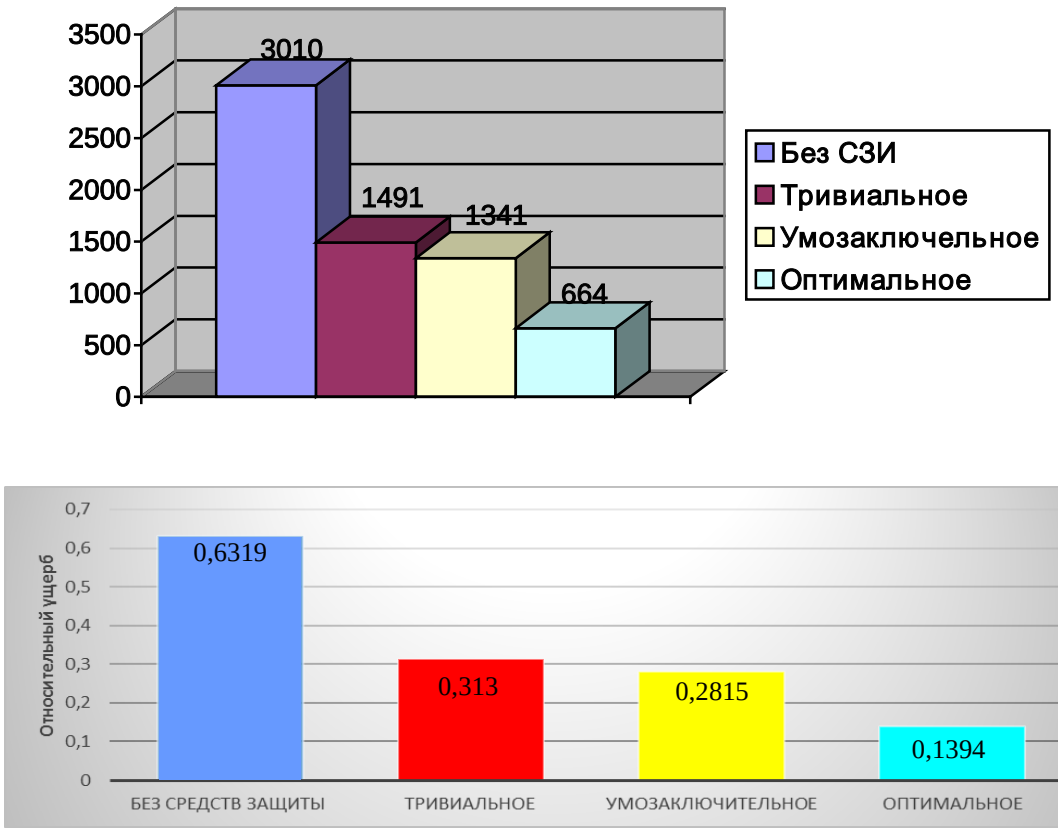


Рисунок 3.37 – Средства защиты однородные и универсальные

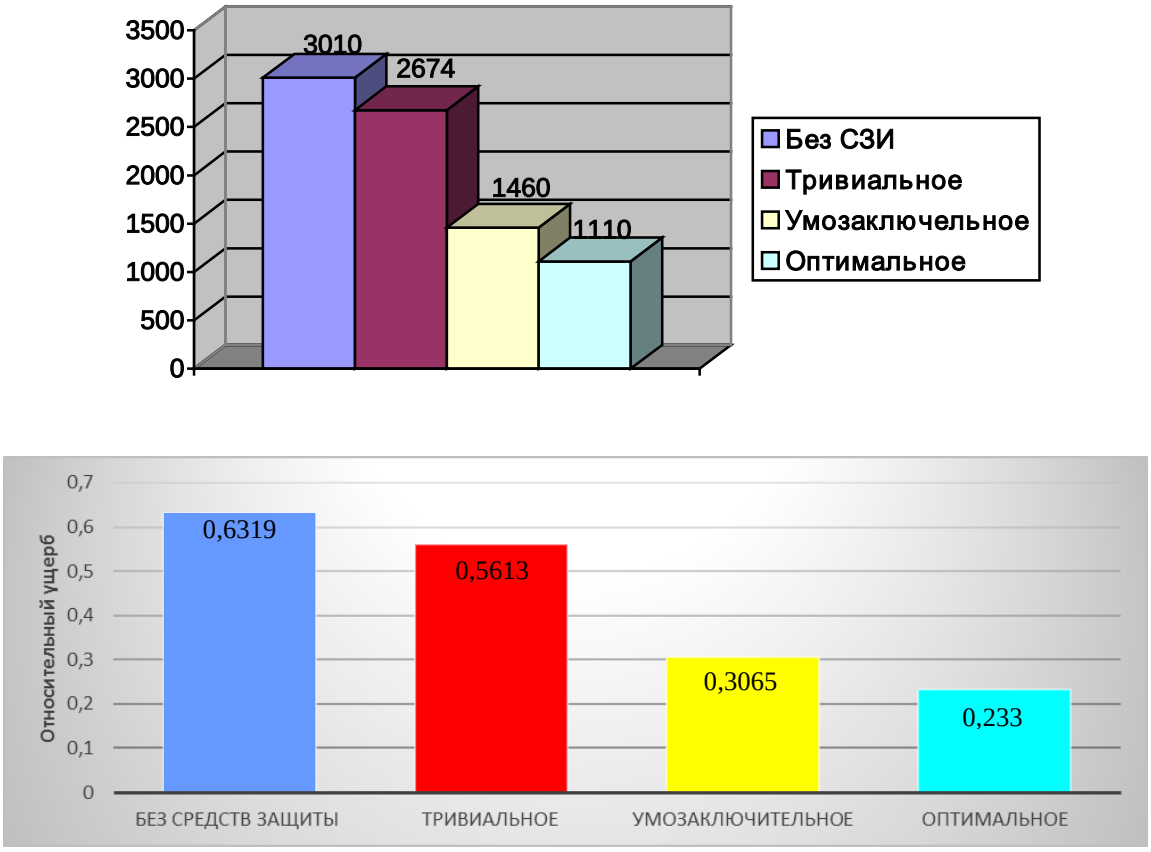


Рисунок 3.38 – Средства защиты неоднородные и универсальные

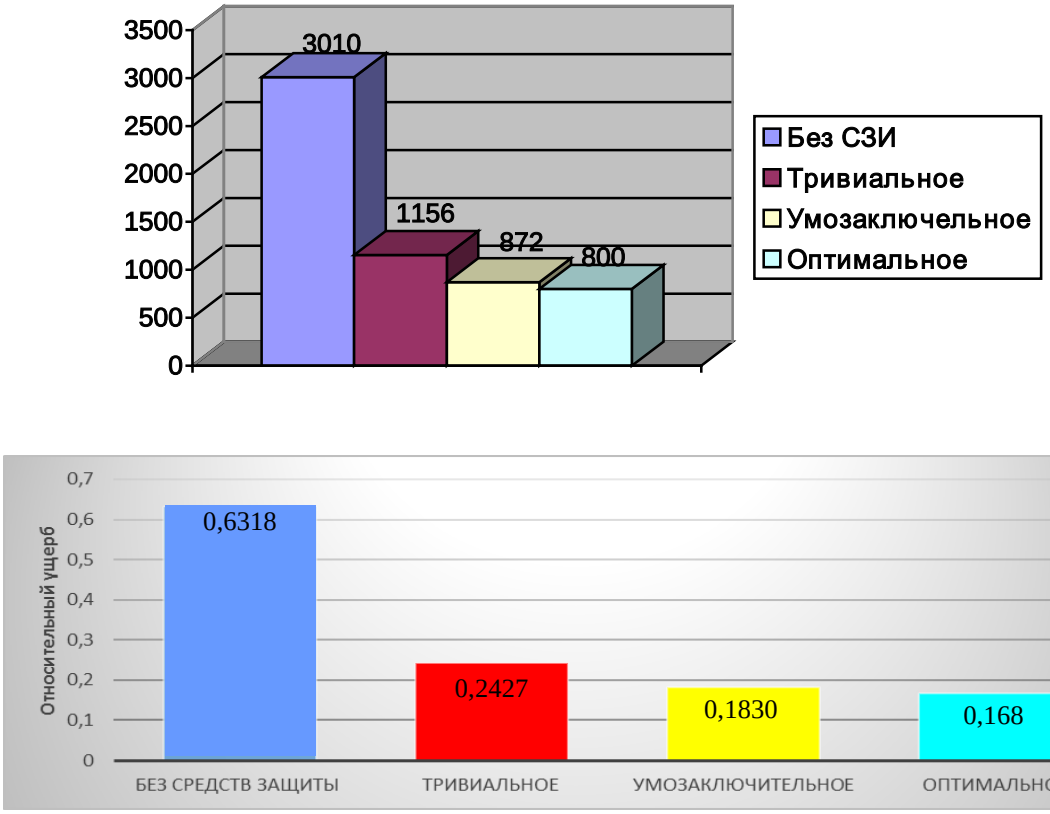


Рисунок 3.39 – Средства защиты однородные и не универсальные

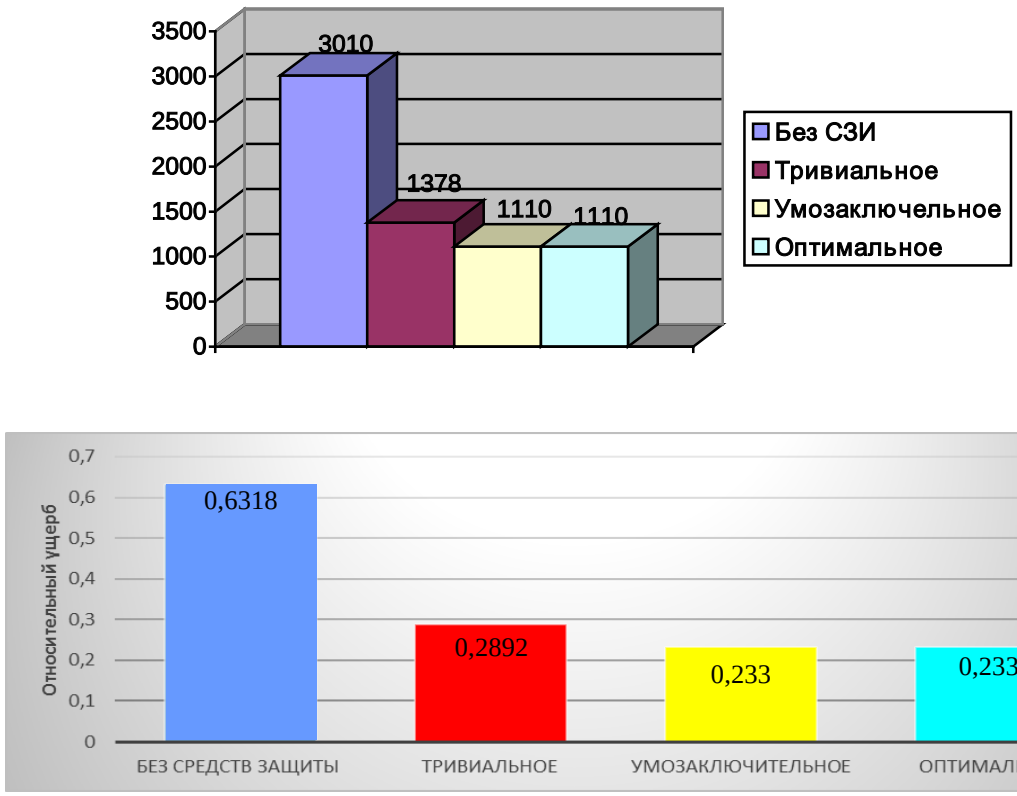


Рисунок 3.40 – Средства защиты неоднородные и не универсальные

Обобщенные результаты расчетов при использовании различных комбинаций и методов (для наглядности) изображены на рисунке 3.41.

Совпадение результатов ручного счета, выполненного в п.3.1.1 – 3.1.4 с результатами, полученными с использованием разработанного программного средства, подтверждает его работоспособность и достоверность выдаваемых результатов.

Многочисленные расчеты, выполненные с использованием разработанного программного средства при различных исходных данных, показали, что время расчетов на ЭВМ с характеристиками, описанными в п. 2.3.3 с усложнением задачи растет незначительно (не превышает десятков секунд).

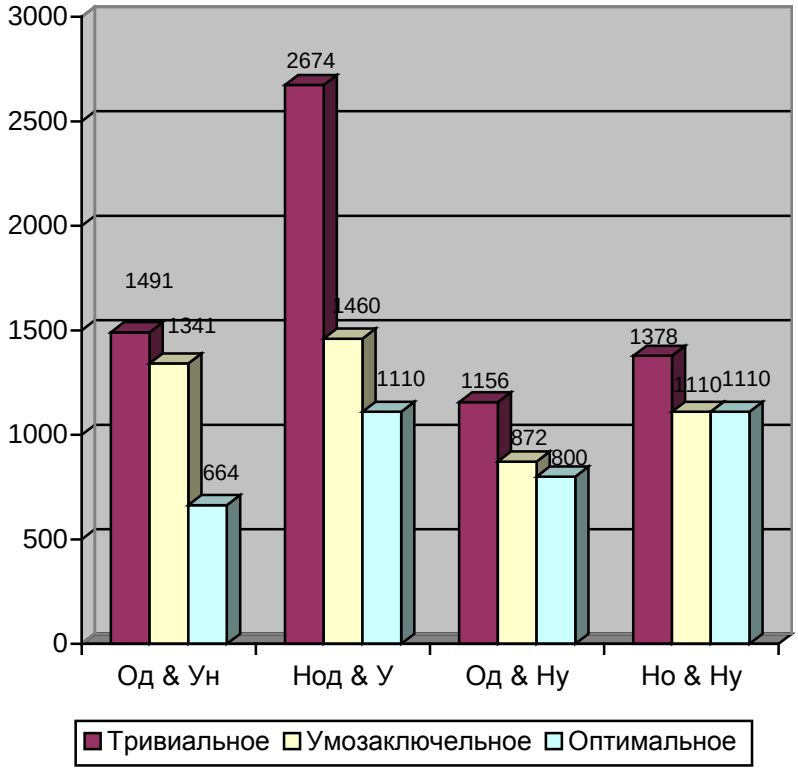


Рисунок 3.41 – Обобщенные результаты расчетов

Результаты расчетов при одном из вариантов усложненных исходных данных (таблица 3.15), приведены в таблицах 3.16–3.19 и на рисунках 3.42-3.46.

Таблица 3.15 – Усложненные исходные данные

Количество попыток воздействия – 20		
Количество средств защиты – 12		
Количество типов СЗИ (для неоднородных) – 4		
Характеристика неоднородных СЗИ		
Тип	Вероятность преодоления	Количество
1	0,6	4
2	0,4	2
3	0,8	5
4	0,1	1

Возможность размещения (для не универсальных СЗИ)				
Тип СЗИ	Канал воздействия			
	1	**2**	**3**	**4**
1	0	0	1	1
2	0	1	1	1
3	1	1	1	1
4	1	0	1	1

Результаты расчетов для усложненных исходных данных

Таблица 3.16 – Средства защиты однородные и универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключительный	Оптимальный
W	4072	537	459	664
$< a >(< a^* >)$	<0,0,0,0>	<3,3,3,3>	<1,1,3,7>	<0,0,6,6>
$< n^* >$	<0,0,2,18>	<0,0,8,12>	<1,0,19,0>	<3,0,17,0>

Таблица 3.17 – Средства защиты неоднородные и универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключи-тельный	Оптималь-ный
W	4072	2674	1341	664
$\|a\|(\|a^*\|)$	$\begin{vmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{vmatrix}$	$\begin{vmatrix}1&1&1&1\\0&1&1&0\\1&1&2&1\\0&0&0&1\end{vmatrix}$	$\begin{vmatrix}1&0&1&2\\0&0&1&1\\1&1&1&2\\0&0&0&1\end{vmatrix}$	$\begin{vmatrix}0&0&2&2\\0&0&0&2\\0&0&2&3\\0&0&1&0\end{vmatrix}$
$<n^*>$	<0,0,2,18>	<1,0,12,7>	<3,0,17,0>	<2,0,7,11>

Таблица 3.18 – Средства защиты однородные и не универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключи-тельный	Оптималь-ный
W	4072	238	872	96
$<a>(<a^*>)$	<0,0,0,0>	<4,0,4,4>	<1,0,4,7>	<0,0,6,6>
$<n^*>$	<0,0,2,18>	<0,0,17,3>	<2,0,18,0>	<3,0,17,0>

Таблица 3.19 – Средства защиты неоднородные и не универсальные

Показатели	Вариант размещения средств защиты			
	Без СЗИ	Тривиальный	Умозаключи-тельный	Оптималь-ный
W	4072	572	748	268
$\|a\|(\|a^*\|)$	$\begin{vmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\\0&0&0&0\end{vmatrix}$	$\begin{vmatrix}0&0&2&2\\0&1&1&0\\1&1&2&1\\0&0&0&1\end{vmatrix}$	$\begin{vmatrix}0&0&2&2\\0&1&0&1\\1&1&1&2\\0&0&0&1\end{vmatrix}$	$\begin{vmatrix}0&0&2&2\\0&0&0&2\\0&0&2&3\\0&0&1&0\end{vmatrix}$
$<n^*>$	<0,0,2,18>	<2,0,18,0>	<3,0,15,2>	<2,0,17,0>

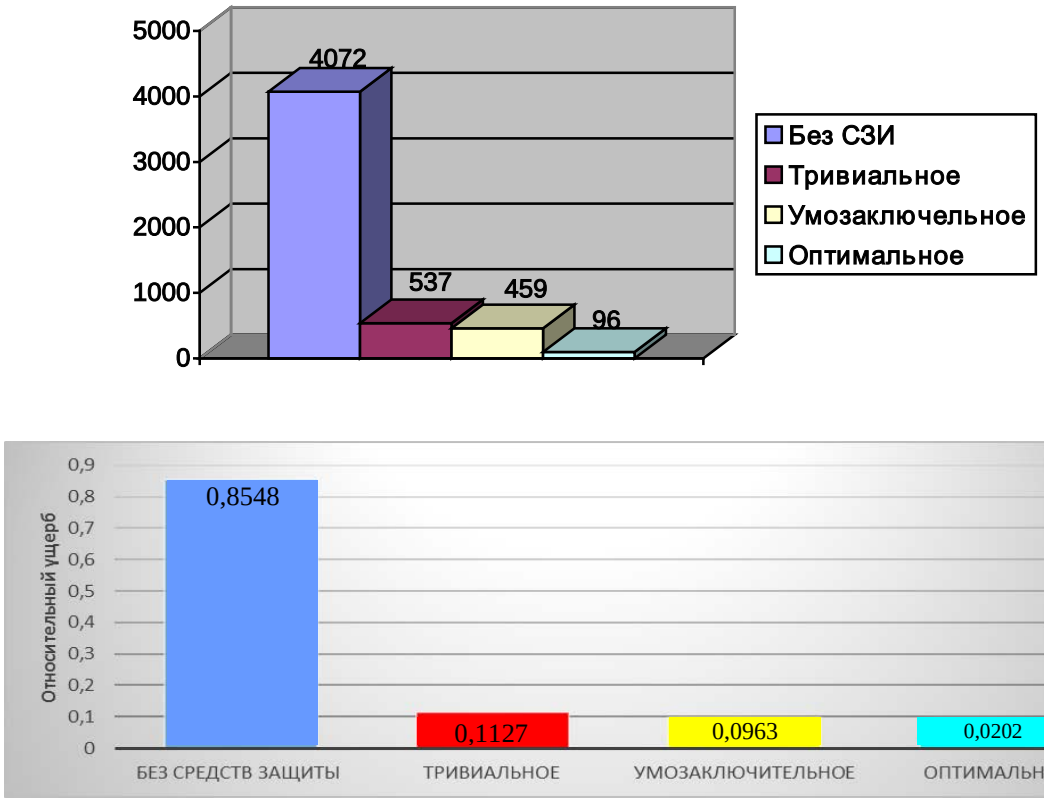


Рисунок 3.42 – Средства защиты однородные и универсальные

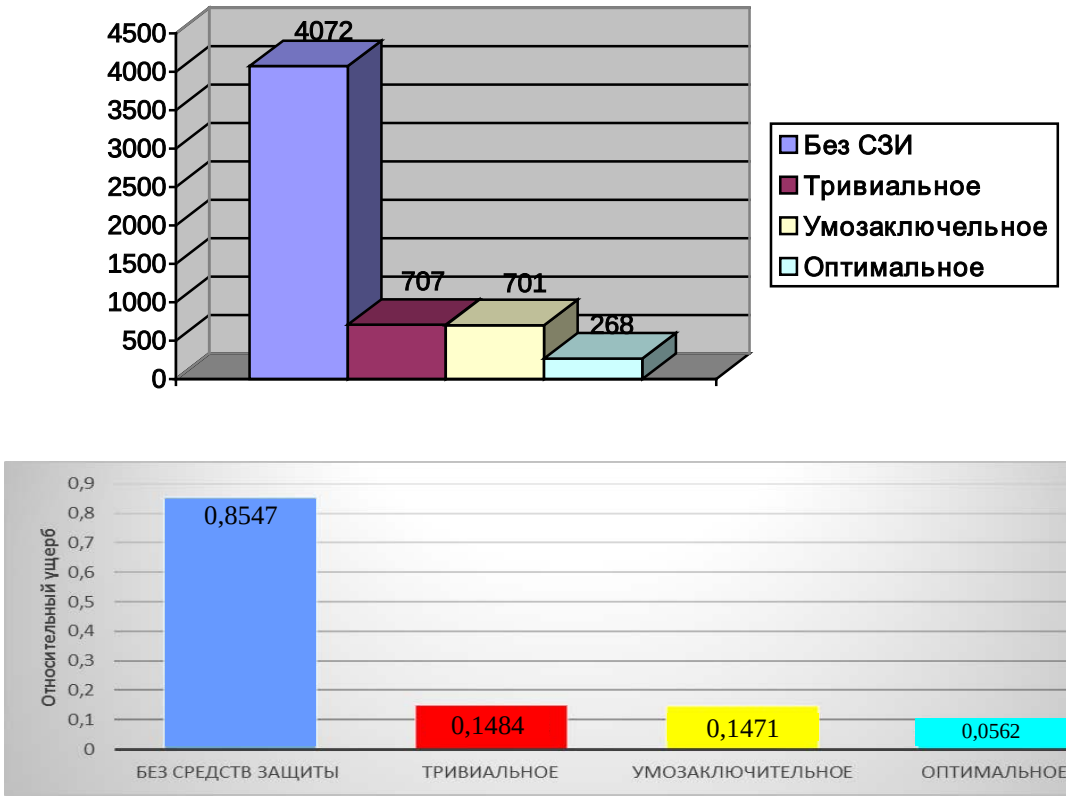


Рисунок 3.43 – Средства защиты неоднородные и универсальные

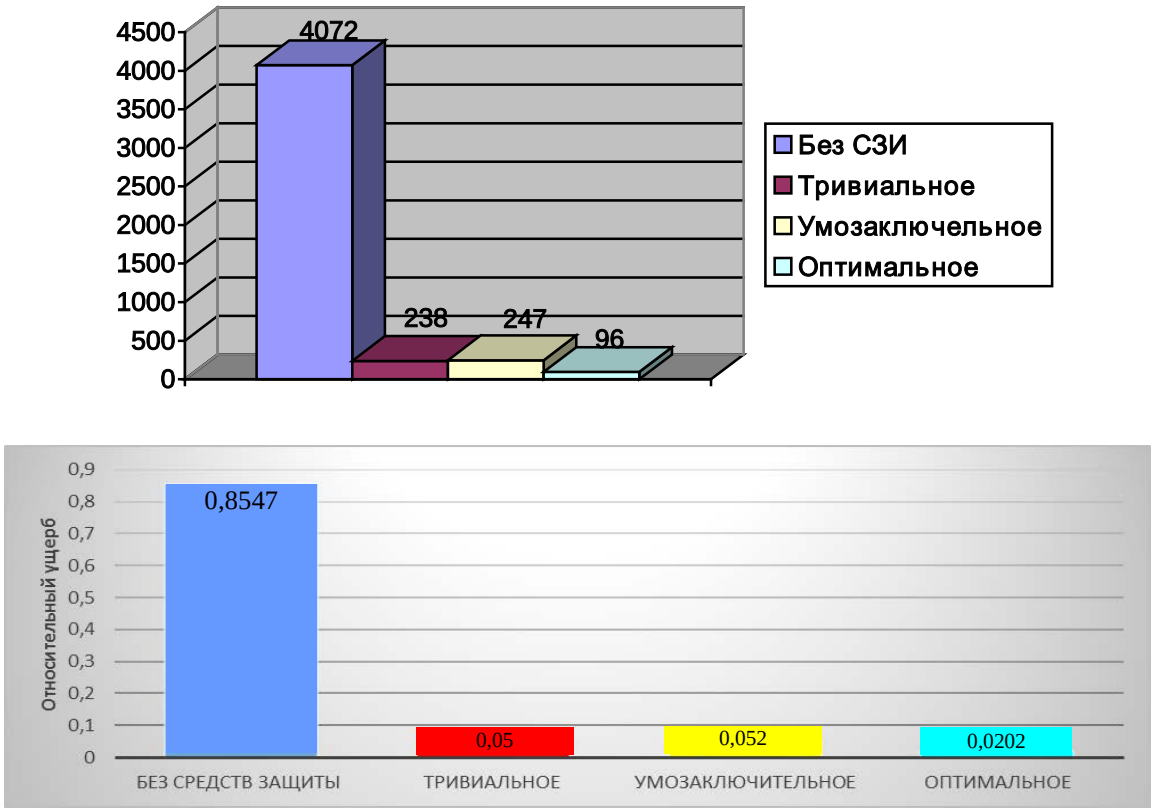


Рисунок 3.44 – Средства защиты однородные и не универсальные

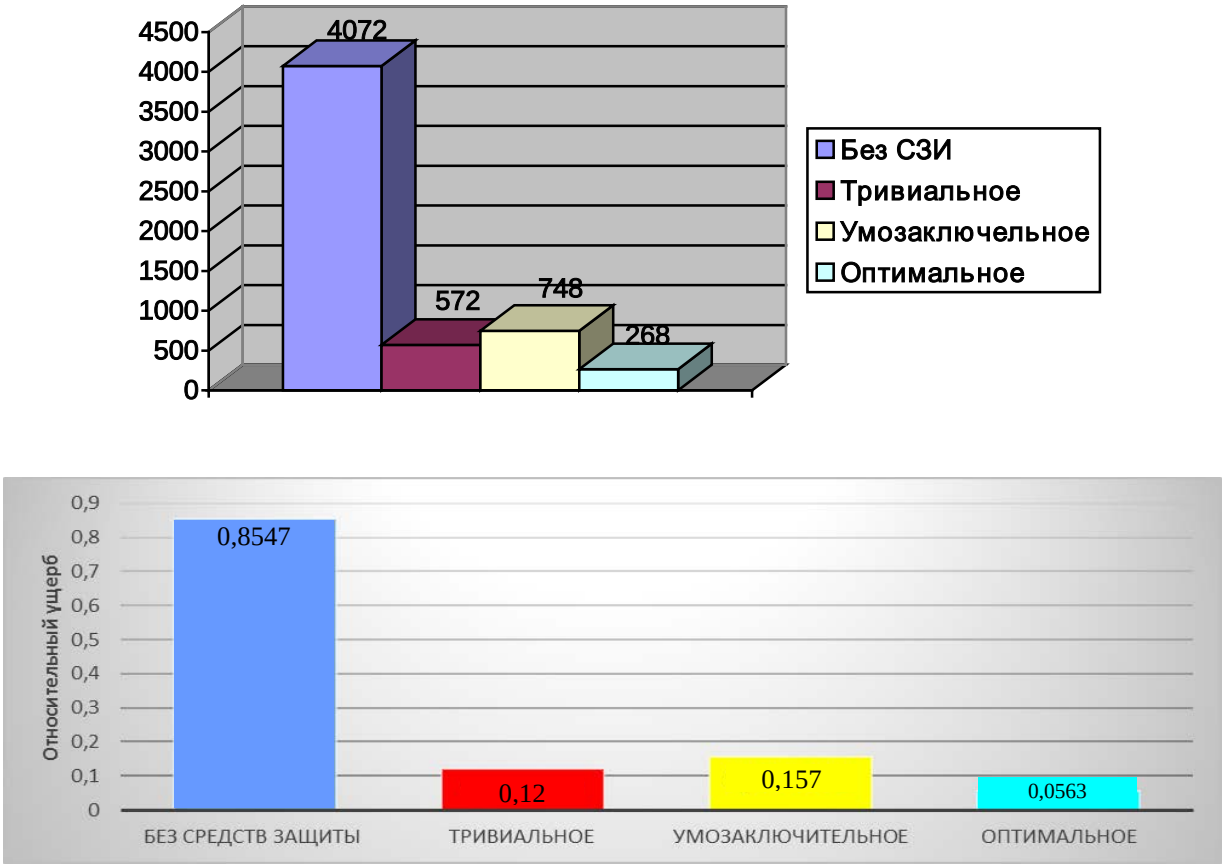


Рисунок 3.45 – Средства защиты неоднородные и не универсальные

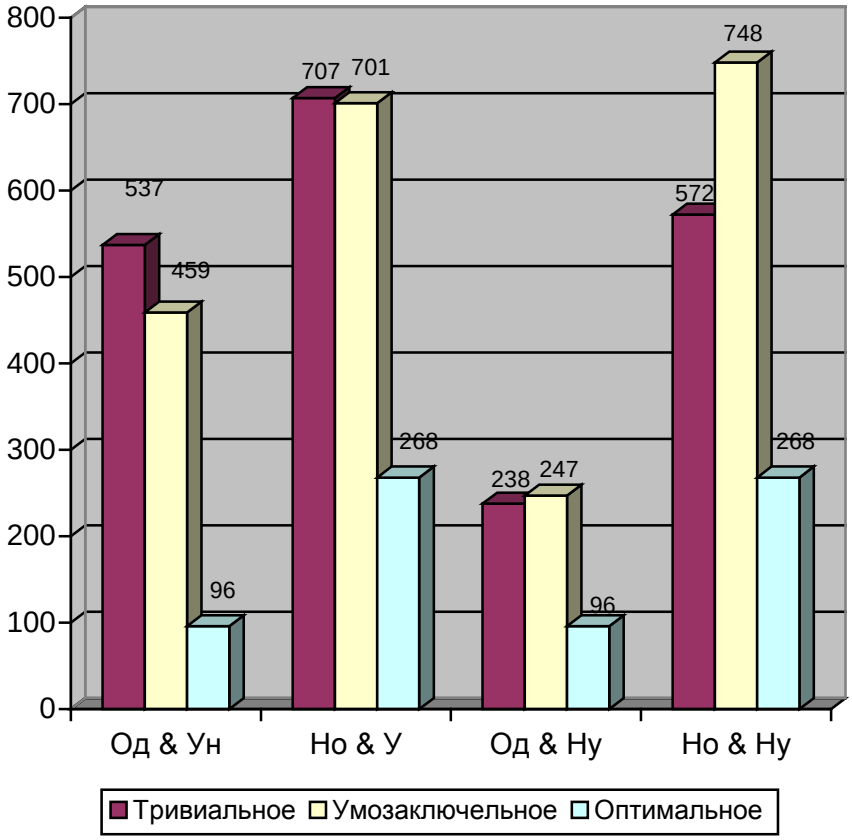


Рисунок 3.46 – Обобщенная диаграмма по всем методам

ВЫВОДЫ ПО РАЗДЕЛУ

Среди задач повышения защищенности информации, хранимой на некотором ИОС ИТС, особое место занимает задача размещения имеющихся или приобретаемых средств защиты по различным каналам воздействия.

Исследования, проведенные в данном разделе, позволяют сделать следующие выводы.

1. Добиться повышения защищенности информации можно не только экстенсивным путем (увеличением числа средств защиты и совершенствованием их характеристик, что требует приложения дополнительных финансовых ресурсов), но и оптимизацией размещения имеющихся и приобретаемых средств защиты по каналам воздействия. При этом суммарный вероятный ущерб, наносимый информации, хранящейся во всех массивах объекта, как показали расчеты, проведенные в п.3.3, может быть снижен до 2 - х раз.

2. Для нанесения ущерба информации, хранимой на объекте, злоумышленник может применять различные стратегии воздействия. Наиболее опасной, с точки зрения хранителя информации, является так называемая оптимальная стратегия, т.е. стратегия, при которой за одно и тоже количество попыток – n, злоумышленник достигает максимума нанесенного ущерба при прочих равных условиях. Решение этой задачи со стороны злоумышленника может быть найдено в соответствии с алгоритмом, приведенным на рисунке 3.5.

3. Информация, хранящаяся в массивах, может иметь различную важность, число массивов и число попыток воздействия– достаточно велики, средства защиты однородны и неоднородны, универсальны и не универсальны. Все это приводит к тому, что задача оптимизации размещения средств защиты по каналам воздействия, приобретает высокую сложность.

4. Для решения такой задачи разработана методика, позволяющая при различных исходных данных получить минимально возможное однозначное количественное значение показателя суммарного вероятного ущерба W. Математическую основу методики составляет пошаговая процедура определения оп-

тимальной стратегии злоумышленника и решение задачи оптимального размещения средств защиты на каждом шаге, реализуемая посредством совокупности метода максимального элемента и вероятностно-игрового метода. Достоверность получаемых результатов проверена решением задачи с теми же исходными данными методом полного перебора.

5. Получить решение задачи оптимизации размещения средств защиты на ИОС ИТС при значительном числе массивов (M > 20-30), средств защиты (A > 50-60) и попыток воздействия (N > 100) ручным способом не представляется возможным, поэтому в работе разработано программное средство, позволяющее автоматизировано получить однозначное решение задачи при всем диапазоне реально возможных исходных данных. Программное средство реализовано в среде визуального программирования и имеет удобный человеко-машинный интерфейс.

6. Совпадение результатов, полученных ручным способом и с помощью разработанного программного средства, позволяет судить о работоспособности автоматизированного способа реализации методики и достоверности получаемых результатов, во всем приемлемом диапазоне исходных данных, не превышает десятков секунд, а целевой эффект от применения разработанной методики растет с увеличением сложности задачи (рисунки 3.37 и 3.42).

7. Оптимизация размещения имеющихся средств защиты на типовом ИОС ИТС позволяет уменьшить ущерб, наносимый информации на 17-25%.

8. Дальнейшее повышение уровня защищенности информации в ИОС ИТС лежит на пути создания комплекса перспективных средств защиты информации.

ЗАКЛЮЧЕНИЕ

В ходе выполнения диссертационного исследования получены следующие основные научные результаты, представляемые к защите:

1. Аналитические и имитационная модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети.

2. Автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат.

В результате исследований, проведенных в работе, выявлено, показано, доказано и разработано следующее:

- В настоящий момент для построения VPN используется ряд протоколов, которые не шифруют данные, а лишь определяют, как используются алгоритмы шифрования и ряд других условий, необходимых для построения VPN. При реализации VPN на базе уже существующего сетевого оборудования, возможны атаки, которые могут нарушить как функционирование самого устройства, так и временно взаимодействие защищаемых с их помощью сетей и узлов. Кроме того, зачастую VPN реализуется чисто программными средствами, что приводит к уязвимости операционной системы и могут свести на нет все защитные механизмы VPN.

- Защищенность информации в ИТС является комплексным свойством. Однако, с точки зрения ИТС можно выделить три основных атрибутивных свойства: достоверность, сохранность и конфиденциальность и на них сосредоточить внимание разработчиков СЗИ для ИТС. В ряде работ доказано, что ни один из способов защиты информации, методов, мер, средств и мероприятий не является абсолютно надежным, а максимальный эффект достигается при объединении их всех в единую комплексную СЗИ ИОС ИТС и эта комплексность должна быть: концептуальной, целевой и временной.

- В зависимости от конкретных условий задачи исследования, в первом разделе пояснительной записки сформулирована постановка задачи, которая может быть направлена как на достижение минимума вероятности (1.22), максимума стоимости (1.24), так и минимума величины потерь (ущерба) от взлома всех механизмов защиты, используемых в СЗИ (1.29). Критерий выбора СЗИ представлен в виде (1.8).
- В настоящее время единая и общепринятая модель воздействия ещё не создана. Одноуровневые и многоуровневые матричные модели носят в основном теоретический характер и практического применения без существенных доработок найти не могут.
- Результаты моделирования СЗИ ИОС ИТС с помощью разработанных во втором разделе пояснительной записки моделей показали, что полученные результаты отличаются от известных в сторону увеличения вероятности преодоления на 17…21 %, что еще раз подчеркивает необходимость совершенствования СЗИ в существующей и создаваемых ИТС управленческого типа.
- Добиться повышения защищенности информации можно не только экстенсивным путем, но и оптимизацией размещения имеющихся и приобретаемых средств защиты по каналам воздействия. При этом суммарный вероятный ущерб, наносимый информации, хранящейся во всех массивах объекта, как показали расчеты, проведенные в п.3.3, может быть снижен до 2 - х раз.
- Для решения задачи оптимизации размещения средств защиты по каналам воздействия, в третьем разделе пояснительной записки разработана методика, позволяющая при различных исходных данных получить минимально возможное однозначное количественное значение показателя суммарного вероятного ущерба W. Математическую основу методики составляет пошаговая процедура определения оптимальной стратегии злоумышленника и решение задачи оптимального размещения средств защиты на каждом шаге, реализуемая

посредством совокупности метода максимального элемента и вероятностно-игрового метода.

- Достоверность получаемых результатов проверена решением задачи с теми же исходными данными методом полного перебора. Кроме того, в работе разработано программное средство, позволяющее автоматизировано получить однозначное решение задачи при всем диапазоне реально возможных исходных данных. Программное средство реализовано в среде визуального программирования и имеет удобный человеко-машинный интерфейс.

Таким образом, оптимизация размещения имеющихся средств защиты на типовом ИОС ИТС позволяет уменьшить ущерб, наносимый информации на 17-25%.

Результаты опубликованы в 31-й публикации, из них: 29 статей в научно-технических сборниках, в том числе 5 статей в журналах из Перечня ВАК; 1 отчёт об ОКР и 1 патент на полезную модель.

Результаты работы реализованы:

1. В МОУ «Институт инженерной физики» в СЧ ОКР «Модуль-ИИФ» (акт о реализации МОУ «ИИФ» от 17.11.2016 г.).

2. В АО «Центральный научно-исследовательский институт экономики информатики и систем управления» при обосновании размещения средств защиты информации в узлах коммутации VPN сети специального назначения в рамках ОКР «Заполье», ОКР «Ретранслятор» (акт о реализации АО «ЦНИИ ЭИСУ» от 19.01.2017 г.).

3. В филиале Военной академии РВСН имени Петра Великого в учебном процессе по кафедре «Автоматизированные системы боевого управления» при изучении дисциплины «Криптографические методы и средства защиты информации» (акт о реализации ФВА РВСН от 26.01.2017 г.).

Дальнейшее повышение уровня защищенности информации в ИОС ИТС лежит на пути создания комплекса перспективных средств защиты информации.

СПИСОК ПРИНЯТЫХ СОКРАЩЕНИЙ

АИС - автоматизированная информационная система;

БД - база данных;

ИОС – информационный объект сети;

ИТС - информационная телекоммуникационная сеть;

ЛВС - локальная вычислительная сеть;

М - маршрутизатор;

МСЭ - межсетевой экран;

НСД – несанкционированный доступ;

ОС – операционная система;

ПС – программное средство;

ПК – персональный компьютер;

СЗИ – система защиты информации;

СрЗИ – средство защиты информации;

УК - узел коммутации;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ЭМВОС - эталонная модель взаимодействия открытых систем;

MPLS – Multi Protocol Label Switching;

NGN – Next Generation Network;

QoS – Quality of Service;

VPN - Virtual Private Network.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Абрамов, С. А. Математические построения и программирование / С. А. Абрамов // Наука. Гл. ред. физ.-мат. лит. - М.: 1978. - 191 С.

2. Агеев, А. С. Компьютерные вирусы и безопасность информации/ А. С. Агеев // Зарубежная радиоэлектроника. – М.: 1989. - № 12. – С. 71-75.

5. Андрианов, Ю. М. Квалиметрия в приборостроении и машиностроении / Ю. М. Андрианов, А. И. Субетто // Л.: Машиностроение, 1990. - 216 С.

6. Аршинов, М. Н. Коды и математика / М. Н. Аршинов, Л. Е. Садовский // Наука. Гл. ред. физ.-мат. лит. - М.: 1983. - 114 С.

7. Барни, К. ИС шифратора, облегчающая процесс распределения ключей / К. Барни // Электроника. – М.: 1986. - Т. 59, № 16. - С.6-8.

8. Барсуков, В.С. Обеспечение информационной безопасности. Технология электронных коммуникаций / В. С. Барсуков // М.: 1996.

9. Батурин, Ю. М. Компьютерная преступность и компьютерная безопасность / Ю. М. Батурин, А. М. Жиджитский // М.: Юридическая литература, 1991. - 162 С.

10. Бияшев, О. Г. Основные направления развития и совершенствования криптографического закрытия информации. / О. Г. Бияшев, С. И. Диев, М. К. Размахнин // М.: Зарубежная радиоэлектроника, 1989. - № 12.

11. Борисов В.И. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов модуляцией несущей псевдослучайной последовательностью.// Под ред. В.И. Борисова. – М.: Радио и связь, 2003. – 640с.

12. Борисов В.И. и др. Помехозащищенность систем радиосвязи с расширением спектра сигналов методом псевдослучайной перестройки рабочей частоты. – М.: Радио и связь, 2000. – 384с.

13. Бриккел, Э. Ф. Криптоанализ: обзор новейших результатов / Э. Ф. Бриккел, Э. М. Одлишко // М.:ТИИЭР, 1988. – Т. 76, №5. – С. 75-94.

14. Бронштейн, И. Н. Справочник по математике для инженеров и учащихся втузов.- 13-е изд. исправленное / И. Н. Бронштейн, К. А. Семендяев // М.: Наука. Гл. ред. физ.-мат. лит., 1986. - 544 С.

15. Бурков, В. Н. Основы математической теории активных систем / В. Н. Бурков // М.: Наука, 1997.

16. Бусленко, Н. П. Моделирование сложных систем / Н. П. Бусленко // М.: Наука, 1968.

17. Бусленко, В. Н. Автоматизация имитационного моделирования сложных систем / В. Н. Бусленко // М.: Наука,1977. - 240 С.

18. Бусленко, Н. П. Лекции по теории сложных систем / Н. П. Бусленко, В. В. Калашников, И. Н. Коваленко // М.: Советское радио, 1973. - 438 С.

19. Бэйлс, Б. «Керберос» – новая схема защиты информации / Б. Бэйлс // М.: Сети, 1994. - № 4. – С. 45-47.

20. Основы исследования операций / Г. Вагнер // М.: Мир, 1972. - Т. 1. - 332 С.

21. Вентцель, Е. С. Исследование операций / Е. С. Вентцель // М.: Советское радио, 1972. - 552 С.

22. Вентцель, Е. С. Теория вероятностей / Е. С. Вентцель // М.: Наука, 1980. - 564 С.

23. Галатенко, В.А. Стандарты информационной безопасности : курс лекций : учебное пособие / Втрое издание / Под редакцией академика РАН В.Б. Бетелина / М : ИИТУИТ.РУ «Интернет-университет Информационных Технологий», 2006.

24. Герасименко, В. А. Защита информации в вычислительных, информационных и управляющих системах / В. А. Герасименко, М. К. Размахнин // М.: Зарубежная радиоэлектроника, 1985. - № 8.

25. Герасименко, В. А. Защита информации в автоматизированных системах обработки данных / В. А. Герасименко // М.: Энергоатомиздат, 1994.

26. Герасименко, В. А. Организация работ по защите информации в системах электронной обработки данных / В. А. Герасименко, Размахнин М. К. // М.: Зарубежная радиоэлектроника, 1989. - № 12. - С. 110-120.

27. Герасименко, Новые направления применения криптографических методов защиты информации / В. А. Герасименко, А. А. Скворцов, А. И. Харитонов // М.: Зарубежная радиоэлектроника, 1989. - № 12. - С. 92-101.

29. Горбатов, В. А. Основы дискретной математики.: Учеб. пособие для студентов вузов / В. А. Горбатов // М.: Высш.шк., 1986. - 311 С.

30. Грибунин, В.Г. Комплексная система защиты информации на предприятии / В. Чудовский // Изд-во «Академия», 2009. – 416 С.

31. Давыдов, В.Е. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем / А.Е. Давыдов, Р.В. Максимов, О.К. Савицкий. – Москва: ОАО «Воентелеком», 2015. – 520 с.: ил.

32. Давыдовский, А. И. Защита информации в вычислительных сетях / А. И. Давыдовский, П. В. Дорошевич // М.: Зарубежная радиоэлектроника, 1989. - № 12. - С. 60-70.

33. Девянин, П.Н. Модели безопасности компьютерных систем: Учеб, пособие для студ. высш. учеб, заведений / Петр Николаевич Девянин. — М.: Издательский центр «Академия», 2005. — 144 с.

34. Денисов, А. А. Теория больших систем управления: Учебное пособие для вузов / А. А. Денисов, Д. Н. Колесников // Л.: Энергоиздат, 1982. – 288 С.

35. Диев, С. Н. Защита информации в персональных компьютерах / С. Н. Диев // М.: Зарубежная радиоэлектроника, 1989. - № 12. - С. 57-59.

36. Диффи, У. Защищенность и имитостойкость: Введение в криптографию / У. Диффи, М. Е. Хеллман // М.: ТИИЭР, 1979. - Т. 67, № 3. - С.71-109.

37. Диффи, У. Первые десять лет криптографии с открытым ключом / У. Диффи // М.: ТИИЭР, 1988. - Т. 76, № 5. - С. 54-74.

38. Жук, А. Защита информации. Учебное пособие / Е. Жук, О. Лепешкин, А. Тимошкин // Изд-во «Инфра-М», 2015. – 392 С.

39. Казаков, В. А. Введение в теорию марковских процессов и некоторые радиотехнические задачи / В. А. Казаков // М.: Сов. радио, 1973. - 232 С.

40. Касперский, Е. «Дыры» в MS DOS и программы защиты информации / Е. Касперский // М.: Компьютер-Пресс, 1991. - № 10.

41. Кемени, Джон. Дж. Конечные цепи Маркова / Джон. Дж. Кемени, Дж. Ларк Снелл // М.: Наука, 1970. - 272 С.

42. Кент, С. Обеспечение безопасности в вычислительных сетях. В кн. Протоколы и методы управления в сетях передачи данных / С. Кент // М.: Радио и связь, 1985. - 480 С.

43. Клиот-Дашинский, М. И. Алгебра матриц и векторов / М. И. Клиот-Дашинский // Л.: Изд.-во Ленингр. ун.-та, 1974. - 160 С.

44. Кнут, Д. Искусство программирования для ЭВМ. Т. 1. Основные алгоритмы / Д. Кнут // М.: Мир, 1976.

45. Кнут, Д. Искусство программирования для ЭВМ. Т.2 / Д. Кнут // М.: Мир,1977.

46. Ковалёв, М. С. Моделирование многоэшелонированных систем защиты информации [Текст] / М. С. Ковалев, В. А. Цимбал // Информационные технологии в проектировании и производстве. – М., 2010. – №4. – С. 42–48.

47. Ковалёв, М. С. Системный уровень проектирования защищенных сетей [Текст] / М. С. Ковалев, А. П. Галкин, А. Д. Р. Хамид, О. Х. Мохаммед Али, М. М. Амро // Известия Ин-та инженерной физики : науч.-техн. журн. – Серпухов, 2013. – № 4 (30) – С. 10–12.

48. Ковалёв, М. С. Синтез пользовательской структуры для информационной защиты сети с маршрутизаторами с использованием САПР [Текст] / М. С. Ковалев, А. П. Галкин, А. Бадван, М. М. Амро, М. М. А. Альджарадат, И. Дарахма // Известия Ин-та инженерной физики : науч.-техн. журн. – Серпухов, 2014. – № 1 (31) – С. 11–14.

49. Ковалёв, М. С. Выбор рациональной информационной защиты корпоративных сетей с криптографией [Текст] / М. С. Ковалев, А. П. Галкин, Е. Г. Суслова, А.-Д. Р. Хамид, О. Х. Мохаммед Али // Известия Ин-та инженерной физики : науч.-техн. журн. – Серпухов, 2014. – № 3 (33) – С. 7–12.

50. Ковалёв, М.С. Оценка своевременности доставки многопакетных сообщений в TCP-соединении VPN MPLS-сети [Текст] / Ковалёв М.С., Цимбал В.А., Исаева Т.А., Бернюков А.К., Якимова И.А. // Известия Института инженерной физики. 2015. Т. 4. № 38. С. 25-30

51. Ковалёв, М. С. Системный подход к оценке эффективности ведомственной системы связи [Текст] // Тр. Рос. науч.–техн. общ. радиотехн., электрон. и связи им. А.С. Попова. ; Серия : научная сессия, посвященная Дню радио ; – М. : ООО «Инсвязьиздат», 2008. – Вып. LXIII. – С. 435–437.

52. Ковалёв, М. С. Концепция управления уровнем безопасности системы потенциально опасных объектов [Текст] / М. С. Ковалёв, Е. В. Смирнова, М. Ю. Бессмертный // Новые информационные технологии в системах связи и управления : Тр. VIII Рос. НТК / Мин-во промышленности и торговли РФ, ФГУП «Калужский НИИ телемеханических устройств», Рос. инженерная академия. – Калу-га: Изд. ООО «Ноосфера», 2009. – 4-5 июня. – С. 494–498.

53. Ковалёв, М. С. Общий подход к созданию системы управления уровнем безопасности комплекса распределенных потенциально опасных объектов [Текст] / М. С. Ковалёв, М. Ю. Бессмертный // Тр. XXIX Всерос. НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» / Серпуховский военный институт ракетных войск. – Серпухов, 2009. – Ч. 4. – С. 156–161.

54. Ковалёв, М. С. Нахождение характеристик системы защиты информации объекта информатизации с универсальным «скользящим» средством защиты [Текст] / М. С. Ковалёв, М. Ю. Бессмертный // Материалы VIII Междун. науч.-техн. конф. «Перспективные технологии в средствах передачи информации» / Владим. гос. университет ; редкол.: А. Г. Самойлов [и др.]. – Владимир : ВлГУ, 2009. – Т. 1. – С. 129–131.

55. Ковалёв, М. С. Оптимизация параметров узла коммутации сети передачи данных с интеграцией служб [Текст] / М. С. Ковалёв, В. Б. Девятияров // Тр. Рос. науч.–техн. общ. радиотехн., электрон. и связи им. А.С. Попова. ; Серия : научная сессия, посвященная Дню радио ; – М. : ООО «Инсвязьиздат», 2010. – Вып. LXV. – С. 420–422.

56. Ковалёв, М. С. Системный анализ применения разнотипных средств защиты информации на звеньях управления АСУ [Текст] // Новые информационные технологии в системах связи и управления : Тр. IX Рос. НТК / Минво промышленности и торговли РФ, ФГУП «Калужский НИИ телемеханических устройств», Рос. инженерная академия. – Калуга: Изд. ООО «Ноосфера», 2010. – 2-3 июня. – С. 218–219.

57. Ковалёв, М. С. К вопросу обмена ключевыми данными по открытому каналу в условиях активного нарушителя [Текст] / М. С. Ковалёв, О. П. Мало-фей, Ю. И. Бутов // Тр. XXIX Всерос. НТК «Проблемы эффективности и без-опасности функционирования сложных технических и информационных систем» / Серпуховский военный институт ракетных войск. – Серпухов, 2010. – Ч. 4. – С. 162–165.

58. Ковалёв, М. С. Оценка структурных свойств нелинейной ПСП для шифросистемы гаммирования [Текст] / М. С. Ковалёв, Т. А. Исаева, П. С. Смородов // Сб. тр. IV междун. НПК «Информационные технологии в образовании, науке и производстве». – Серпухов, 2010. – С. 338–340.

59. Ковалёв, М. С. Новые технологии защиты информации с использованием непозиционных систем счисления [Текст] / М. С. Ковалев, И. А. Калмыков, О. А. Кихтенко, А. В. Барильская // Тр. Рос. науч.–техн. общ. радиотехн., электрон. и связи им. А.С. Попова. ; Серия : научная сессия, посвященная Дню радио ; – М. : ООО «Информпресс-94», 2011. – Вып. LXVI. – С. 30–32.

60. Ковалёв, М. С. Многомерная модель разграничения доступа в объект-но-ориентированных системах [Текст] / М. С. Ковалев, А. Ф. Чипига, А. А. Ерещенко // Тр. Рос. науч.–техн. общ. радиотехн., электрон. и связи им.

А.С. Попова. ; Серия : научная сессия, посвященная Дню радио ; – М. : ООО «Информ-пресс-94», 2011. – Вып. LXVI. – С. 34–35.

61. Ковалёв, М. С. Оптимизация размещения средств защиты информации на объекте [Текст] // Новые информационные технологии в системах связи и управления : Тр. X Рос. НТК / Мин-во промышленности и торговли РФ, ОАО «Концерн «Вега», ОАО «Калужский НИИ телемеханических устройств». – Ка-луга: Изд. ООО «Ноосфера», 2011. – 1-2 июня. – С. 313–315.

62. Ковалёв, М. С. Подход к методологии обнаружения сетевых атак к контентной фильтрации [Текст] / М. С. Ковалёв, А. Ф. Чипига, А. В. Епишев // Тр. XXX Всерос. НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» / Серпуховский военный институт ракетных войск. – Серпухов, 2011. – Ч. 4. – С. 222–225.

63. Ковалёв, М. С. Модулярная схема разделения секрета для беспроводных самоорганизующихся сетей [Текст] / М. С. Ковалёв, И. А. Калмыков, Е. М. Яковлева // 67-я Всерос. конф. с междун. участ. «Научная сессия, посвященная Дню радио» (RDC-2012) ; Тр. Рос. науч.–техн. общ. радиотехн., электрон. и связи им. А.С. Попова. – М. : ООО «Информпресс-94», 2012. – Вып. LXVII. – С. 62–64.

64. Ковалёв, М. С. Исследование модулярной схемы разделения секрета для беспроводных самоорганизующихся сетей [Текст] / М. С. Ковалёв, И. А. Калмыков, Е. М. Яковлева // Новые информационные технологии в системах связи и управления : Тр. XI Рос. НТК / Мин-во промышленности и торговли РФ, ОАО «Концерн «Вега», ОАО «Калужский НИИ телемеханических устройств». – Калуга: Изд. ООО «Ноосфера», 2012. – 6 июня. – С. 259–261.

65. Ковалёв, М. С. Методы защиты PHP приложений от XSS атак и SQL инъекций [Текст] / М. С. Ковалёв, В. С. Пелешенко // Тр. XXXI Всерос. НТК «Проблемы эффективности и безопасности функционирования сложных технических и информационных систем» / Серпуховский военный институт ракетных войск. – Серпухов, 2012. – Ч. 3. – С. 125–131.

66. Ковалёв, М. С. Математическая модель системы связи защищенной автоматизированной системы с управляемыми структурами [Текст] / М. С. Ковалев, В. И. Граков // Междун. конф. «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (RES-2013) ; Доклады ; Серия: науч. конф. посвящ. Дню радио / Рос. науч.-техн. общ. радиотехн., электрон. и связи им. А.С. Попова. – М. : ООО «Информпресс-94», 2013. – Вып. LXVIII. – С. 23–26.

67. Ковалёв, М. С. Модель уязвимости сети пакетной передачи данных [Текст] / М. С. Ковалёв, П. С. Смородов // Новые информационные технологии в системах связи и управления : Тр. XII Рос. НТК / Мин-во промышленности и торговли РФ, ОАО «Концерн «Вега», ОАО «Калужский НИИ телемеханических устройств». – Калуга: Изд. ООО «Ноосфера», 2013. – 5 июня. – С. 283–286.

68. Ковалёв, М. С. Динамическая модель системы защиты информации с универсальным «скользящим» средством защиты [Текст] // Междун. конф. «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (RES-2014) ; Доклады ; Серия: науч. конф. посвящ. Дню радио / Рос. науч.-техн. общ. радиотехн., электрон. и связи им. А.С. Попова. – М. : ООО «Брис-М», 2014. – Вып. LXIX. – С. 418–420.

69. Ковалёв, М. С. Методика оптимизации размещения средств защиты объекта обработки информации [Текст] // Новые информационные технологии в системах связи и управления : Тр. XIII Рос. НТК / Мин-во промышленности и торговли РФ, ОАО «Концерн «Вега», ОАО «Калужский НИИ телемеханических устройств». – Калуга: Изд. ООО «Ноосфера», 2014. – С. 133–137.

70. Ковалёв, М. С. Исследование СМО с групповыми отказами и восстановлением обслуживающих приборов при примитивном входном потоке [Текст] / М. С. Ковалёв, И.А. Якимова // Сб. тр. VIII междун. НПК «Информационные и коммуникационные технологии в образовании, науке и производстве». – Протвино, 2014. – С. 745–748.

71. Ковалёв, М. С. Математическая постановка и решение задачи распределения средств защиты информации в узле коммутации сети передачи данных [Текст] // Новые информационные технологии в системах связи и управления : Тр. XIII Рос. НТК / Мин-во промышленности и торговли РФ, ОАО «Концерн «Вега», ОАО «Калужский НИИ телемеханических устройств». – Калуга: Изд. ООО «Ноосфера», 2015. – С. 190–194.

72 Ковалев М.С., Проблемы обнаружения компьютерных атак на нижних уровнях сетевой инфраструктуры [Текст] / Ковалев М.С., Пасечник Р.М., Евтушенко С.А., Гладушенко С.Г. // Междун. конф. «Радиоэлектронные устройства и системы для инфокоммуникационных технологий» (REDS-2017) ; Доклады ; Серия: науч. конф. посвящ. Дню радио / Рос. науч.-техн. общ. радиотехн., электрон. и связи им. А.С. Попова. – М. : ООО «БРИС-М», 2017. – Вып. LXXII. – С. 511–514.

73 Ковалёв, М. С. Создание правил для IDS/IPS на основе данных банков известных уязвимостей [Текст] / Пасечник Р.М., Евтушенко С.А., Гладушенко С.Г. // Новые информационные технологии в системах связи и управления : Тр. XVI Рос. НТК / Мин-во промышленности и торговли РФ, ОАО «Концерн «Вега», ОАО «Калужский НИИ телемеханических устройств». – Калуга: Изд. ООО «Ноосфера», 2017. – С. 64–68.

74. Ковалев М.С. и др. Технический проект СЧ ОКР. «Модуль-ИИФ». Главный конструктор Шиманов С.Н. - Серпухов МОУ «ИИФ», 2016. С. 79-95.

75. Кокарев, В. Н. Построение новой архитектуры информационной безопасности OSI / В. Н. Кокарев // М.: Сети, 1993. - № 4. - С. 35-41.

76. Коцыняк, М.А. Устойчивость информационно-телекоммуникационных сетей / М.А. Коцыняк, И.А. Кулешов, О.С. Лаута. – СПб.: Изд-во Политехн. Ун-та, 2013. – 92 с.

77. Краснов, А. В. Некоторые проблемы безопасности в сетях ЭВМ и способы их решения / А. В. Краснов // М.: Защита информации, 1992. - № 3,4.

78. Кураленко, А. И. Методика аудита информационной безопасности информационно-телекоммуникационной системы [Текст] : дис. ... канд. техн.

наук : 05.13.19 : защищена 28.12.15 / Кураленко Алексей Игоревич. – Томск, 2015. - 125 с.

79. Лёвин, В. Ю. Развитие методов и средств обеспечения целостности и конфиденциальности регистрируемой информации системы информационной безопасности организации воздушного движения [Текст] : дис. ... канд. физ.-мат. наук : 05.13.19 : защищена 29.11.10 : / Лёвин Валерий Юрьевич. – М., 2010. - 132 с.

80. Липаев, В. В. Надежность программного обеспечения АСУ / В. В. Липаев // М.: Финансы и статистика, 1983. - 263 С.

81. Липаев, В. В. Проектирование программных средств / В. В. Липаев // М.: Мир, 1990. - 301 С.

82. Ловцов, Д. А. Защита информации / Д. А. Ловцов // М.: Информатика и образование, 1995. - №4. - С.117-123.

83. Ловцов, Д. А. Введение в информационную теорию / Д. А. Ловцов // М.: 1996. - 434 С.

84. Ловцов, Д. А. Информационно-математическое обеспечение управления безопасностью эргатических систем. II Математические модели / Д. А. Ловцов, Н. А. Сергеев // М.: Научно-техническая информация, 1998. - Серия 2, № 6.

85. Мальцев, А. Администрирование системы защиты информации ViPNet версии 4.x / А. Мальцев, А. Чефранова, А. Белев // Изд-во «Беловодье», 2016. – 192 С.

86. Малюк, А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб, пособие для вузов. М: Горячая линия-Телеком, 2004. -280 с. ил.

87. Мафтик, С. Механизмы защиты в сетях ЭВМ: Пер. с англ. / С. Мафтик // М.: Мир, 1993. - 216 С.

88. Мельников, В. Защита информации. Учебник / В. Мельников , А. Куприянов , А. Схиртладзе // Изд-во «Академия», 2014. – 304 С.

89. Мельников, В. В. О концепции и оценке системы защиты информации от несанкционированного доступа в системах обработки данных / В. В. Мельников // М.: МИР ПК ДИСК, 1993. - № 1.

90. Мельников, Ю. Н. Достоверность информации в сложных системах / Ю. Н. Мельников // М.: Сов. Радио, 1973.

91. Месарович, М. Теория иерархический многоуровневых систем / М. Месарович, Д. Мако, Я. Такахара // М.: Мир, 1973.

92. Месси, Дж. Л. Введение в современную криптологию / Дж. Л. Месси // М.: ТИИЭР, 1988. - Т.76, № 5. - С.24-42.

93. Михалевич, В. С. Вычислительные методы исследования и проектирования сложных систем / В. С. Михалевич, В. Л. Волкович // М.: Наука, 1982. - 286 С.

94. Модели обеспечения достоверности и доступности информации в информационно-телекоммуникационных системах : монография / М. Ю. Монахов [и др.] ; Владим. гос. ун-т им. А. Г. и Н. Г. Столетовых. - Владимир : Изд-во ВлГУ. 2015. - 208 с.

95. Монахова, М. М. Модели и алгоритмы контроля инцидентов информационной безопасности в корпоративной телекоммуникационной сети [Текст] : дис. ... док. техн. наук : 05.12.13 / Монахова Мария Михайловна. - Владимир, 2016. - 137 с.

96. Монахов, М. Ю. Методы и модели обработки и представления информации в распределенных образовательных системах [Текст] : дис. ... док. техн. наук : 05.13.01 : защищена 22.06.05 : / Монахов Михаил Юрьевич. - Владимир, 2005. - 222 с.

97. Монахов, Ю. М. Вредоносные программы в компьютерных сетях [Текст] : учебное пособие для студентов высших учебных заведений, обучающихся по специальности 090104 "Комплексная защита объектов информатизации" / Ю. М. Монахов, Л. М. Груздева, М. Ю. Монахов ; М-во образования и науки Российской Федерации, Гос. образовательное учреждение высш. проф. образования Владимирский гос. ун-т

98. Мур, Дж. Х. Несостоятельность протоколов криптосистем / Дж. Х. Мур // М.: ТИИЭР, 1988. - Т.76, № 5. - С.94-104.

99. Никифоров, И. Уголовные меры борьбы с преступностью / И. Никифоров // М.: Защита информации. Кофидент, 1995. - № 5/3.

100. Новиков, С.Н. Защита информации в сетях связи с гарантированным качеством обслуживания / Учебное пособие. – Новосибирск: 2003. – 84 с.: ил.

101. Петраков, А Основы практической защиты информации. Учебное пособие / А. Петраков // Изд-во «Академия», 2013. – 492 С.

102. Петров, А. А. Компьютерная безопасность. Криптографические методы защиты. - М.: ДМК, 2000. - 448 с.: ил.

103. Петров, В. А. Информационная безопасность. Защита от несанкционированного доступа. Учебное пособие / В. А. Петров, А. С. Пискарев, А. В. Шеин // М.: МИФИ, 1995.

104. Петухов, Г. Б. Методологические основы внешнего проектирования целенаправленных процессов и целеустремленных систем / Г. Б. Петухов, В. И. Якунин. – М.: АСТ, 2006. – 504 С.

105. Расстригин, Л. А. Кибернетика как она есть / Л. А. Расстригин, П. С. Граве // М.: «Молодая гвардия», 1975. - 208 С.

106. Резников, Б. А. Системный анализ и методы системотехники. Ч. 1. Методология системных исследований / Б. А. Резников // МО, 1990. - 522 С.

107. Росляков, А.В. Виртуальные частные сети. Основы построения и применения. – М.: Эко-Тренз, 2006. – 304.: ил.

108. Рябко, Б. Я. Криптографические методы защиты информации / Б. Я. Рябко, А. Н. Фионов // Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2005. - 229 с.: ил.

ISBN 5-93517-265-8.

109. Симмонс, Г. Дж. Обзор методов аутентификации информации / Г. Дж. Симмонс // М.: ТИИЭР, 1988. - т. 76, № 5. - С. 106-125.

110. Стреляный, Т. Информационные войны. Человек и компьютер. / Т. Стреляный // Специальный выпуск,1998.

111. Сяо, Д. Защита ЭВМ. Пер.с англ / Д. Сяо, Д. Керр, С. Мэдник // М.: Мир, - 1982.

112. Сюнтюренко, О. В. Формирование норм защищенности информации в АСОД / О. В. Сюнтюренко // М.: Зарубежная радиоэлектроника, 1993. - № 7,8,9.

113. Ухлинов, Л. М. Принципы построения системы управления безопасностью данных / Л. М. Ухлинов // М.: Автоматика и вычислительная техника, 1990. - № 5. - С. 11-17.

114. Феллер, В. Введение в теорию вероятностей и ее приложения / В. Феллер // М.: Мир,1984. - Т. 2.

115 Федеральная целевая программа «Электронная Россия» (2002-2010 гг.). Утверждена постановлением Правительства РФ от 28 января 2002 г. №65.

116. Хоффман, Л. Дж. Современные методы защиты информации. Пер. с англ / Л. Дж. Хоффман // М.: Сов. Радио, 1980. - 263 С.

117. Холл, М. Комбинаторика / М. Холл // М.: Мир, 1970. - 127 С.

118. Уолкер, Б. Дж. Безопасность ЭВМ и организация их защиты: Пер. с англ / Б. Дж. Уолкер, Я. Ф. Блейк // М.: Связь, 1980.

119. Шаньгин, В. Комплексная защита информации в корпоративных системах / В. Шаньгин // Изд-во «Инфра-М», 2010. – 592 С.

120. Щербаков, А. Защита от копирования / А. Щербаков // М.: Эдэль, 1992.

121. G. J. Simmons «Cryptology», in Encyclopaedia Britannica, ed.16. Chicago, lt: Encyclopaedia Britannica inc., 1986, pp.913-9248.

122. D. Khan, The Codebreakers, The Story of Secret Writing, abridged ed. New York, NY: Signet, 1973.

123. R. S. Merkle and M. E. Hellman, «Hiding information and signatures trapdoor knapsacks», IEEE Trans. Informat. Theory, vol. IT-24, pp. 525-530, Sept. 1978.

124. A. Shamir, «A polinomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem», IEEE Trans. Informat. Theory, vol. IT-30, pp. 699-704, Sept, 1984.

125. T. Siegenthaler, «Correlation-immunitety of nonlinear combining functions for cryptographig applicftions», IEEE Trans. Informat. Theory, vol. IT-30, pp. 776-780, Sept. 1984.

126. J. L. Massey and I. Ingemarsson, «The Rip van Winkle cipher-A simple and provable computationalle secure cipher with a finite key», in IEEE Int/ Symp. On Informat. Theory, (Brighton, England),(abstr.), p. 146, June 24-28, 1985.

127. R. Rueppel, Analysis and Design of Stream Ciphers. New York, NY: Springer, 1986.

ПРИЛОЖЕНИЕ А

Перечень типовых сертифицированных средств защиты информации

№ п/п	Название	Разработчик	Описание	Приблизительная стоимость (руб)
1	Программное средство ЗИ Secret Net	Компания «Код Безопасности»	СЗИ от несанкционированного доступа на рабочих станциях и серверах	7000
2	Программно-аппаратное средство ЗИ «Соболь»	Компания «Код Безопасности»	Программно-аппаратный комплекс защиты ПЭВМ от несанкционированного доступа. Обеспечивает доверенную загрузку, контроль и регистрацию доступа пользователей к ПЭВМ, осуществляет контроль целостности программной среды и доверенную загрузку установленных операционных систем	10000
3	Программно-аппаратное средство Аккорд-АМДЗ	ОКБ «САПР»	Аккорд-АМДЗ обеспечивает защиту устройств и информационных ресурсов от несанкционированного доступа	От 9000 до 20000
4	Программное средство Страж NT	Научно-производственный центр «Модуль»	СЗИ от несанкционированного доступа на рабочих станциях и серверах.	От 6750 (в зависимости от количества хостов)
5	Аппаратно-программный комплекс шифрования «Континент»	Компания «Код Безопасности»	Аппаратно-программный комплекс, сочетающий в себе межсетевой экран, средство построения VPN-сетей и маршрутизатор	От 100000 и до 700000 (зависит от аппаратной части и набора СПО)
6	Программно-аппаратные межсетевые экраны StoneGate Firewall/VPN	Stonesoft Corporation	Линейка программных и программно-аппаратных МЭ с возможностью построения отказоустойчивых VPN, в том числе с использованием российских криптографических алгоритмов	От 30000 до 3000000 (зависит от аппаратной части и набора СПО)

7	Программно-аппаратное средство «Система обнаружения и предотвращения вторжений StoneGate IPS»	Stonesoft Corporation	Обеспечивает полный контроль каналов связи, проактивное предотвращение атак на критичные серверы и рабочие станции сети, а также уникальную возможность инспекции зашифрованного web-трафика	От 100000 до 3000000 (зависит от аппаратной части и набора СПО)
8	Аппаратно-программное средство StoneGate SSL VPN	Stonesoft Corporation	Обеспечивает удаленный защищенный доступ удаленных пользователей к корпоративным ресурсам на базе бесклиентской технологии SSL VPN	От 70000 до 2500000 (зависит от аппаратной части и набора СПО)
9	Программное средство XSpider	Positive Technologies	Система анализа защищенности, интеллектуальный сканер безопасности, используемый для анализа и контроля защищенности корпоративных ресурсов	От 2000 до 1000000 (от количества проверяемых хостов)
10	Программное средство КриптоПро CSP 3.6	КриптоПро	Криптопровайдер КриптоПро CSP предназначен для: авторизации и обеспечения юридической значимости электронных документов и проверки электронной цифровой подписи (ЭЦП); обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты	От 1000 до 25000 (в зависимости от платформы операционной системы)
11	Программное средство «Антивирус Касперского»	Лаборатория Касперского	Средство антивирусной защиты	От 2000
12	Программное средство Dr.Web	Dr.Web	Средство антивирусной защиты	От 2500
13	Программное средство VipNet	«ИнфоТеКС»	Межсетевой экран	От 3200

ПРИЛОЖЕНИЕ Б

Копии актов об использовании результатов диссертационной работы

Межрегиональное общественное учреждение
"Институт инженерной физики"
(Научное, образовательное и производственное учреждение)
ИИФ РФ

Большой Ударный пер., д. 1а, г. Серпухов, Московская обл., 142210
Адрес для закрытой переписки: Б.Ударный пер., д. 1а г. Серпухов Московская обл.
ОКПО 42232569, ОГРН 1035000008417, ИНН/КПП 5043014134/504301001
тел. 8(4967)353133; 351371; факс: 354420
e-mail: info@iifmail.ru; www.iifrf.ru
моб. 8(917)58 4874

_____ № _____
на № _____ от _____

УТВЕРЖДАЮ
Генеральный директор –
Первый Вице-президент Института
доктор технических наук, доцент
Д.В. Смирнов
«14» ноября 2016 г.

АКТ
об использовании основных результатов диссертационной работы
КОВАЛЕВА МАКСИМА СЕРГЕЕВИЧА
в МОУ «Институт Инженерной Физики»

Комиссия в составе:

председателя – начальника управления АСУ и связи, кандидата технических наук Прасолова В.А.;

членов комиссии:

старшего научного сотрудника, кандидата технических наук Карпочкина К.В,

старшего научного сотрудника Шломы В.И.,

составила настоящий акт о том, что основные результаты диссертационной работы Ковалева М.С. на тему «Оптимизация размещения средств защиты информации в узлах коммутации VPN сети», а именно:

- аналитические модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети,
- автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети,

использованы в СЧ ОКР «Модуль-ИИФ».

Председатель комиссии: В.А. Прасолов
Члены комиссии: К.В. Карпочкин
В.И. Шлома

ЦНИИ ЭИСУ

АКЦИОНЕРНОЕ ОБЩЕСТВО
«ЦЕНТРАЛЬНЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ
ЭКОНОМИКИ, ИНФОРМАТИКИ И СИСТЕМ УПРАВЛЕНИЯ»

Ул. Малая Бронная, 2/7, стр.1, Москва, 123104 Тел.: (495) 539-22-49 Факс: (495) 539-22-50 www.cniieisu.ru E-mail: cniieisu@cniieisu.ru ОКПО 07529749

_____ № _____
На № _____ от _____

«УТВЕРЖДАЮ»
Директор по специальным проектам
кандидат технических наук
А.Фортинский
«__» января 2017 г.

А К Т
об использовании основных результатов диссертационной работы
КОВАЛЕВА МАКСИМА СЕРГЕЕВИЧА в АО «ЦНИИ ЭИСУ»

Комиссия в составе:
председателя - директора центра, кандидата технических наук,
Полещука В.В.;
членов комиссии:
директора центра, кандидата технических наук, доцента
Кокорина Н.И.;
начальника отдела, кандидата технических наук Слабова Р.И.
составила настоящий акт о том, что основные результаты диссертационной работы Ковалева М.С., на тему «Оптимизация размещения средств защиты информации в узлах коммутации VPN сети»:

-аналитические и имитационная модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети;

- автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат,

использованы при обосновании размещения средств защиты информации в узлах коммутации VPN сети специального назначения в рамках ОКР «Заполье» и ОКР «Ретранслятор».

Председатель комиссии: В.Полещук

члены комиссии: Н.Кокорин

Р.Слабов

УТВЕРЖДАЮ
Заместитель начальника филиала
ВА РВСН им. Петра Великого
по учебной и научной работе
кандидат технических наук, доцент
полковник
А. Людоговский
«26» января 2017 года

А К Т
об использовании результатов диссертационной работы
КОВАЛЁВА МАКСИМА СЕРГЕЕВИЧА
в образовательной деятельности ВА РВСН им. Петра Великого
(филиал в г. Серпухов Московской области)

Комиссия в составе:

председателя – начальника учебно-методического отдела филиала ВА РВСН им. Петра Великого кандидата технических наук, доцента, полковника Сивоплясова Д.В.;

членов комиссии:

начальника кафедры №41 кандидата технических наук, полковника Кабановича С.Г.;

заместителя начальника кафедры №41, кандидата технических наук, подполковника Чайкова С.С.

составила настоящий акт о том, что результаты диссертационной работы Ковалёва М.С. на тему «Оптимизация размещения средств защиты информации в узлах коммутации VPN сети», а именно:

- аналитические и имитационная модели воздействия нарушителя на многоэшелонированную систему защиты информации в информационных объектах сети;

- автоматизированная методика оптимизации размещения средств защиты информации на информационных объектах сети, позволяющая повысить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат

использованы в образовательной деятельности филиала академии при проведении практических занятий по дисциплине «Криптографические методы и средства защиты информации».

Председатель комиссии: полковник Д. Сивоплясов

Члены комиссии: полковник С. Кабанович

подполковник С. Чайков

«26» января 2017 г.