На правах рукописи

КОВАЛЕВ МАКСИМ СЕРГЕЕВИЧ

ОПТИМИЗАЦИЯ РАЗМЕЩЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В УЗЛАХ КОММУТАЦИИ VPN СЕТИ

Специальность: 05.12.13 Системы, сети и устройства телекоммуникаций

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Владимир 2017

Работа выполнена в Межрегиональном общественном учреждении «Институт инженерной физики» (г. Серпухов)

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

Официальные оппоненты: **Куприянов Александр Ильич** доктор технических наук, профессор, профессор Московского авиационного института (национального исследовательского университета), г. Москва.

Мазин Анатолий Викторович доктор технических наук, доцент, заведующий кафедрой «Информационная безопасность автоматизированных систем» Калужского филиала федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» г. Калуга.

Ведущая организация: АО «Калужский научно-исследовательский институт телемеханических устройств» г. Калуга.

Защита состоится «10» октября 2017 года в 14^{00} на заседании диссертационного совета ДС 212.025.04 при Владимирском государственном университете имени Александра Григорьевича и Николая Григорьевича Столетовых по адресу: 600000, г. Владимир, ул. Горького, д.87, ВлГУ.

Отзывы, заверенные печатью, просим направлять по адресу: 600000, г. Владимир, ул. Горького, д.87, ВлГУ.

С диссертацией можно ознакомиться в библиотеке Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых и на сайте http://diss.vlgu.ru

Автореферат разослан «30» июня 2017 г.

Ученый секретарь диссертационного совета
Д 212.025.04
доктор технических наук, профессор

А.Г. Самойлов

I. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность: 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.

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. При этом внутри транспортной сети также имеются свои маршрутизаторы.

Одной из важных задач, решаемых VPN сетью, является задача обеспечения устойчивости функционирования самой сети, а также обеспечение безопасности циркулирующей в ней информации. 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.

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. Все это приводит к огромным материальным и финансовым потерям (ущербу).

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. 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.

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

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 выделенной 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.

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 ИОС 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».

Целью диссертационных исследований является повышение уровня информационной безопасности комплекса технических средств организации защищенного канала связи в VPN сети.

Объектом исследования является комплекс технических средств организации защищенного канала связи в VPN сети.

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

Для достижения поставленной цели в диссертационной работе решена **научная задача:** 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.

Основными направлениями исследования являются:

- 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 ИОС VPN сети.

Основные 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 результатов:

1. 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.

2. 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 результатов, полученных в диссертационной работе, подтверждается 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 результатов диссертационного исследования заключается 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%.

Результаты исследований представляют практический интерес для научно-исследовательских учреждений и проектных организаций с целью усовершенствования существующих и создания перспективных адаптивных ППК. Кроме того, результаты работы могут быть использованы в вузах при изучении учебных дисциплин, соответствующих тематике данной диссертационной работы.

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 26.01.2016 г.).

Апробация работы и публикации. Основные результаты работы докладывались, обсуждались и были одобрены на LXIII - LXXII научной сессии Российского НТОРЭС имени А.С. Попова, посвященной Дню радио (Москва, 2008 – 2017 г.г.); на Российской НТК «Новые информационные технологии в системах связи и управления» (Калуга, 2009-2017); на Российской НТК «Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем» (Серпухов, 2009-2013 г.).

Работа выполнена лично автором и является результатом исследований, в которых автор принимал непосредственное участие в течение последних 9 лет. За это время непосредственно по теме диссертации опубликовано 31 работа, в том числе: 29 научных статей (5 статьи в журналах из Перечня ВАК), 1 отчёт об ОКР и получен 1 патент на полезную модель.

Структура и объём работы. Диссертация состоит из введения, трех разделов, заключения, двух приложений, списка использованной литературы, и изложена на 156 страницах машинописного текста. В список использованной литературы внесено 127 научных источников.

II. СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность темы диссертации, сформулирована цель и задача исследования, изложены научные результаты, представляемые к защите, приведены аннотация и структура работы.

В первом разделе проведён обобщенный анализ принципов организации VPN сетей с помощью комплекса технических средств, включающего средства хранения ключевой информации, средства обмена ключевой информации, СЗИ от несанкционированного доступа на рабочих станциях и серверах (таких как Secret Net), программно-аппаратные комплексы защиты ПЭВМ от несанкционированного доступа (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), а также различное антивирусное ПО. Показано, что существует несколько вариантов технической реализации VPN сетей, отличающихся производительностью и стоимостью: VPN на базе межсетевых экранов, маршрутизаторов, программного обеспечения и специализированных аппаратных средств. В свою очередь можно выделить следующие варианты взаимного расположения VPN-устройств в сети:

- 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.

Учитывая комплексный характер системы защиты информации (СЗИ) информационно-телекоммуникационной сети (ИТС), задача синтеза качественной СЗИ и эффективных алгоритмов ее функционирования формулируется 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 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:

$$\text{Найти: } \{X\} \subset \{X^{\partial}\} \Rightarrow Y_0 \geq Y^{mp} \Rightarrow W \geq W^{mp} \quad , \qquad (1)$$

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

По своему характеру задача (1) является оптимизационной и состоит в

выборе такого набора значений $\{X\} \subset \{X^{\partial}\}$, который бы при условии некоторого подмножества входных воздействий – $\{Z\}$, обеспечил экстремум функционала полезности, задающего математическую модель СЗИ с ограничениями на $\{Y\}$, $\{R\}$, $\{T\}$ и допустимые $\{X\}$: $Y = F\{X(S,A,L),Z,T\}$ (2)

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

В качестве показателя качества СЗИ выбран комплексный показатель атрибутивных свойств: $K = \langle k_1, k_2, ..., k_n \rangle$, (3)

где k_i - показатель *i*-го атрибутивного свойства.

Для формирования критерия выбора того или иного варианта построения СЗИ, выбран следующий принцип принятия решения. Если показатель качества, выбранного *j*-го варианта системы, описывается кортежем частных атрибутивных свойств (3), а показатель допустимого качества

$$K^{\partial} = \langle k_1^{\partial}, k_2^{\partial}, ..., k_n^{\partial} \rangle \quad (4)$$

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:

$$G: \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial np}\right) \cong U, \ j = \overline{1,m} \quad (5)$$

$$O: \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial np}\right) \cap \left(K_{\langle n \rangle}^{j} = K_{\langle n \rangle}^{onm}\right) \cap \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial onm}\right) \cong U, \ j = \overline{1,m} \quad (6)$$

$$S: \left(K_{\langle n \rangle}^{j} \in K_{\langle n \rangle}^{\partial np}\right) \cap \left(K^{j} \geq\leq K^{l}\right) \cong U, \ j = \overline{1,m}, \ l = 1, L, \ j \neq l, \quad (7)$$

где *U* - символ достоверного события.

В (5) - (7) $K^{\partial np}$, $K^{\partial onm}$ - соответственно области допустимых значений показателя качества пригодной и оптимальной СЗИ.

В итоге получена формальная постановка задачи в виде:

Пусть защита объекта $A_i \in A, \ i = \overline{1,n}$ определяется выбором совокупности M_j средств и методов защиты информации (механизмов) $j = \overline{1,k}$, характеризующихся подуровнями защиты L_j. $C_{\Sigma}(M)$ – суммарная стоимость реализации 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 $P_{\Sigma}(M_i)$, суммарной стоимостью взлома всех механизмов $C_{B\Sigma}$, а также суммарными временными затратами $T_{B\Sigma}$, 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 $C_{Д\Sigma}$. Событие взлома *j*-го механизма определяет ве-

личину 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

$$M_r(w_i) \cup m_i(w_j) \subseteq M(w_j),\ j = \overline{1,r},\ r = \overline{1,\sigma}. \quad (8)$$

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

$$Y(w_i): Y_r \subseteq Y^T \forall r \quad (9)$$

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 $M_r(w_i) \subseteq M(w_i),\ r = \overline{1,\sigma}$ (10)

и может быть формализована в следующем варианте:

Минимизировать величину ущерба, нанесенного информации в результате взлома всех механизмов защиты объекта A_i:

$$W(w_i) = \sum_{i=1}^{M} c_i \cdot P_{\Pi i} \to \min \quad (11)$$

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

$$\begin{cases} C_\Sigma(M) = \sum_{i=1}^{K} C_i \le C_u \\ T_{B\Sigma} = \tau_n \cdot \sum_{i=1}^{M} n_i \le T_{доп} \\ \sum_{i=1}^{M} a_i \le K \end{cases} \quad (12)$$

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 злоумышленника, а затем уже решать задачи оценки наносимого ущерба, а также способов и

средств его снижения.

Во втором разделе на основе анализа известных моделей воздействия нарушителя были сформированы логико-вероятностные модели следующих типов:

1. Простая вероятностная модель воздействия, в соответствии с которой вероятность непреодоления системы защиты с *k* попыток равна

$$P_{n}^{(k)} = 1 - \left(1 - P_{n}^{(1)}\right)^{k};\ P_{нп}^{(k)} = 1 - P_{n}^{(k)} = \left(P_{нп}^{(1)}\right)^{k}, \tag{13}$$

2. Простая эшелонированная модель, в соответствии с которой вероятность непреодоления системы защиты $P_{нп_m}^{(k)}$ с *k* попыток при однородности всех эшелонов защиты равна:

$$P_{нп_m}^{(k)} = \left(1 - \left(P_{ni}^{(1)}\right)^{m}\right)^{k}, \tag{14}$$

а если эшелоны защиты неоднородны ($P_{n1} \neq P_{n2} \neq ... \neq P_{ni} \neq P_{nm}$), то выражение (14) примет вид:

$$P_{нп_m}^{(k)} = \left(1 - \left(\prod_{i=1}^{m} P_i\right)\right)^{k}. \tag{15}$$

3. Модель очаговой системы защиты, т.е. при наличии обходных путей взлома объектов ТСИ. Для оценки защищенности информации в такой модели можно использовать следующий подход:

- вероятность преодоления системы преград с одной попытки:

$$P_{n}^{(1)} = P_{nn} \cdot P_{n}^{(1)} + P_{нпп} - P_{nn} \cdot P_{n}^{(1)} \cdot P_{нпп}, \tag{16}$$

- вероятность непреодоления с одной попытки:

$$P_{нпр}^{(1)} = 1 - P_{пр}^{(1)}, \tag{17}$$

- вероятность преодоления с *k* попыток:

$$P_{пр}^{(k)} = 1 - \left(1 - P_{пр}^{(1)}\right)^{k}, \tag{18}$$

- вероятность непреодоления с *k* попыток:

$$P_{нпр}^{(k)} = 1 - P_{пр}^{(1)}, \tag{19}$$

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

Логическим продолжением исследования предметной области стали разработанные аналитические модели воздействия следующего содержания:

1. Простая марковская модель защиты.

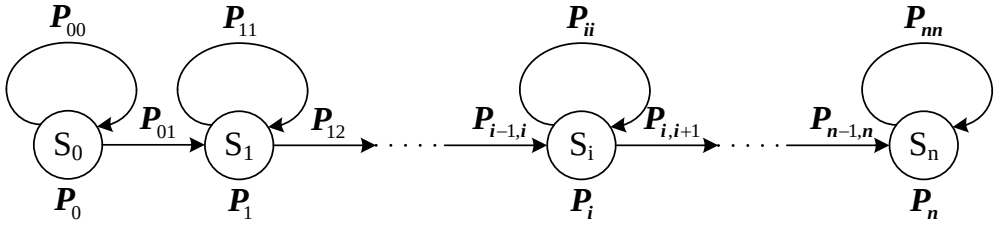

Рисунок 1 – Граф состояний и переходов при простой модели защиты

Матрица переходных вероятностей для такого процесса примет вид

(20), а вероятность преодоления системы защиты за k попыток будет определяться по уравнению Колмогорова – Чепмена (21):

$$P_{[n+1,n+1]} = \begin{vmatrix} P_{00} & P_{01} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & P_{11} & P_{12} & \dots & 0 & 0 & \dots & 0 \\ 0 & 0 & P_{22} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & P_{ii} & P_{ii+1} & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & P_{i+1i+1} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 1 \end{vmatrix} \quad (20)$$

$$P^{(k)}_{\langle n+1\rangle} = P^{(0)}_{\langle n+1\rangle} \cdot P^{k}_{[n+1,n+1]} = P^{(k-1)}_{\langle n+1\rangle} \cdot P_{[n+1,n+1]}, \quad (21)$$

где вектор начальных вероятностей состояний $P^{(0)}_{<n>} = (1 \quad 0 \quad 0 \quad 0 \quad \dots \quad 0)$ (22)

2. Марковская модель с восстановлением

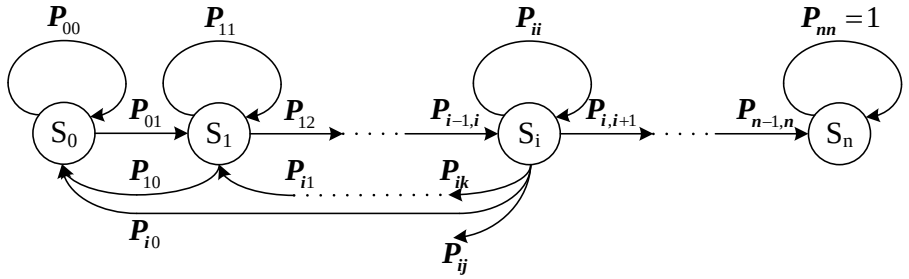

Рисунок 2 – Граф состояний и переходов при модели с восстановлением

При этом расчеты проводятся аналогично предыдущей модели.

3. Марковская модель очаговой системы защиты

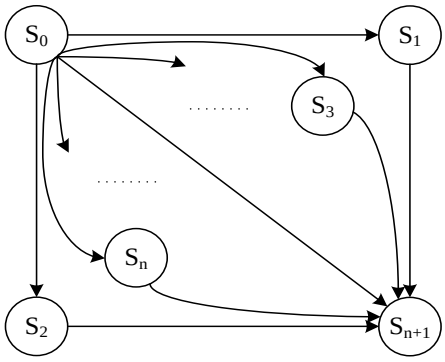

Рисунок 3 – Граф состояний и переходов при модели очаговой защиты

Матрица вероятностей переходов имеет вид (23), методика оценки вероятности преодоления остается аналогична предыдущим моделям.

$$P_{[n+2,n+2]} = \begin{vmatrix} 0 & P_{nn1} & \dots & P_{nn3} & \left(P_{обх1} + P_{обх2} + \dots + P_{обхк}\right) \\ 0 & \left(1 - P_{nn1}\right) & \dots & 0 & P_{n1} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \left(1 - P_{n3}\right) & P_{n3} \\ 0 & 0 & \dots & \dots & 1 \end{vmatrix} \quad (23)$$

Также во втором разделе разработана имитационная модель воздействия, программная реализация которой представлен на рисунке 4.

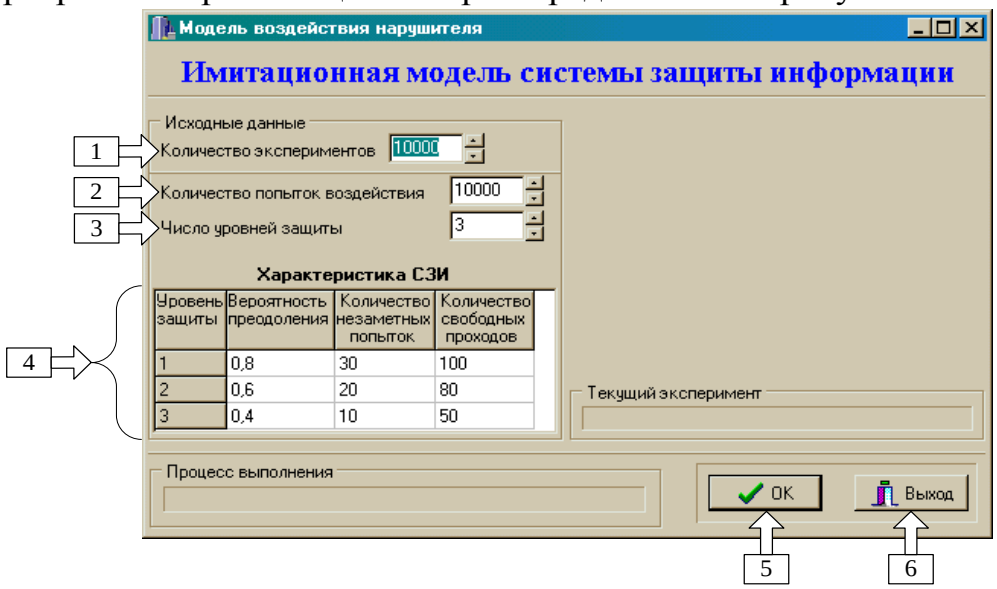

Рисунок 4 – Основной экран ПС имитационно модели

Адекватность разработки модели подтверждена сходимостью ее результатов с результатами математического моделирования с помощью марковских моделей при одинаковых исходных данных.

В третьем разделе на основе сформированных математических и имитационной моделей защиты была получена методика оптимального размещения средств защиты информации на объектах ИТС, основные этапы которой представлены на рисунке 5.

При этом оценка частных ущербов от действий злоумышленников оценивалась по формуле:

$$W[N] = \sum_{j=1}^{M} C_j \left[1 - \left(1 - P_j \right)^{n_j} \right], \qquad (24)$$

где $W = \sum_{j=1}^{M} w_j$ – суммарный вероятный ущерб, наносимый M массивам информации; $w_i = C_j P_{Пj}$; C_j – коэффициенты относительной важности (стоимости) хранимой информации; $P_{Пj}$ – вероятность взлома защиты.

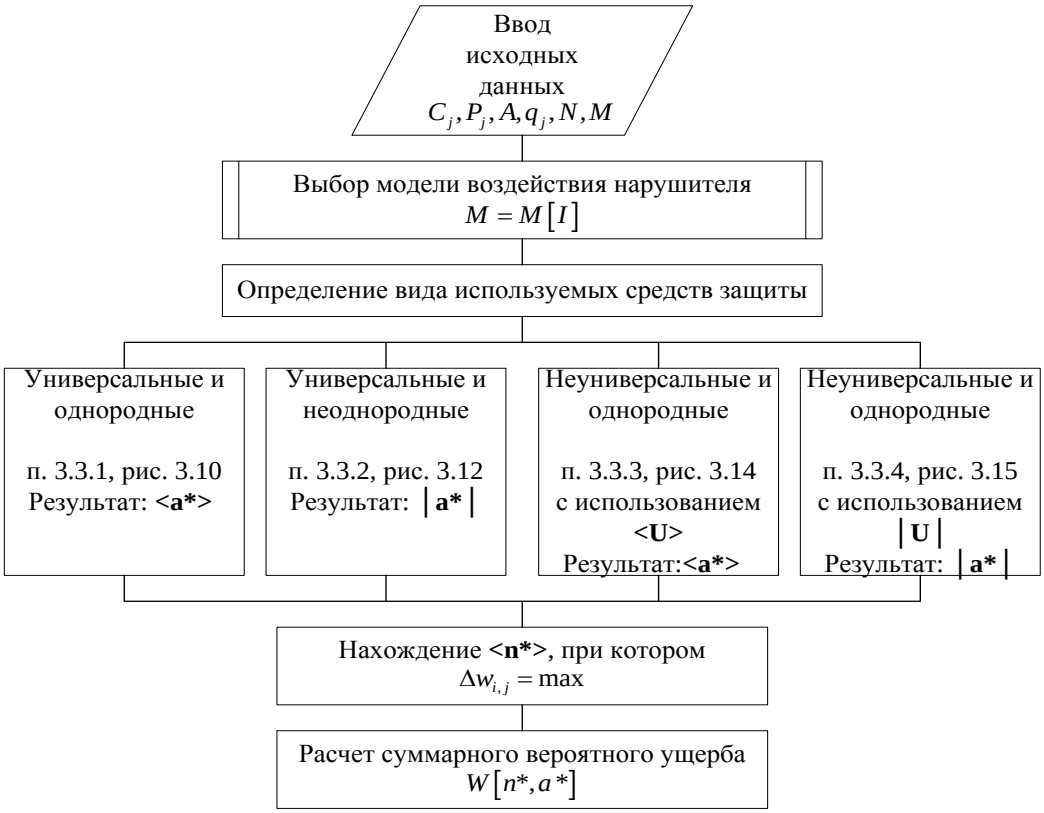

Рисунок 5 – Основные этапы методики оптимизации размещения СЗИ

Необходимо отметить, что в зависимости от однотипности и однородности средств защиты методика оптимизации размещения СЗИ обладает определёнными особенностями, и результаты её применения также имеют разницу.

Разработанная методика оптимизации размещения СЗИ нашла своё воплощение в виде программного продукта, интерфейс которого представлен на рисунке 6.

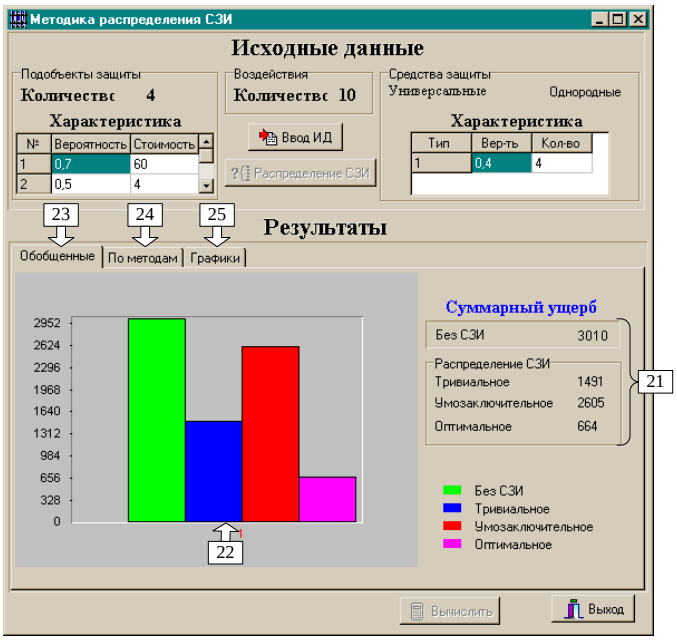

Рисунок 6 – Основной экран программного средства с результатами расчетов

Проведённые с его помощью расчёты относительного ущерба от воздействия злоумышленников на объекты ТСИ при типовых исходных данных представлены на рисунке 7. В качестве СЗИ предполагается аппаратно-программный комплекс шифрования «Континент» и программно-аппаратное средство ЗИ «Соболь».

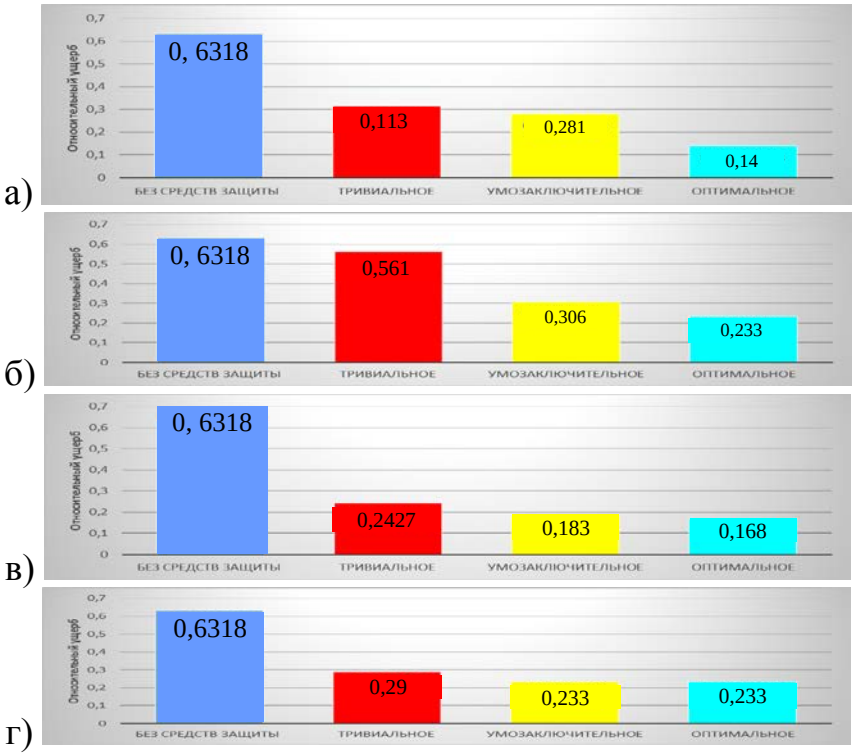

Рисунок 7 – результаты расчётов ущерба от воздействия злоумышленников

а) Средства защиты однородные и универсальные
б) Средства защиты неоднородные и универсальные
в) Средства защиты однородные и не универсальные
г) Средства защиты неоднородные и не универсальные

Из анализа графиков следует, что применение разработанной методики оптимизации размещения СЗИ позволяет существенно снизить ущерб от действий злоумышленников по сравнения с тривиальным и умозаключительным методом распределения СЗИ на объектах ТСИ.

При увеличении количества СЗИ и попыток воздействия наблюдается увеличение положительного эффекта от применения предлагаемого методического аппарата, что наглядно иллюстрируют гистограммы на рисунке 8.

Незначительное увеличение времени расчетов значений ущерба при усложнении задачи оптимизации свидетельствует о применимости разработанного программно-методического аппарата для решения более объемных задач.

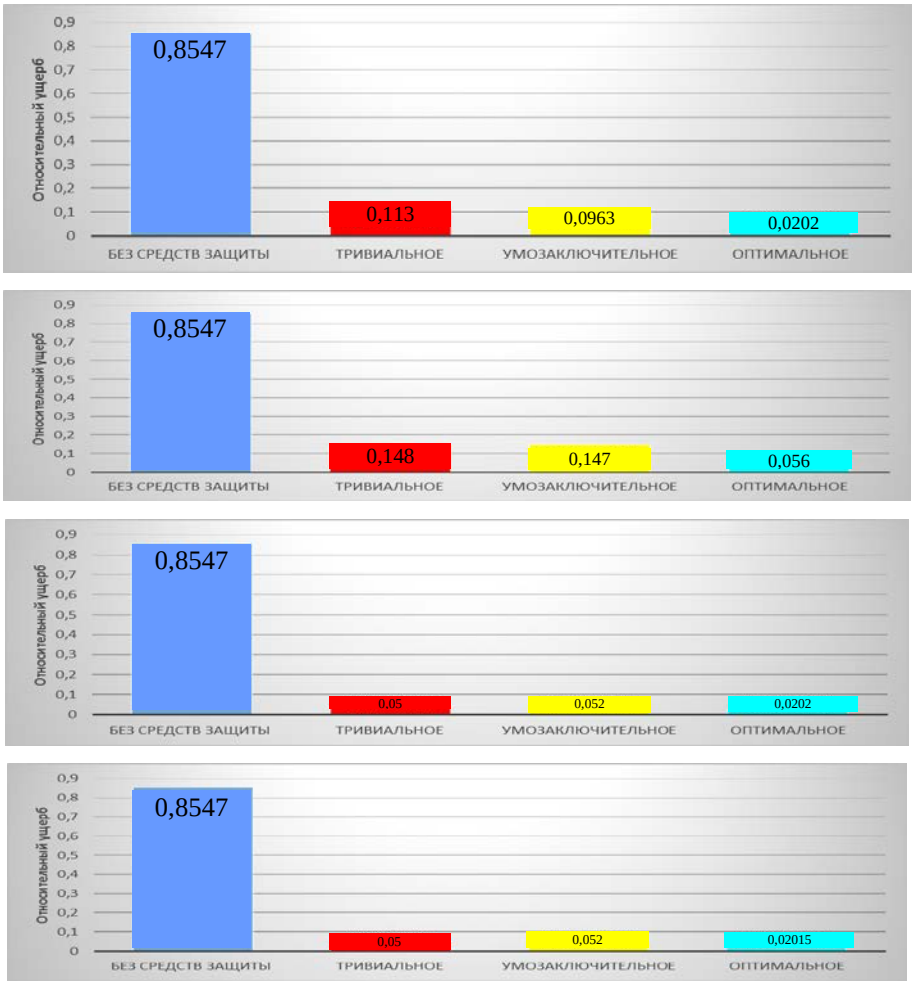

Рисунок 8 – Диаграммы ущербов по всем методам распределения СЗИ

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

III. ЗАКЛЮЧЕНИЕ

В результате проведенного диссертационного исследования решена актуальная, имеющая важное для развития информационно-телекоммуникационных сетей задача научного обоснования 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.

В области теоретических исследований получены следующие основные результаты:

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 повы-

сить эффективность функционирования защиты информации без дополнительных существенных финансовых затрат.

В работе доказано, что 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, может быть снижен до 2 - х раз.

Разработанная методика позволяет при различных исходных данных получить минимально возможное однозначное количественное значение показателя суммарного вероятного ущерба.

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

Дальнейшие исследования целесообразно продолжить в области повышения уровня защищенности информации в ИОС ИТС за счёт создания комплекса перспективных средств защиты информации.

Список основных трудов, опубликованных по теме диссертации

1. 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.

2. 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.

3. 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.

4. 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.

5. 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

6. 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.

7. 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. – Калуга: Изд. ООО «Ноосфера», 2009. – 4-5 июня. – С. 494–498.

8. 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.

9. 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.

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

11. Ковалёв, М. С. Многомерная модель разграничения доступа в объектно-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 «Информпресс-94», 2011. – Вып. LXVI. – С. 34–35.

12. 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». – Калуга: Изд. ООО «Ноосфера», 2011. – 1-2 июня. – С. 313–315.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. Патент № 108702 на полезную модель РФ, МПК H03K 3/00. Генератор псевдослучайной последовательности / Заявитель и патентообладатель СВИ РВ. – № 2011113222/08; заявл. 05.04.2011. Цимбал В.А., Попов М.Ю., Ковалев М.С.

22. Технический проект СЧ ОКР. «Модуль-ИИФ». Главный конструктор Шиманов С.Н. - Серпухов МОУ «ИИФ», 2016. С. 79-95.

Подписано в печать 28.06.2017 г.
Формат 60х84/16. Усл. печ. л. 1,25. Тираж 100 экз. Заказ
Издательство
Филиала Военной академии
Ракетных войск стратегического назначения имени Петра Великого
(г. Серпухов Московской области)
142210, г. Серпухов, ул. Бригадная, д.17