УДК 621.383

05.00.00 Технические науки

ПРОЕКТИРОВАНИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ ВОЕННОГО НАЗНАЧЕНИЯ

Хисамов Франгиз Гильфанетдинович
Доктор технических наук, профессор
Краснодарское высшее военное училище, Краснодар, Россия

Лойко Валерий Иванович
Заслуженный деятель науки РФ, доктор технических наук, профессор
Кубанский государственный аграрный университет, Краснодар, Россия

Шерстобитов Роман Сергеевич
Адъюнкт
Краснодарское высшее военное училище, Краснодар, Россия

В работе разработано структурное моделирование оптимального выбора средств защиты информации при проектировании автоматизированных систем в защищенном исполнении при переходе к сетецентрическим методам управления войсками и оружием

Ключевые слова: АВТОМАТИЗИРОВАННАЯ СИСТЕМА В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП

Doi: 10.21515/1990-4665-126-037

UDC 621.383

Technical sciences

DESING OF AUTOMATED SYSTEMS IN SECURED EXECUTION OF MILITARY USE

Khisamov Frangiz Gilfanetdinovich
Dr.Sci.Tech., professor
Krasnodar high military academy, Krasnodar, Russia

Loyko Valeriy Ivanovich
Honoured science worker of the Russian Federation, Dr.Sci.Tech., professor
Kuban state agrarian university, Krasnodar, Russia

Sherstobitov Roman Sergeevich
Postgraduate student
Krasnodar high military academy, Krasnodar, Russia

In the work we have developed a structural modeling of the optimal choice of information security devices in the design of automated systems in the protected execution in the transition to network centric methods of control of troops and weapons

Keywords: AUTOMATED SYSTEM IN SECURE EXECUTION, INFORMATION SECURITY SYSTEM, INFORMATION SECURITY DEVICES, ILLEGAL ACCESS

Обеспечение безопасности государства в информационной сфере является вопросом обеспечения национальной безопасности Российской Федерации (РФ). Информационные технологии и автоматизация информационных процессов приобрели всеобъемлющий характер и стали привычной частью жизнедеятельности личности и государства.

Важнейшую роль в информационной инфраструктуре РФ, в связи с широкой информатизацией общества, внедрением компьютерных технологий в сферу управления объектами гражданского и военного назначения, играют автоматизированные системы (АС), надежная работа

которых имеет исключительное значение для обороноспособности страны, устойчивого развития экономики и социальной сферы, защиты суверенитета государства в самом широком смысле этого слова.

В этих условиях возрастает угроза кибератак в отношении государственных систем управления жизненно важными объектами: транспортом, связью, энергетикой, банками, оружием и Вооруженными Силами в целом, которые относятся к критическим объектам [1,2].

Не случайно, в принятой в декабре 2016 года Доктрине информационной безопасности Российской Федерации [3] подчеркивается, что «…национальными интересами в информационной сфере является обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы, агрессии и в военной время».

Целевые кибератаки известны достаточно давно, но в последнее время о них заговорили особенно активно. Между тем, по оценкам профессиональных экспертов Positive Technologies [4] большинство кибератак не являются технически изощренными, использование ранее не известных уязвимостей составляет менее чем в 20% случаев. Злоумышленники чаще всего идут в атаку с минимальными затратами, используя известные уязвимости.

Преднамеренное или непреднамеренное разрушение, перехват, а также модификация циркулирующей в системах управления критическими объектами информации может привести к авариям, разрушениям с материальными потерями и человеческим жертвами. Вероятность таких событий возрастает в особые периоды функционирования АС, например, в ходе военных конфликтов или других кризисных ситуаций, когда следует ожидать массированного применения средств радиоэлектронного

подавления и перехвата. Поэтому одной из важных задач является надежная защита информации ограниченного распространения, циркулирующей в системах управления критическими объектами от подавления, перехвата и модификации посторонними лицами в повседневных условиях и в особые периоды их функционирования [1,2].

Особенно актуально данная проблема стоит перед Вооруженными Силами (ВС), где успешное функционирование критических объектов в мирное и особенно в военное время полностью определяется надежностью, устойчивостью, непрерывностью и скрытностью управления. Наглядным подтверждением тому служит опыт многочисленных локальных войн в последние 10-15 лет, включая военные действия на территории СНГ, Балканах, Ближнем Востоке, а также борьбу с международным терроризмом в Сирии и Ираке [1].

С появлением технологии сетецентрических войн, ракетно-ядерного и высокоточного оружия, широкой информатизацией военного управления и внедрения автоматизированных систем управления войсками (АСУВ), а также с принятием на вооружение передовыми странами мира новейших средств ведения радиоэлектронной войны, роль и значение криптографических методов защиты информации неизмеримо возрастают.

В принятой Доктрине информационной безопасности Российской Федерации [3] прямо указывается на «…необходимость совершенствования системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства».

В связи с этим, исключительно важное значение приобретают вопросы проектирования автоматизированных систем в защищенном исполнении (АСЗИ), обрабатывающих информацию ограниченного распространения. Широкое применение локальных и глобальных сетей для

передачи данных еще более усугубляет проблему обеспечения информационной безопасности, так как создаются возможности удаленного несанкционированного доступа к управляющей информации и вычислительному процессу в целом, например, через корпоративные ресурсы, включая веб-сервисы. Такие атаки неуклонно возрастают, только в прошедшем году их рост составил 30% [4]. Это обусловлено тем, что зачастую веб-сервис дает прямой доступ к корпоративной инфраструктуре и конфиденциальным данным. Проведенный анализ показывает, что за последние три года доля веб-приложений, где обнаруживаются критически опасные уязвимости, выросла до 70% [4]. В связи с этим возникает весьма актуальная и практически значимая задача обеспечение защиты информационных ресурсов и процессов в АСЗИ от несанкционированного доступа (НСД), уничтожения, модификации и искажения, циркулирующей в них информации.

Данные задачи в АСЗИ выполняют системы защиты информации (СЗ), задача построения которых вследствие интенсивного развития современных информационных технологий и средств телекоммуникаций выходит на передний план при проектировании и создании автоматизированных систем защищенного исполнения [7-9].

СЗ являются сложными системами, использующими организационные меры, программный и технический инструментарий и являются подсистемой самой АСЗИ, ориентированной на задачи информационной безопасности [5-9]. Основой СЗ является комплекс средств защиты информации (КСЗИ), представляющий собой сложный массив программных и технических средств и элементов, характеризующийся большим количеством разнородных параметров.

Следовательно, повышение эффективности процесса разработки СЗ требует совершенствования существующего и разработки нового методического обеспечения, охватывающего различные задачи и этапы

процесса проектирования, которое должно основываться на создании соответствующего математического обеспечения и реализовываться в программном обеспечении, что позволит повысить качество и автоматизировать основные этапы проектных работ [9]. Такие методики должны охватывать и техническую, и программную стороны формируемых КСЗИ, учитывать многоэтапность его разработки, включать в себя целый ряд процедур синтеза и анализа, характерных как для разработки различных программно-методических и программно-технических комплексов, а также учитывать специфику СЗ особенно на начальном этапе проектирования. Так как ошибки, допущенные на начальном этапе проектирования, как правило, приводят к необходимости пересмотра всех последующих этапов создания АСЗИ для устранения проблем, связанных с неверными решениями, допущенными в начале проектирования.

При разработке КСЗИ требуется решать два типа задач: осуществить синтез (структурный и параметрический) проектируемого комплекса в рамках возможных угроз и каналов утечки информации и провести анализ его эффективности в процессе функционирования с целью выбора наиболее эффективных в заданных условиях способов и средств защиты информации (СрЗИ). При этом решение таких задач осложняется тем, что для каждого структурного элемента КСЗИ и выполняемой функции возможно применение различных программных и технических средств, во множестве представленных на рынке [6]. Следовательно, возможно построить множество вариантов КСЗИ в конкретном АСЗИ, отличающихся структурой, составом, технико-экономическими показателями (быстродействие, надежность, стоимость и т.д.).

Так как большинство подобных показателей взаимно противоречивы, то выбор конкретного КСЗИ на основе принципа «необходимой достаточности» приводит к необходимости решать оптимизационную

задачу, что требует наличия набора показателей эффективности защиты информации и соответствующих критериев оптимальности построения комплекса. Одной из важнейших таких задач является выбор из множества имеющихся (сертифицированных) СрЗИ, которые позволяют получить наиболее рациональную структуру и в ее рамках сформировать состав конкретного КСЗИ, который обеспечивает перекрытие всех выявленных каналов утечки и НСД с заданной эффективностью [7,8].

Анализ содержания этапов разработки КСЗИ и входящих в них процедур позволяет сделать вывод, что они содержат задачи как слабоформализуемые, требующие для выполнения квалифицированных специалистов, привлечения экспертов, применения эвристических методов и подходов, так и такие, которые могут быть формализованы в рамках задач и методов структурного синтеза с привлечением положений теории математического программирования (формирование структуры КСЗИ, оптимальный выбор состава СрЗИ), а также на основе методов математического моделирования случайных процессов и систем (расчет, оценка и анализ показателей эффективности СрЗИ и КСЗИ в целом).

Используемые в настоящее время подходы к построению методического обеспечения для решения рассмотренных задач, имеющиеся методики и алгоритмы не носят комплексного характера, недостаточно учитывают взаимосвязь и взаимозависимость частных задач, не уделяют достаточного внимания вопросам оптимальности формирования и выбора наиболее рациональных вариантов КСЗИ с учетом требуемых значений показателей эффективности. Общим недостатком многих работ, особенно рассматривающих задачу создания СЗ в формальной постановке, является слабое применение в целевых функциях и ограничениях основного показателя эффективности, связанного с вероятностными характеристиками функционирования СрЗИ и КСЗИ в целом.

Таким образом, задача развития и разработки методического обеспечения формирования структуры, оптимального выбора состава СрЗИ и оценки показателей эффективности КСЗИ при проектировании СЗ в АСЗИ является весьма актуальной.

Ниже, на основе анализа руководящих документов и научных источников по вопросам защиты информации от НСД, проведено структурное моделирование процесса проектирования СЗ для АСЗИ в виде алгоритма, показанного на рис. 1. Сформулированные в соответствии с данным алгоритмом основные этапы и мероприятия позволяют обеспечить в ходе проектирования оптимальный состав КСЗИ.

1. Анализ проектируемой АС. На данном этапе анализируется информации о создаваемой АС. Определяется ее предназначение и выполняемые функции. Анализируется структура, информационная и функциональная архитектура АС, создаются и применяются различные базы данных информационных ресурсов АС и связей между ними, а также со сторонними информационными сетями. Выделяются особенности размещения

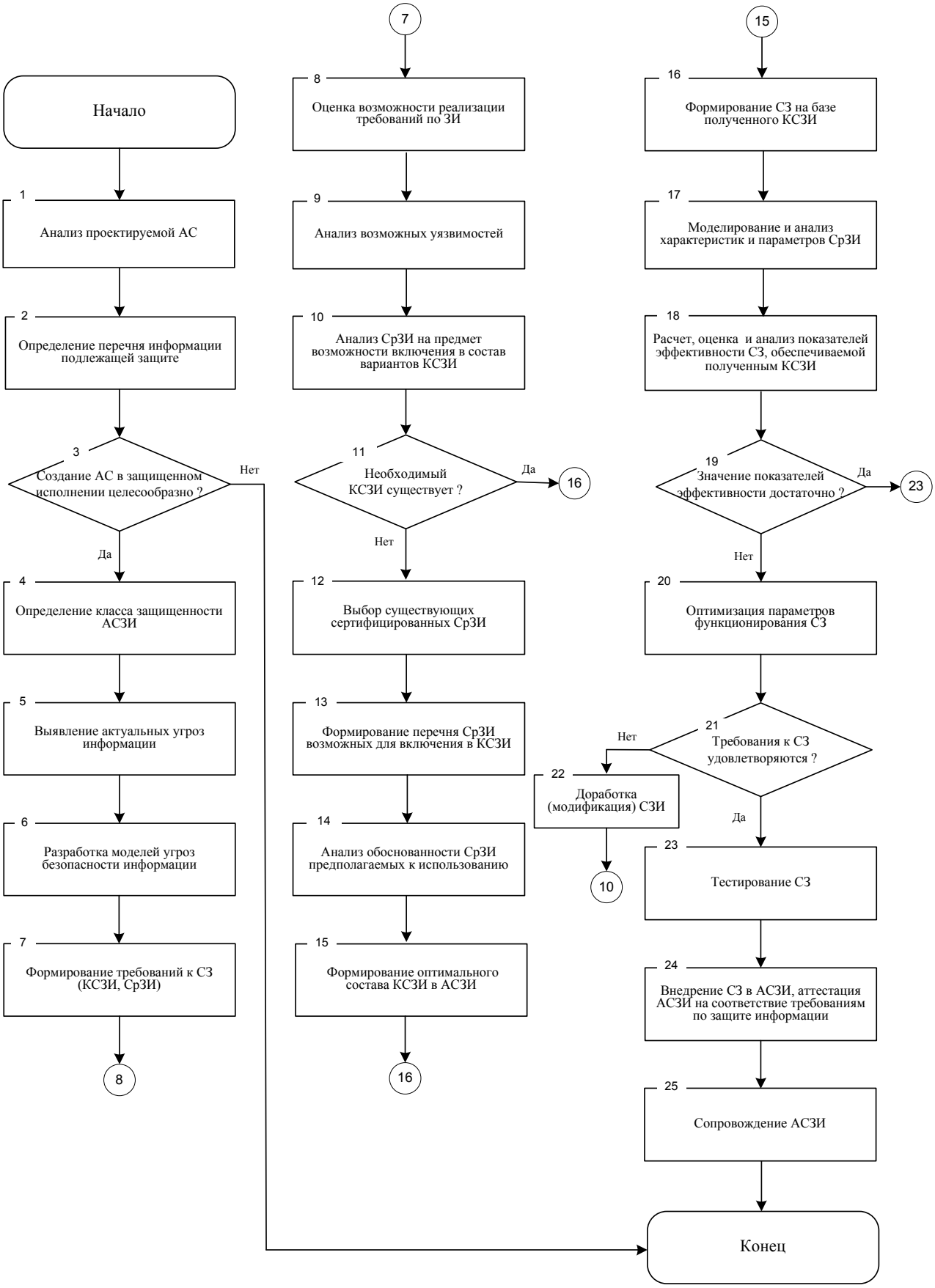

рис. 1 Алгоритм процесса проектирования систем защиты информации для защищенных автоматизированных систем

АС. Изучается оргштатная структура организации для определения круга лиц, участвующего в процессах обработки информации.

2. Определение перечня информации подлежащей защите. На данном этапе определяется информация, которая в соответствии с руководящими документами РФ по информационной безопасности, а также интересами организации подлежит защите.

3. В случае, если создание АС в защищенном исполнении нецелесообразно, проектирование системы защиты информации прекращается. Прежде всего это имеет место, когда затраты на создание СЗ больше чем стоимость самих информационных ресурсов. Если построение в защищенном исполнении целесообразно переходим на 4 этап.

4. Определение класса защищенности АСЗИ. Определяются основные характеристики АСЗИ для сопоставления с существующей классификацией, присваивается соответствующий класс в соответствии с руководящими документами ФСТЭК.

5. Выявление актуальных угроз информации. Целью данного этапа является выявление возможных каналов НСД и утечки защищаемой информации путем поиска недостатков и уязвимых мест системы. По результатам формируется перечень актуальных угроз информации и потенциальных мест установки СрЗИ в АСЗИ.

6. Разработка моделей угроз безопасности информации. На данном этапе осуществляется моделирование сценариев при реализации актуальных угроз и возможные последствия (нарушение конфиденциальности, целостности, доступности), определяется ценность информации, на которую они воздействуют. На основе нормативной документации, литературных источников, предшествующего опыта и специфических условий работы АСЗИ проводится формирование модели

потенциальных нарушителей, в основе которой лежит выбор содержательной модели поведения нарушителей, определение конкретного канала НСД в АСЗИ, потенциально возможного для использования нарушителями определенного класса.

7. Формирование требований к СЗ (КСЗИ, СрЗИ). На данном этапе проводится полный анализ исходных данных, выработка требований к СЗ в АСЗИ. Осуществляется формирование набора показателей ее качества, в их числе выделяют: технические, целевые, эффективности жизненного цикла, эффективности управления, экономические, и др. Устанавливаются их граничные значения, обеспечивающие минимально допустимый уровень безопасности информации. Требования к СЗ включаются в техническое задание.

8. Оценка возможности реализации требований по ЗИ. На данном этапе оценивается сама возможность реализации требований по ЗИ в проектируемой АСЗИ с точки зрения финансовых, трудовых, временных затрат. При необходимости разрабатываются альтернативные концепции построения СЗ и выбирается приемлемая.

9. Анализ возможных уязвимостей. В рамках проведения данного этапа проводится анализ возможных уязвимостей и актуальных угроз безопасности АСЗИ.

10. Анализ СрЗИ на предмет возможности включения в состав вариантов КСЗИ. На данном этапе анализируются сертифицированные средства защиты на предмет возможности включения в состав КСЗИ в соответствии с возможными уязвимостями и актуальными угрозами информации. Определяется совместимость средств защиты с функционирующей системой на программном и техническом уровнях, которые должны обеспечивать перекрытие существующих и предупреждение появления новых каналов НСД и утечки информации.

11. На данном этапе осуществляется выбор существующего сертифицированного КСЗИ, являющегося основой СЗ. В случае, если требуемый сертифицированный КСЗИ существует, переходим к 16 этапу. Если нет, то переходим к 12 этапу.

12. Выбор существующих сертифицированных СрЗИ. На данном этапе осуществляется выбор СрЗИ, возможных для включения в КСЗИ.

13. Формирование перечня СрЗИ, возможных для включения в КСЗИ.

14. Анализ обоснованности СрЗИ предполагаемых к использованию. Цель данного этапа – обоснование СрЗИ, предполагаемых для использования в КСЗИ с точки зрения материальных, трудовых, финансовых затрат и исключение из перечня средств, применение которых существенно затрудняет проектирование по указанным параметрам.

15. Формирование оптимального состава КСЗИ в АСЗИ. На данном этапе формируется оптимальная структура и состав КСЗИ на базе выбранных СрЗИ, окончательно формируется техническое задание.

16. Формирование СЗ на базе полученного КСЗИ. В ходе данного этапа осуществляется построение на базе полученного КСЗИ СЗ в целом - интеграция элементов ЗИ, СрЗИ в АСЗИ.

17. Моделирование и анализ характеристик и параметров СрЗИ. На данном этапе строится модель функционирования СЗ в АСЗИ, проводится анализ и построение модели взаимозависимостей СрЗИ с техническими и программными средствами, другими элементами структуры АСЗИ при выполнении функций защиты информации.

18. Расчет, оценка и анализ показателей эффективности СЗ. В ходе данного этапа производится расчет, оценка и анализ заданных показателей эффективности СЗ. Оценке подлежит каждый предлагаемый способ защиты, СрЗИ в соответствии с перекрываемыми ими каналами утечки и

угрозами, воздействующими на информацию, а также оценка КСЗИ в целом.

19. В случае, если показатели эффективности функционирования СЗ соответствуют требованиям заказчика и достаточны, переходим на 23 этап. Если показатели значение показателей эффективности не достаточны, переходим на 20 этап.

20. Оптимизация параметров функционирования СЗ. На данном этапе с целью повышения показателей эффективности СЗ производится наладка ее функционирования, изменение параметров и режимов работы СрЗИ, их взаимодействия, другие задачи оптимизации системы.

21. В случае, если требования заказчика к СЗ удовлетворяются, переходим на 23 этап. Если не удовлетворяются, то переходим на 22 этап.

22. Доработка (модификация) СЗ. Цель данного этапа – выявление ошибок, допущенных на предыдущих этапах проектирования СЗ, их устранение. Для чего производится изменение структуры и состава КСЗИ посредством замены отдельных СрЗИ, их дублирование, применением дополнительных мер защиты, доработкой других компонентов СЗ и их взаимодействием с самой АСЗИ. В целью выполнения данных мероприятий переходим на 10 этап.

23. Тестирование СЗ. На данном этапе проводится мероприятия по разработке программных СрЗИ, их настройке и тестированию СЗ в целом. Проверяется работоспособность, совместимость компонентов СЗ с другими программными и техническими средствами АСЗИ при выполнении задач защиты информации.

24. Внедрение СЗ и аттестация АСЗИ на соответствие требованиям по защите информации. На данном этапе производится установка и комплексная настройка всех средств СЗ. Проводятся предварительные испытания и опытная эксплуатация СЗ с целью проверки функционирования СЗ в составе АСЗИ, ее доработка и оптимизация в

соответствии с выявленными недостатками. Аттестация АСЗИ проводятся органами, имеющими лицензию на право проведения таких работ, и заключается в оценки соответствия ее СЗ требованиям руководящих документов по безопасности информации при выполнения задач согласно предназначения.

25. Сопровождение АСЗИ. В рамках данного этапа проводятся мероприятия по устранению недостатков СЗ, выявленных в ходе эксплуатации АСЗИ, влияющих на эффективность защиты информации.

Разработанное структурное моделирование процесса проектирования СЗ для АСЗИ позволяет научно обоснованно подходить к выбору оптимальной структуры КСЗИ в ходе построении методического обеспечения при формализации задачи создания оптимальной структуры СЗ, которые будут подробно исследованы в следующих работах авторов.

Список литературы

1. Проблемы защиты от информационного оружия в условиях глобальной информатизации общественных формаций. Специальная связь и безопасность информации (ССБИ-2012), сборник трудов международного симпозиума (Россия. Краснодар – Терскол, 20-30 апреля 2012 г.) / НЧОУ ВПО «Кубанский институт информзащиты. Краснодар: Экоинвест, 2012. – 296 с. С 286-294.

2. Новиков А.А. Уязвимость и информационная безопасность телекоммуникационных технологий: Учебное пособие для вузов / А.А. Новиков, Г.Н. Устинов - М.: Радио и связь, 2003. 296 с. № 6. С. 46-48

3. Доктрина информационной безопасности Российской Федерации.- Опубликованов печати 6 декабря 2016 года.

4. Positiv Research 2016. Сборник исследований по практической безопасности. https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf.

5. Бочков П.В. Методика решения задачи оптимизации размещения информационных ресурсов в локальной вычислительной сети / П.В. Бочков //Известия Орел ГТУ. 2005. № 7-8. С.30-37.

6. Гайкович В.Ю. Рынок средств защиты от НСД: текущее состояние и перспективы развития / В.Ю. Гайкович // Труды международной выставки-конференции "Безопасность информации". Москва, 1997. С. 33-35.

7. Дидюк Ю.Е. Методика выбора средств защиты информации в автоматизированных системах / Ю.Е. Дидюк // Радиотехника и системысвязи, 2003. Вып. 4.3. С. 45-47.

8. Малюк А.А. Введение в защиту информации в автоматизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожий — М.: Горячая линия - Телеком, 2004. 147 с.

9. Язов Ю.К. Технология проектирования систем защиты информации в информационно-телекоммуникационных системах / Ю.К. Язов - Воронеж: ВГТУ, 2004. 146 с.

References

1. Problems of protection from information weapons in conditions of global informatization of the social formations.Special communication and information security (SSBI-2012) proceedings of the international symposium (Russia. Krasnodar-Terskol, 20-30 april 2012) / NCHOU VPO Kuban Institute InfoSec. Krasnodar: Ekoinvest, 2012. 296 s. S. 286-294.

2. Novikov A.A. Vulnerability and information security of telecommunication technologies: textbook for universities / A.A. Novikov, G.N. Ustinov - M.: Radio and communication, 2003. 296 s. No. 6. S. 46-48.

3. Information security doctrine of the Russian Federation.- Published 6 December 2016.

4. Positiv Research 2016. Collection of studies on practical security. https://www.ptsecurity.com/upload/ptru/analytics/Positive-Research-2016-rus.pdf.

5. Bochkov P.V. Method of solving the problem of optimizing the placement of information resources within a local area network / Bochkov P.V. // proceedings of Orel GTU. 2005. No. 7-8. S. 30-37.

6. Gaikovich, V.Y. Market information security devices from protection illegal access: current state and development prospects / V.Y. Gaikovich // Proceedings of the international conference exhibition "information Security". Moscow, 1997. S. 33-35.

7. Didyuk Y.E. Method of selection of information security in automated systems / Y.E. Didyuk // Radio engineering and communication systems, 2003. Vol. 4.3. S. 45-47.

8. Malyuk A.A. Introduction to the protection of information in automated systems / A.A. Malyuk, S.V. Pazizin, N.S. Pogoji — M.: Hot line - Telecom, 2004. 147 s.

9. Yazov Y.K. Technology of designing information security systems in information and telecommunication systems / Y.K.Yazov - Voronezh: VSTU, 2004. 146 s.