О ПОДХОДАХ К РЕАЛИЗАЦИИ ЦЕНТРАЛИЗОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ АСУ ВОЕННОГО И СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Бородакий Юрий Владимирович, *академик РАН, доктор технических наук, профессор*
Добродеев Александр Юрьевич, *кандидат технических наук, старший научный сотрудник*
Нащекин Павел Александрович
Бутусов Игорь Викторович

В статье рассматриваются актуальные практические подходы к реализации централизованной системы управления информационной безопасностью современных автоматизированных систем управления военного и специального назначения. Предложены перспективные элементы и комплексы средств защиты информации и возможные направления развития систем комплексной защиты информации.

Ключевые слова: *информационная безопасность, система управления, комплексная защита, средства защиты информации.*

THE APPROACH TO IMPLEMENTING A CENTRALIZED SYSTEM FOR INFORMATION SECURITY MANAGEMENT AS MP

Yuri Borodakiy, *Member of the RAS, Doctor of Technical Sciences, Professor*
Alexander Dobrodeyev, *Ph.D., Associate Professor*
Pavel Nashchekin
Igor Butusov

The practical implementation of a centralized system for information security management of modern automated systems of military and special purpose is discussed. The promising elements and complexes of information security and possible directions of development of integrated systems of information protection are offered.

Keywords: *information security, management system, comprehensive protection, information security tools.*

Непрерывное совершенствование информационных технологий, повышение их роли и значимости, расширение сферы применения автоматизированных систем управления военного и специального назначения (АСУ ВиСН) в процессах управления государством и его Вооруженными Силами требуют постоянного внимания к вопросам обеспечения их информационной безопасности.

Обеспечение информационной безопасности АСУ ВиСН представляет собой комплексную проблему, которая решается в направлениях нормативного и правового регулирования применения АСУ ВиСН, совершенствования методов и средств их разработки, развития системы оценки соответствия требованиям информационной безопасности, обеспечения соответствующих организационно-технических условий безопасной эксплуатации, включая управление системой обеспечения безопасности обрабатываемой информации.

В России сложилась и определенным образом реализуется система обеспечения информационной безопасности АСУ ВиСН. Основы функционирования этой системы определяются Федеральными законами, Указами Президента Российской Федерации, руководящими и методическими документами федеральных органов исполнительной власти, относящимися к сфере

информационных технологий и информационной безопасности.

Вместе с тем, в настоящее время противоборствующими сторонами активно развивается широкий спектр новых методов и технологий информационного воздействия как на отдельные средства вычислительной техники (СВТ), так и на информационно-телекоммуникационные системы (ИТС) и АСУ органов государственного и военного управления, реализация которых направлена на получение несанкционированного доступа к информационным ресурсам и нарушение их функциональной устойчивости. Усилено ведется разработка новых информационных технологий для проведения информационных атак на АСУ ВиСН, постоянно совершенствуется уже существующие и появляются новые способы и средства проведения атак, а число компьютерных инцидентов ежегодно увеличивается.

При этом АСУ ВиСН рассматриваются в качестве одного из основных приоритетных объектов комплексного деструктивного воздействия, направленного на завоевание информационного превосходства и нарушение (затруднение) управления. В этих условиях проблема обеспечения информационной безопасности в различных условиях обстановки становиться одной из ключевых в решении задач построения АСУ ВиСН [1-6].

В соответствии с Доктриной информационной безопасности Российской Федерации угрозами безопасности АСУ ВиСН, как уже развернутых, так и создаваемых на территории России, могут являться:

уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи АСУ ВиСН;

несанкционированный доступ к информации (НСД), циркулирующей в АСУ ВиСН, а так же находящейся в банках и базах данных;

противоправные сбор и использование информации, циркулирующей в АСУ ВиСН;

нарушение технологии обработки информации;

утечка информации по техническим каналам;

воздействие на парольно-ключевые системы автоматизированных систем обработки и передачи информации;

внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи;

компрометация ключей и средств криптографической защиты информации, а также сервисов и инфраструктуры электронной подписи;

разработка и распространения вредоносных программ, нарушающих функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации, а также программ сбора информации об объектах информатизации;

уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

перехват информации в сетях передачи данных и на линиях связи, дешифрирование этой информации и навязывание ложной информации;

использование несертифицированных по требованиям безопасности информации отечественных и зарубежных информационных технологий, средств защиты информации и контроля доступа виртуализации, средств информатизации, телекоммуникации и связи и т.д.

Вместе с тем, развитие информационных и коммуникационных технологий вызвало возникновение ряда новых и развитие некоторых существующих угроз информационной безопасности, таких как [2, 3, 7-9]:

деструктивные информационно-технические воздействия (в том числе применение кибероружия, средств радиоэлектронной борьбы (РЭБ), проникновение в компьютерные сети) на информационно-технические объекты АСУ ВиСН;

компьютерные атаки на информационные сегменты АСУ ВиСН (информационно-коммуникационные, функциональные, информационно-психологические и др.);

преднамеренные действия, а также ошибки персонала и диверсионно-подрывная деятельность специальных служб иностранных государств;

электромагнитный терроризм;

внедрения в аппаратные и программные изделия АСУ ВиСН компонентов, реализующих функции, не предусмотренные документацией на эти изделия (НДВ);

использование базы данных скомпрометированных идентификаторов;

доступ к ресурсам неавторизованных пользователей по действующим аппаратным идентификаторам (смарт-карты, токены и т.п.);

подмена «облачной» инфраструктуры обработки информации;

активация служебных режимов функционирования изделия путем получения специальных команд (потоков) при штатной обработке информации;

обеспечение функционирования СВТ под управлением недоверенного гипервизора и т.д.

Основой построения перспективных современных АСУ ВиСН, соответствующим высоким

требованиям к их функциональным возможностям, надежности и функциональной устойчивости в условиях современного информационного противоборства является использование при их построении доверенной программно-аппаратной платформы (среды) [7, 9]. При этом реализация требований доверенности к аппаратной среде предполагает:

- применение основных и вспомогательных технических средств, прошедших специальную проверку и специальные исследования и получивших заключение о спецпроверке и предписание на эксплуатацию;

- обязательную сертификацию по требованиям безопасности информации к средствам вычислительной техники (СВТ) по требуемому классу защиты всех технических средств (составных частей) из состава изделия (системы специального назначения);

- использование аппаратных средств защиты информации (СрЗИ) российской разработки, прошедших сертификационные исследования программных средств на отсутствие недекларируемых возможностей и безопасность исходных кодов, а также подтверждение реально декларируемых возможностей;

- использование сертифицированных активных и пассивных технических средств защиты информации (генераторы шума, фильтры, экраны и т.д.).

Классический подход к созданию современных систем защиты информации (СЗИ) и обеспечению информационной безопасности изделий и объектов эксплуатации показан на рисунке 1.

Опыт разработок ОАО «Концерн «Системпром» АСУ в защищенном исполнении показывает, что основу защиты АСУ ВиСН от НСД должен составлять программно-аппаратный комплекс СЗИ от НСД, составляющими компонентами которого являются аппаратно-программный модуль доверенной загрузки (АПМДЗ) и программное изделие СЗИ от НСД, построенное из следующих функциональных модулей (технологий защиты): разграничения доступа; контроля и управления профилями; управления и регистрации печати; паролирования; антивирусной защиты; тестирования и экстренного уничтожения информации; системы мониторинга и управления событиями безопасности, усиления идентификации и аутентификации с использованием биометрических средств; комплексы «прозрачного» взаимодействия с разнокатегорированными информационными ресурсами.

Модульный подход к созданию систем защиты информации позволяет строить системы защиты требуемого Заказчику класса защищенности.

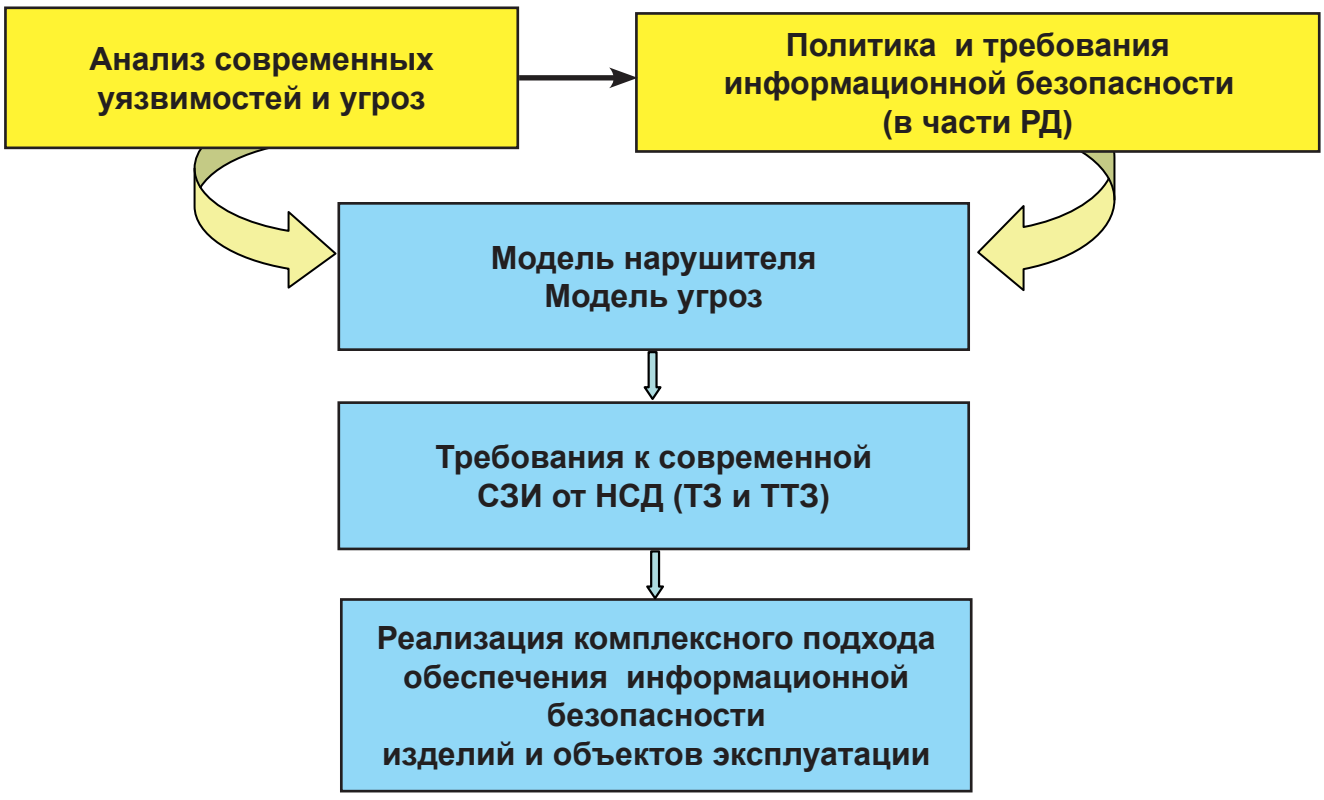

Рис.1. *Классический подход к созданию современных СЗИ и обеспечению информационной безопасности изделий и объектов эксплуатации*

Аналогичный модульный подход может применяться так же для построения системы комплексной защиты информации [10].

Важным критерием реализации ПАК СЗИ от НСД является обеспечение защищенной замкнутой программно-аппаратной среды с реализацией возможности централизованного и интерактивного контроля защищенности АСУ, а также управление всеми элементами СЗИ в АСУ и управления событиями безопасности, включая функциональный контроль.

Особую роль в обеспечении высоких классов защиты распределенных АСУ ВиСН играет разумная реализация системы (подсистемы) криптографической защиты информации. Ее состав и особенность построения и реализации (интеграции) - отдельный вопрос рассмотрения, следует упомянуть несколько слов об основных задачах, на решение которых направлена система (подсистема) криптографической защиты информации: идентификация и аутентификация пользователей; шифрование информации (трафика) в сети; шифрование информации на отчуждаемых и встраиваемых (внутренних) носителях; поддержка инфраструктуры электронной подписи; обеспечение ряда требований руководящих документов в части НСД (регистрация, управление печатью и т.д.).

Следует отметить, что основной особенностью современного этапа в создании защищенных систем является то, что мы находимся на этапе некоторой технической революции, когда на смену дорогой, громоздкой низкоскоростной аппаратуре ЗАС приходят современные высокоскоростные средства шифрования и средства криптографической защиты информации, такие как, IP и Ethernet - шифраторы, криптошлюзы и криптомаршрутизаторы на их основе, масштабируемые криптографические пулы с автоматизированной балансировкой нагрузки.

Разумное применение данных изделий позволяет строить защищенные системы со значительно большими функциональными возможностями и более высокими вероятностно-временными характеристиками. Стремительное развитие компьютерной техники, ее функциональных возможностей закономерно вызвало бурное развитие и разработку новых криптографических средств защиты информации для защиты от НСД самих автоматизированных рабочих мест (АПМДЗ, шифраторы носителей, подключаемых по интерфейсам USB и eSATA, функции однонаправленного ввода информации с отчуждаемых носителей, обеспечение доверенной виртуализации) и сетевого трафика внутри локальной сети и комплекса средств автоматизации (КСА).

Обязательным условием является применение только сертифицированных по требованиям безопасности информации средств и систем. При этом, основными компонентами СЗИ являются системы защиты информации телекоммуникационных сетей, системы защиты информации локальных вычислительных сетей и системы защиты информации АРМ и серверов (рис.2).

Особенностью современного этапа развития информационно-управляющих систем специального назначения (ИУС СН), к числу которых относится АСУ ВиСН, является всё более глубокая интеграция взаимодействующих систем и наполнение их новыми сервисами благодаря внедрению перспективных технологий.

При этом на первый план выходят следующие задачи:

- объединение информационных ресурсов взаимодействующих систем;
- обеспечение виртуализации вычислений с высоконадежной миграцией данных и виртуальных машин;
- реализация специального программного обеспечения (СПО) в виде сервисов и миграции СПО под различные операционные системы;
- создание общей доверенной среды обмена данными взаимодействующих ИУС СН;
- реализация иерархической системы взаимодействующих удостоверяющих центров взаимодействующих ИУС СН;
- переход на новую аппаратно-вычислительную базу;
- совершенствование технологий работы с электронной подписью в свете перехода на новую нормативную базу.

Соответственно в рамках взаимодействующих систем и изменения условий функционирования ИУС СН возникает необходимость реализации системы управления информационной безопасностью.

При этом в качестве перспективных решений целесообразно рассматривать:

- реализацию адаптивной централизованной системы управления информационной безопасностью ИУС СН с применением унаследованных и перспективных решений в области защиты информации;
- реализацию системы комплексной защиты информации на новых технических решениях;
- совершенствование нормативно-методической базы с учётом внедрения в ИУС СН новых технологий обработки информации и защиты.

Учитывая комплексность применения технических решений особую актуальность приобретает задача обеспечения централизованного управления системой комплексной защиты информации в

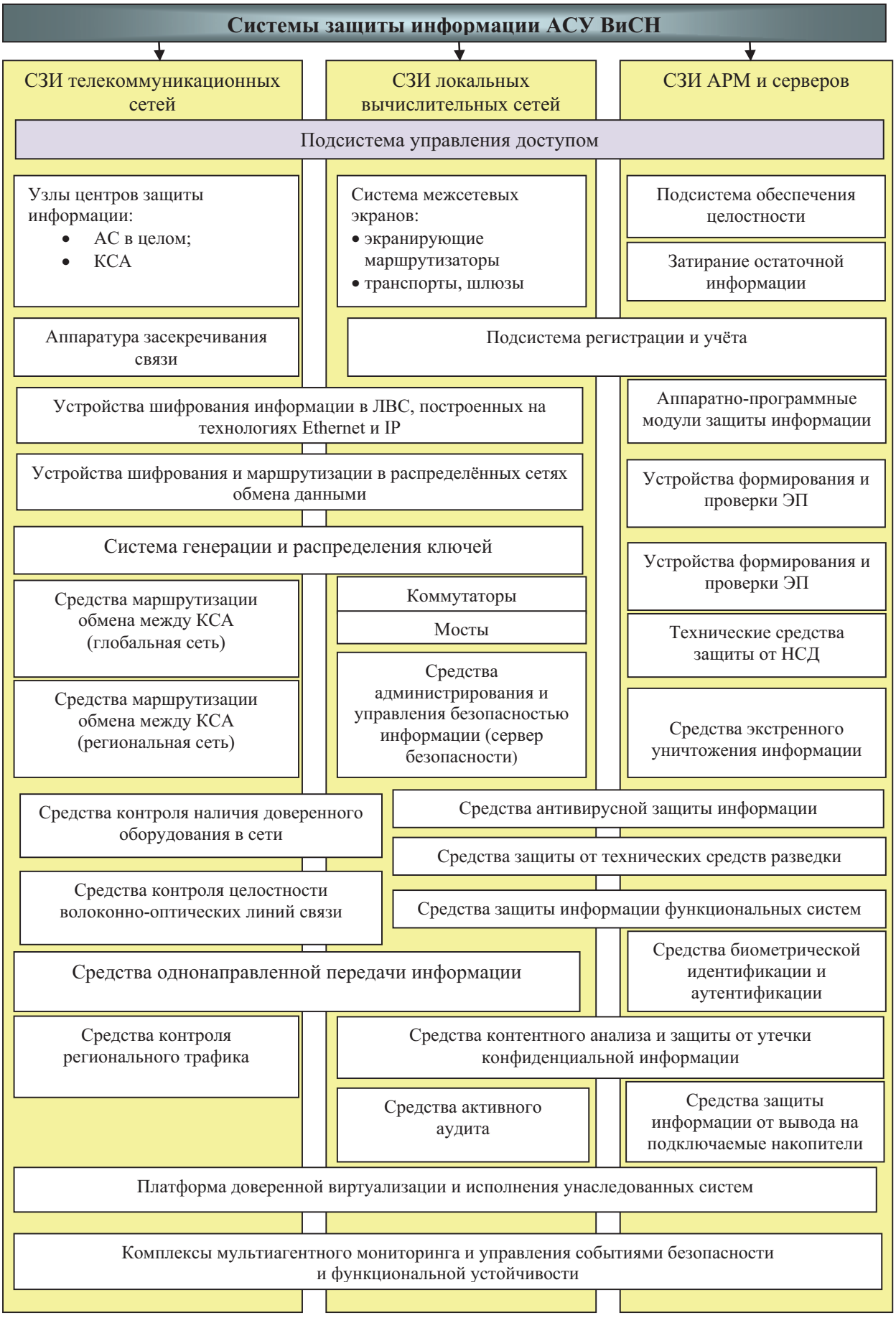

Рис. 2. *Основные компоненты систем защиты информации АСУ ВиСН*

рамках как одной ИУС СН, так и взаимодействующих (ресурсных) систем, с обеспечением следующих основных функций:

контроль защищенности и соответствия заданной топологии;

управление начальной настройкой программных средств СЗИ;

корректировка параметров идентификации и полномочий субъектов доступа к защищаемым ресурсам с учетом централизованной базы актуализации эталонных биометрических образов;

оповещение администратора безопасности информации о попытках НСД к защищаемым ресурсам с реализацией возможности не только локализации точек воздействия, но и с автоматизированным предоставлением сценария противодействия и фиксацией улик действий нарушителя;

управление блокировкой (разблокировкой) технических средств для локализации последствий НСД;

стирание информации в запоминающих устройствах;

создание (определение) защищенных областей магнитных носителей, каталогов, подкаталогов;

контроль за сохранностью (неизменностью, целостностью) информационного обеспечения, в том числе средств защиты, отображение результатов контроля;

архивирование и восстановление информации базы данных безопасности;

ведение журналов регистрации и учета информации на отчуждаемых носителях, ее архивации, просмотра и получение справок;

генерация паролей в соответствии с криптографическими и инженерно-криптографическими требованиями;

централизованное управление средствами антивирусной защиты, а так же изоляция (блокировка) АРМ должностных лиц, на которых выявлена вирусная активность.

Вместе с тем, в условиях взаимодействующих систем целесообразно отдельно выделить проблемы практической реализации централизованного управления средствами систем комплексной защиты информации в рамках нескольких взаимодействующих систем, в процессе которого должны быть реализованы следующие возможности:

реализация централизованной системы управления информационной безопасностью;

централизованное и сетевое управление криптографической подсистемой (настройка, распределение ключей, смена ключей);

централизованное управление подсистемой антивирусной защиты (обновление версий САВЗ и баз вирусных сигнатур, удалённый контроль);

автоматизированный контроль защищённости объектов ИУС СН;

автоматизированный контроль защищённости объектов взаимодействующих ИУС СН на основе мультиагентной системы;

интеграция с техническими средствами охраны и средствами контроля и управления доступом, а так же системами химической, биологической и радиационной безопасности и системой видеонаблюдения;

контроль защищённости от технических средств разведки;

организация однонаправленного ввода информации в ИУС СН;

обеспечение возможности работы должностных лиц в контурах с различной категорией обрабатываемой взаимодействующими системами информации;

обеспечение возможности интерактивного получения информации из разнокатегорированных систем;

автоматизированный прогноз защищенности совокупности взаимодействующих систем в условиях плановой эволюции.

Централизованная систем управления должна охватывать как унаследованные, хорошо себя зарекомендовавшие в условиях реальной эксплуатации, технические решения, так и перспективные, разрабатываемые в настоящее время элементы и комплексы средств защиты информации.

В качестве перспективных элементов и комплексов средств защиты информации целесообразно рассматривать:

- унифицированные аппаратно-программные модули доверенной загрузки с функциями управления по сети ИУС СН, обеспечения доверенной виртуализации и контроля отчуждаемых носителей информации;
- программно-аппаратные комплексы защиты информации от информационно-технического воздействия;
- комплексы защиты информации технологии «тонкий клиент» и средств виртуализации;
- высокопроизводительные криптографические средства защиты информации, включая криптографические пулы;
- программные комплексы централизованного управления средствами защиты информации взаимодействующих ИУС СН в рамках одной мультиплатформенной системы управления информационной безопасностью (СУИБ);
- средства защиты от НСД к вычислительным ресурсам центров обработки данных (ЦОД) на базе Blade-серверов и средства оперативной миграции виртуальных машин и серверов;

- автоматизированные средства построения ложных объектов;
- средства взаимодействия с несколькими удостоверяющими центрами;
- средства централизованной биометрической идентификации и аутентификации.

Современные тенденции развития ИУС СН требуют при создании АСУ ВиСН учитывать следующие перспективные направления развития систем комплексной защиты информации[4]:

разработку средств защиты информации распределённых вычислений и услуг ЦОД («облачные вычисления»);

реализацию криптографических сервисов для распределённых вычислений [5];

обеспечение централизованнго управления инфраструктурой электронной подписи с учетом построения доверенного пространства многоуровневой системы удостоверяющих центров;

реализацию технологии интеграции АС, основанной на интеграции сервисов с предоставлением возможностей виртуализации выносных, рабочих мест, серверных компонентов и электронного документооборота, включающего обработку потоков документов, заданий, индексацию и поиск информации (Интеграционный комплекс информационно сетевых сервисов (ИКИСС);

реализацию автоматизированных средств (сервисов) оценки эффективности защиты взаимодействующих ИУС СН;

защиту информации, обрабатываемой средствами виртуализации, в том числе с использованием виртуальных средств организации взаимодействия между сегментами АСУ (виртуальная сетевая инфраструктура, рабочие места и вычислительные комплексы);

централизованное управление персональными биометрическими данными для доступа к ресурсам АС, а так же на объекты охраны;

реализацию возможностей централизованного управления гетерогенными СЗИ взаимодействующих ИУС СН в рамках единой СУИБ;

построение системы компетенций СЗИ и системы взаимного доверия сервисов взаимодействующих ИУС СН;

криптографическую защиту информации при передаче по беспроводным каналам связи, включая мобильные устройства и оконечные исполнительные устройства;

внедрение перспективных средств идентификации абонентов и носителей ключевой информации и др.

Таким образом, только на основе реализации комплексного подхода в обеспечении информационной безопасности на основе перечисленных технологий и механизмов защиты может быть достигнут требуемый высокий уровень информационной безопасности, надежности и функциональной устойчивости АСУ ВиСН в условиях современного информационного противоборства.

Литература

1. Бородакий Ю.В., Боговик А.В., Карпов Е.А., Курносов В.И., Лободинский Ю.Г., Масановец В.В., Паращук И.Б. Основы теории управления в системах специального назначения. Учебник. М.: Изд. Управление делами Президента Российской Федерации, 2008. 306 с.
2. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1(1). С.2-9.
3. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) // Вопросы кибербезопасности. 2014. № 1 (2). С. 5-12.
4. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Предложения в межведомственную концепцию создания доверенной аппаратно-программной среды для автоматизированных систем органов управления // Вопросы радиоэлектроники. 2013. Т. 3. № 2. С. 15-22.
5. Бородакий Ю.В., Добродеев А.Ю., Свиридюк Ю.П., Нащёкин П.А. Основные задачи и проблемы

References

1. Borodakiy Yu.V., Bogovik A.V., Karpov Ye.A., Kurnosov V.I., Lobodinskiy Yu.G., Masanovets V.V., Parashchuk I.B. Osnovy teorii upravleniya v sistemakh spetsialnogo naznacheniya. Uchebnik, Moscow, Izd. Upravleniye delami Prezidenta Rossiyskoy Federatsii, 2008, 306 p.
2. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 1), Voprosy kiberbezopasnosti, 2013, No 1(1), pp.2-9.
3. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 2), Voprosy kiberbezopasnosti, 2014, No 1 (2), pp. 5-12.
4. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Predlozheniya v mezhvedomstvennuyu kontseptsiyu sozdaniya doverennoy apparatno-programmnoy sredy dlya avtomatizirovannykh sistem organov upravleniya, Voprosy radioelektroniki, 2013, Vol. 3, No 2, pp. 15-22.
5. Borodakiy Yu.V., Dobrodeyev A.Yu., Sviridyuk Yu.P., Nashchekin P.A. Osnovnyye zadachi i problemy

создания криптографической подсистемы защиты распределённых автоматизированных систем управления и связи специального назначения // Информационное противодействие угрозам терроризма. 2005. № 4. С. 176-178.

6. Бородакий Ю.В., Лободинский Ю.Г. Информационные технологии в военном деле (основы теории и практического применения). М.: Горячая линия - Телеком, 2008. 392 с.
7. Безкоровайный М.М., Татузов А.Л. Кибербезопасность - подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). С. 22-27.
8. Зубарев И.В., Жидков И.В., Кадушкин И.В. Кибербезопасность автоматизированных систем управления военного назначения // Вопросы кибербезопасности. 2013. № 1(1). С. 10-16.
9. Макаренко С.И., Чукляев И.И. Терминологический базис в области информационного противоборства // Вопросы кибербезопасности. 2014. № 1(2). С. 13-21.
10. Соснин Ю.В., Куликов Г.В., Непомнящих А.В., Нащёкин П.А. Базовые технологии моделирования процедур защиты информации от несанкционированного доступа // Вопросы защиты информации. 2014. № 1 (104). С. 23-28.

sozdaniya kriptograficheskoy podsistemy zashchity raspredelennykh avtomatizirovannykh sistem upravleniya i svyazi spetsialnogo naznacheniya, Informatsionnoye protivodeystviye ugrozam terrorizma, 2005, No 4, pp. 176-178.

6. Borodakiy Yu.V., Lobodinskiy Yu.G. Informatsionnyye tekhnologii v voyennom dele (osnovy teorii i prakticheskogo primeneniya). M.: Goryachaya liniya - Telekom, 2008. 392 p.
7. Bezkorovaynyy M.M., Tatuzov A.L. Kiberbezopasnost - podkhody k opredeleniyu ponyatiya, Voprosy kiberbezopasnosti, 2014, No 1(2), pp. 22-27.
8. Zubarev I.V., Zhidkov I.V., Kadushkin I.V. Kiberbezopasnost avtomatizirovannykh sistem upravleniya voyennogo naznacheniya, Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 10-16.
9. Makarenko S.I., Chuklyayev I.I. Terminologicheskiy bazis v oblasti informatsionnogo protivoborstva, Voprosy kiberbezopasnosti, 2014, No 1(2), pp. 13-21.
10. Sosnin Yu.V., Kulikov G.V., Nepomnyashchikh A.V., Nashchekin P.A. Bazovyye tekhnologii modelirovaniya protsedur zashchity informatsii ot nesanktsionirovannogo dostupa, Voprosy zashchity informatsii, 2014, No 1 (104), pp. 23-28.