КИБЕРБЕЗОПАСНОСТЬ КАК ОСНОВНОЙ ФАКТОР НАЦИОНАЛЬНОЙ И МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ XXI ВЕКА (Часть 2*)

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

В статье рассматриваются актуальные проблемы обеспечения международной и национальной кибербезопасности и предлагаются подходы к созданию адекватной современным угрозам системы обеспечения кибербезопасности автоматизированных систем органов военного и государственного управления

***Ключевые слова**: кибербезопасность, информационная безопасность, инфосфера, киберпространство, информационное противоборство*

CYBERSECURITY AS A MAJOR FACTOR OF NATIONAL AND INTERNATIONAL SECURITY IN THE XXI CENTURY (Part 2)

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

The actual problems of international and national cybersecurity are considered. The approaches to the development of the cybersecurity system relevant to modern threats to the military and government automated systems are given.

***Keywords**: cybersecurity, cyber security, information security, infosphere, cyberspace, information warfare*

1. СОВРЕМЕННЫЕ ТЕНДЕНЦИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОРГАНОВ ВОЕННОГО И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

В современных условиях, в целях эффективного отражения угроз кибербезопасности и обеспечения возможности проведения симметричного ответа на вызовы или нанесения упреждающего удара, автоматизированные системы органов военного и государственного управления (АСУ ОВГУ), должны совершенствоваться в направлении повышения степени их автоматизации и компьютеризации, то есть создания и развития АСУ в защищенном исполнении. Насущным требованием времени становится пересмотр принципов построения АСУ ОВГУ с позиций обеспечения кибербезопасности как в мирное, так и в военное время.

По мнению специалистов вооружённых сил США в области кибербезопасности, в техническом плане полная адекватная киберзащита предусматривает построение и использование следующих основных подсистем: подсистемы защиты (Protection Capabilities), обеспечивающей скрытность излучений радиоэлектронных средств, систем и средств связи, компьютерную безопасность (Computer Security) и информационную безопасность (InfoSec); подсистемы обнаружения (Detection Capabilities), обеспечивающей распознавания аномалий в сети за счет применения систем их обнаружения; подсистемы реагирования на изменения технических параметров и обстановки (Reaction Capabilities), обеспечивающей восстановление (в том числе реконфигурацию) и выполнение других процессов информационных операций [2].

По мнению авторов, система киберзащиты, созданная в соответствии с вышеуказанными требованиями, не обеспечивает полной кибербезопасности объекта информатизации, и, в первую очередь, АСУ ОВГУ. Обеспечение кибербезопасности АСУ ОВГУ должно осуществляется единой интеллектуальной системой кибербезопасности, являющейся частью системы информационной безопасности. При этом в основу построения перспективной системы кибербезопасности должно быть положено понятие ***эволюции*** системы, т.е. способность её адаптации через изменение параметров под воздействием

* Первая часть опубликована в №1 за 2013 г.

внешних и внутренних киберугроз (кибератак) и применяемых технологий противодействия им на протяжении своего жизненного цикла [3-11].

Эволюционирующая интеллектуальная система кибербезопасности АСУ ОВГУ должна обеспечить не только обнаружение новых и неизвестных киберугроз и кибератак в ходе мониторинга (разведки) киберпространства, но и анализ выявленных киберугроз (кибератак) и автоматический выбор параметров функционирования АСУ в условиях деструктивных воздействий без ухудшения ее основных характеристик.

В системе кибербезопасности АСУ ОВГУ также должны быть реализованы возможности: автоматического изменения свойств и параметров систем и средств обеспечения кибербезопасности в зависимости от изменения состояния киберпространства (выявления активности потенциальных источников киберугроз, обнаружения кибератак) и результатов проведенных кибератак; автоматической оценки изменения уровня защищенности АСУ от киберугроз при изменении условий функционирования; автоматизированной поддержки принятия решений о противодействии кибератакам и автоматическое воздействие на источники кибератак; автоматизированной поддержки принятия решения о перераспределении ресурсов систем и средств кибербезопасности в случае их функционального поражения в результате кибератак; учета в процессе обеспечения кибербезопасности всех взаимосвязанных, взаимодействующих и изменяющихся во времени факторов, влияющих на уровень кибербезопасности АСУ; снижения нецелевой нагрузки на комплекс средств автоматизации системы кибербезопасности АСУ; прогнозирования, на основе заложенных и накопленных в процессе эксплуатации знаний, факторов, влияющих на уровень защищенности АСУ от всех видов киберугроз.

Определяя задачи борьбы с угрозами кибербезопасности, нельзя отбрасывать разработку и реализацию активных способов и методов обеспечения кибербезопасности. Поэтому в системе кибербезопасности АСУ должны быть предусмотрены возможности проведения упреждающих аппаратно-программных воздействий (упреждающих ударов) и активных атак на выявленные источники кибератак, информационные системы и ресурсы противоборствующей стороны, а так же способность к дезинформации противоборствующей стороны об истинных свойствах и параметрах АСУ и ее системы кибербезопасности.

Важнейшим условием создания системы обеспечения кибербезопасности АСУ ОВГУ является применение аппаратной и программной платформ из состава доверенной программно-аппаратной среды [11]. Доверенность – это строгое, гарантированное соответствие необходимым требованиям в части информационной безопасности, надежности и функциональной устойчивости в условиях современного информационного противоборства при соблюдении определенных условий технологической независимости. Под доверенной программно-аппаратной средой следует понимать совокупность технических и программных средств, организационных мер, обеспечивающих создание, применение и развитие систем специального назначения в защищенном исполнении, отвечающих необходимым требованиям информационной безопасности, надежности и функциональной устойчивости, подтвержденных сертификатами соответствия (заключениями) в соответствующих обязательных системах сертификации Российской Федерации (рис.1). Главный критерий «доверенности» - это соответствие требованиям информационной безопасности в современных условиях информационного противоборства. Доверенность аппаратно-программной среды фактически определяется доверенностью используемых аппаратных (программно-аппаратных) средств и программного обеспечения.

Большой опыт ОАО «Концерн «Системпром» по разработке и сертификации по требованиям безопасности информации (ТБИ) систем и комплексов специального назначения в защищенном исполнении и СЗИ позволяет предложить следующий под-

Рис.1. *Реализация основ обеспечения доверенной программно-аппаратной среды*

ход к оценке доверенности используемого программного обеспечения (ПО) и программно-аппаратных средств в соответствии с определенными критериями, в основу которого закладываются неразрывность понятия «доверенность» с гарантиями и уровнями обеспечения информационной безопасности, т.е. главным критерием доверенности должна выступать информационная безопасность.

При этом, доверенность ПО имеет несколько уровней оценки: статус разработчика; доступность исходных кодов; наличие сертификата соответствия (заключения); возможности разработки, тиражирования и поставки ПО, его технической поддержке (см. таблицу 1).

Создание эффективной системы кибербезопасности АСУ ОВГУ предусматривает полнодостаточную реализацию комплексного подхода в обеспечении информационной безопасности изделий и объектов АСУ, заключающегося в рациональном сочетании следующих составляющих: защита от утечки по техническим каналам и противодействие техническим средствам разведки; применение аппаратно-программных средств защиты информации для создания системы защиты информации от НСД; разработки и реализация комплекса организационно-технических мер (рис.2).

Система кибербезопасности АСУ ОВГУ, по мнению авторов, должна включать в себя взаимосвязанные между собой следующие основные функциональные системы: мониторинга (разведки) киберпространства, комплексной защиты информации, оперативного оповещения о кибератаках (угрозах) и активного противодействия им, в свою очередь состоящих из определенных функциональных подсистем.

Предлагаемая структурная схема системы кибербезопасности АСУ ОВГУ представлена на рисунке 3.

Функционирование всех вышеперечисленных систем и подсистем должно быть регламентировано соответствующими нормативными правовыми актами и руководящими документами.

***Таблица 1.**- Уровни доверенности программного обеспечения*

Уровни доверенности ПО	**Критерии оценки доверенности ПО**				
	Разработчик ПО	**Предоставление исходных кодов**	**Наличие сертификата соответствия (заключения) на ПО по ТБИ**	**Наличие аттестованного производства ПО**	**Тиражирование и поставка продукции ПО**
1 уровень доверенности	Российская компания, обладающая всеми необходимыми лицензионными возможностями	Исходные коды ПО в наличии и предъявляются для проверок соответствия ТБИ	В наличии сертификат соответствия (заключение) на ПО по ТБИ (в части отсутствия НДВ) при строгом соответствии РДВ	Аттестованное в рамках сертификации по ТБИ производство	Осуществляется тиражирование и поставка ПО и обеспечивается техподдержка на всех этапах жизненного цикла
2 уровень доверенности	Зарубежная компания, положительно зарекомендовавшая себя на международном рынке	Исходные коды ПО открыты и свободно предъявляются (предоставляются) в части проверок соответствия ТБИ, либо их наличие в сети Интернет	В наличии сертификата соответствия (заключения) на ПО по ТБИ в части отсутствия НДВ при строгом соответствии РДВ, при обязательном условии, что Заявителем на сертификацию является российская компания, обладающая соответствующими лицензиями ФСБ России и лицензиями на разработку и производство ПО	Аттестованное в рамках сертификации по ТБИ производств	Осуществляется тиражирование и поставка ПО и обеспечивается техподдержка на всех этапах жизненного цикла Тиражирование и поставка продукции ПО обеспечивается Заявителем на сертификацию по ТБИ
3 уровень доверенности	Зарубежная компания, положительно зарекомендовавшая себя на международном рынке	Исходные коды ПО предъявляются (предоставляются) по согласованию с Заявителем на сертификацию	Соответствует 2-му уровню доверенности	Соответствует 2-му уровню доверенности	Соответствует 2-му уровню доверенности
4 уровень доверенности	Зарубежная компания	Исходные коды ПО недоступны для проверок на соответствие ТБИ	Соответствует 3-му уровню доверенности	Соответствует 3-му уровню доверенности	Соответствует 3-му уровню доверенности

Далее рассмотрим более подробно основные функциональные системы и подсистемы, их предназначение и возможны й состав.

Система мониторинга (разведки) киберпространства должна представлять собой совокупность специализированных аппаратно-программных средств, предназначенных для оценки обстановки в киберпространстве, систематического сбора и обработки информации о возможных угрозах кибербезопасности АСУ ОВГУ (источники, характер, содержание, масштаб, время и т.п.), прогнозирования возможных вариантов и технологий реализации кибератак и потенциально опасных объектов, способных осуществлять кибератаки, выявления признаков и фактов кибератак на информационные объекты и выдачи информации о возможном воздействии кибератак на информационную инфраструктуру. Ведение разведки в киберпространстве требует цифрового проникновения в сети и компьютеры потенциального противника и предусматривает использование совершенно новых источников, форм и способов сбора данных и информации, разработки новых разведывательных средств и технологий, тактических и технических приемов. На систему мониторинга и разведки киберпространства должна возлагаться функция обеспечения формирования и ведения базы данных по вскрытым (обнаруженным) различным видам и источникам киберугроз (кибератак), что предусматривает создание и ведение каталога потенциальных угроз кибербезопасности и признаков кибервоздействий на информационные ресурсы АСУ ОВГУ, определение номенклатуры потенциальных угроз кибербезопасности, создание и ведение банка критериев обнаружения кибератак на информационные системы.

Комплексная система защиты информации должна включать в свой состав современные системы защиты информации (СЗИ) и средств контроля их эффективности. В состав системы должны входить:

- система предупреждения и обнаружения компьютерных атак (СПОКА);
- подсистема программно-аппаратных средств защиты от НСД;
- подсистема криптографической защиты информации и шифрования;
- подсистема контроля состояния и функциональной устойчивости.

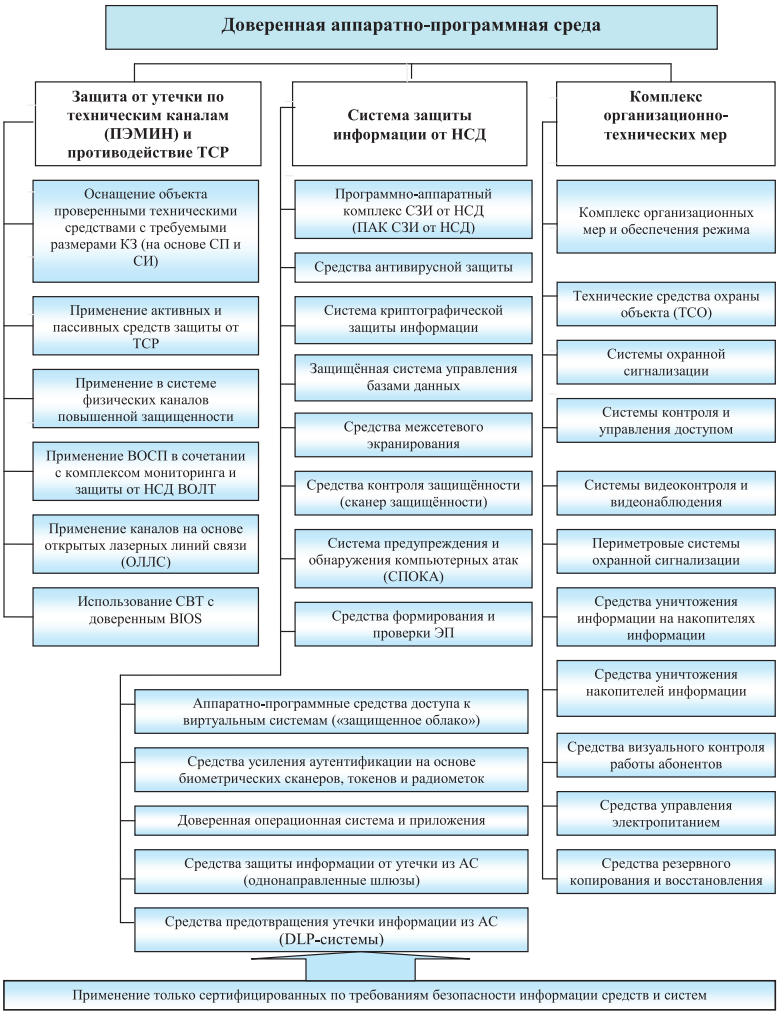

Рис.2. *Реализация комплексного подхода в обеспечении информационной безопасности АСУ ОВГУ*

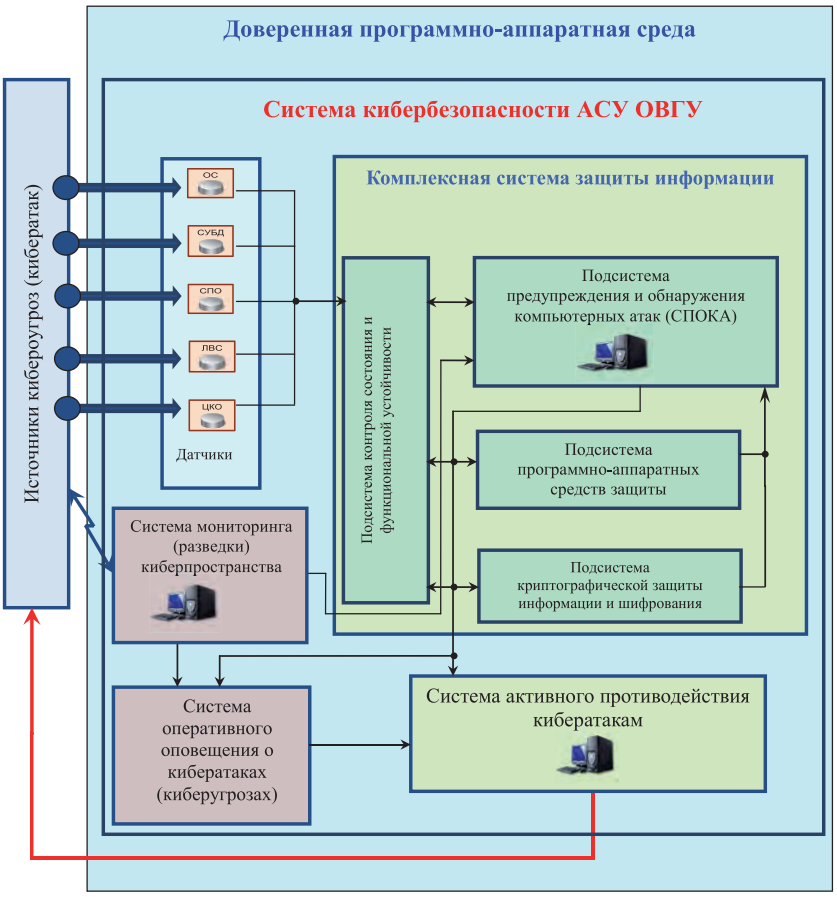

Рис.3. *Структурная схема системы кибербезопасности АСУ ОВГУ*

СПОКА представляет собой совокупность взаимосвязанных программно-аппаратных средств, предназначенных для: прогнозирования сценариев и классификации компьютерных атак; идентификации признаков вторжения и обнаружения компьютерных атак; анализа уязвимостей и технологических циклов управления; контроля технических и программных средств компьютера, информационной системы или сети с целью предупреждения о возможном вторжении; применения методов противодействия компьютерным атакам; оценки и обеспечения функциональной устойчивости функционирования АСУ в условиях кибератак.

Подсистема программно-аппаратных средств защиты от НСД должна включать в свой состав, помимо традиционно применяемых систем и средств защиты (идентификации и аутентификации пользователей, средства разграничения доступа, антивирусной защиты, защищенные системы управления базами данных, средства межсетевого экранирования), также средства формирования и проверки электронной подписи; аппаратно-программные средства доступа к виртуальным системам («защищенное облако»); средства усиления аутентификации на основе биометрических сканеров, токенов и радиометок; средства защиты информации от утечки (однонаправленные шлюзы) и средства предотвращения утечки информации из АС (DLP-системы); средства контроля защищенности (сканер защищенности); программно-аппаратные средства защиты информации технологии «тонкий клиент»; средства защиты от спама и др.

Необходимо также безусловное применение технических средств охраны СВТ, обрабатывающих критически важную информацию и комплексов средств защиты от ИТР и РЭБ.

Подсистема криптографической защиты информации и шифрования представляет собой совокупность аппаратных, программных и аппаратно-программных средства, систем и комплексов, предназначенных для защиты информации, циркулирующей в технических средствах, при ее обработке, хранении и передаче по каналам связи, включая шифровальную технику и обеспечивающих криптографическое преобразование информации и управление процессом распределения ключей. Средства криптографии и шифрования должны защищать не только информации внутри сети и каналах связи, ни и внутренние информационные ресурсы технических средств (внутренние и внешние носители информации) и являются самым сильным рубежом защиты в системе обеспечения кибербезопасности.

Подсистема контроля состояния и функциональной устойчивости предназначена для обеспечения непрерывного контроля состояния и функциональной устойчивости АСУ, ее системы защиты с выдачей информации и рекомендаций в систему управления кибербезопасностью с принятием адекватных мер по корректировке работы СЗИ для борьбы с текущими кибератакам и осуществление их своевременной плановой (внеплановой) смены. Подсистема должна включать в себя: средства мониторинга и сбора информации о состоянии функциональной устойчивости и параметрах АСУ ОВГУ и ее СЗИ от НСД; средства анализа и оценки количественных показателей уровня защищенности АСУ и ее СЗИ от НСД; средства подготовки и принятия решений для формирования сигналов управления средств регулирования параметров СЗИ АСУ (подсистему адаптации); средства централизованного перехода к новым настройкам СЗИ и т.п.

Система активного противодействия кибератакам должна включать в себя средства выбора оптимальной стратегии противодействия, средства активного воздействия на процесс совершения атаки, средства планирования и ведения упреждающих атакующих действий, а также средства активного поражения критически важных информационных объектов противоборствующей стороны.

Система оперативного оповещения о кибератаках (киберугрозах) должна представлять собой совокупность взаимосвязанных программно-аппаратных и телекоммуникационных средств, предназначенных для организации своевременного доведения информации в режиме реального времени до соответствующих субъектов управления о возможных (выявленных) кибератаках (угрозах), их сущности и параметрах, попытках НСД к информации и принятых (необходимых) мерах защиты и противодействия.

2. ОСНОВНЫЕ НАУЧНО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ АСУ ОВГУ И ВОЗМОЖНЫЕ ПУТИ ИХ РЕШЕНИЯ

В современных реалиях система национальной безопасности России пока еще во многом не готова как к созданию и обеспечению эффективного и защищенного киберпространства для нужд государства, так и к эффективному противодействию постоянно возрастающим угрозам в киберпространстве, которые реальны для всех, без исключения, элементов военной и государственной организации страны.

Одной из основных проблем является отсутствие глубокой научной проработки вопросов обеспечения кибербезопасности. Огромное количество руководящих, нормативно-методических и прочих документов в области защиты информации разработаны в прошлом веке и не учитывают возможные современные каналы утечки информации. Критическая ситуация сложилась в области телекоммуникационных систем для нужд государственного управления и передачи информации ограниченного доступа, построенных с использованием современного импортного оборудования. Современные АСУ ОВГУ, как правило, построены на базе ПЭВМ импортного производства или на базе комплектующих импортного производства, что также создает предпосылки к утечке информации и успешной реализации кибератак на них.

Важной особенностью является технологическая отсталость российских компаний ИТ-индустрии от ведущих зарубежных вендоров, что неизбежно ведет к опасности масштабных сбоев аппаратных и программных средств. Количества сертифицированных в системе сертификации Минобороны и ФСБ России средств защиты информации явно недостаточно. И это далеко не полный перечень проблемных вопросов.

Мировой опыт обеспечения кибербезопасности говорит о необходимости создания целостной системы, сочетающей организационные, оперативные и технические меры защиты с использованием современных методов прогнозирования, анализа и моделирования ситуаций. При этом важнейшей составной частью этой системы должна являться задача обеспечения кибербезопасность АСУ ОВГУ. Критичность обеспечения киберзащиты подобных АСУ обусловлена тем, что ущерб от реализации угроз кибербезопасности может привести к нарушению управления государством и его Вооруженными Силами, а следовательно – к снижению национальной безопасности государства.

По мнению авторского коллектива, основными направлениями развития и совершенствования системы кибербезопасности АСУ ОВГУ могут являться:

- формирование на государственном уровне единой научно-технической политики в области кибербезопасности, развитие и совершенствование нормативно-правовой базы и формирование единого понятийного аппарата в области кибербезопасности, законодательный перевод кибероружия и суперкомпьютеров в статус образцов вооружения;

- создание единых реестров программных и аппаратных средств, перспективных АСУ ОВГУ (взаимодействующих АСУ, систем и средств связи), рекомендуемых к разработке или внедрению и выработка требований к ним, создание баз данных, касающихся надежности функционирования АСУ, состояния их защищенности, состояния техниче-

ского оборудования, оценки эффективности действующих и внедряемых мер безопасности, создание хранилища эталонного программного обеспечения, используемого в АСУ ОВГУ;

- создание и функционирование системы постоянного мониторинга киберпространства; организация работы по реализации комплекса мер, направленных на своевременное обнаружение, предупреждение, отражение и нейтрализацию угроз кибербезопасности АСУ ОВГУ, разработка методов и средств своевременного выявления угроз и оценки их опасности для АСУ, прогнозирования возможных крупномасштабных киберконфликтов;

- развитие исследований в области математического моделирования процессов обеспечения кибербезопасности АСУ ОВГУ, направленных на разработку вероятных сценариев развития ситуации и поддержку управленческих решений;

- разработка и реализация комплексной целевой программы, определяющей основные направления и мероприятия по построению систем кибербезопасности АСУ ОВГУ с учетом вновь возникающих угроз (информационное оружие [13,14], кибертерроризм, инсайдеры, электромагнитный терроризм), разработку научно-методических основ создания программно-аппаратных средств выявления кибератак, оценки и обеспечения реального уровня защищенности критически важных информационных систем и устойчивости функционирования в условиях активных кибератак с учетом особенностей их функционирования;

- разработка комплекса мер по созданию и внедрению телекоммуникационного оборудования, устойчивого к кибератакам;

- разработка и внедрение импортозамещающих технологий, материалов, комплектующих и других видов продукции, используемых в АСУ ОВГУ и системах кибербезопасности;

- создание отечественных базовых информационных технологий, включающих в себя необходимый и достаточный для функционирования единого информационного пространства комплекс программных средств;

- разработка и создание средств противодействия информационному оружию, развитие и совершенствование программно-технических методов предотвращения утечек, разрушения, уничтожения, искажения и перехвата информации (в том числе и исключения НСД к ней) и криптографических средств ее защиты при передаче по каналам связи, а также интенсификация разработок собственных систем и средств для проведения адекватных мер при применении противоборствующей стороной информационного оружия;

- использование технологии нейронных сетей при построении систем кибербезопасности АСУ ОВГУ, обладающих способностью к обучению на примерах и обобщению данных, адаптироваться к изменению свойств объекта управления и внешней среды, высокой устойчивостью к повреждениям своих элементов в силу изначально заложенного в нейросетевую архитектуру параллелизма;

- формирование специальных испытательных баз (полигонов) для проведения испытаний (проверок) по оценке функциональной устойчивости АСУ ОВГУ и систем кибербезопасности в реальных изменяющихся условиях функционирования с использованием реальных кибератак и сведений по инцидентам, возникающих (появившихся) на объектах АСУ и оценки эффективности систем кибербезопасности;

- разработка современных СЗИ на основе использования технологий и механизмов СПОКА, в том числе отвлечения удара, создания ложных целей, разработка комплексов (механизмов) активного противодействия кибератакам, а также средств подавления источников кибератак и обеспечения ответного противодействия;

- разработку для АСУ ОВГУ специализированных экономически целесообразных информационных технологий, исключающих или в максимальной степени снижающих на технологическом уровне обмен информацией, подлежащей обязательной защите;

- проведение комплекса мероприятий по развитию систем, средств и методов мониторинга и технической оценки уровня реальной защищенности АСУ ОВГУ в условиях кибератак, создание баз данных, содержащих сведения об устойчивости функционирования, состоянии защищенности, оценки эффективности действующих и внедряемых мер кибербезопасности;

- проведение исследований технологий, способов и методов проведения кибератак на информационно-коммуникационные сети и компьютерные системы, особое внимание обратив на выявление и противодействие внедряемым боевым программным агентам [15], и противодействия им;

- разработка основных положений, определяющих возможность, характер и порядок применения средств кибервоздействий в мирное и военное время, особенно в глобальных сетях иностранных государств и увязку их с нормами международного права;

- создание единого государственного ситуационного центра системы мониторинга, контроля и защиты киберпространства информационно-телекоммуникационной инфраструктуры и межведомственных

ситуационных специализированных центров противодействия кибертерроризму и кибератакам;

- совершенствование системы подготовки и переподготовки кадров в области кибербезопасности на базе профильных образовательных учреждений.

Кибербезопасность в настоящее время приобретает значение новой отрасли в нашем военно-промышленном комплексе, предназначенной в конечной цели обеспечить национальную безопасность нашей страны, и отношение к ее формированию должно носить и иметь не ведомственный, а государственный характер. Своевременное планирование и реализация мероприятий обеспечения кибербезопасности и информационного противоборства на глобальном и региональном уровнях становится одним из приоритетных направлений обеспечения национальной безопасности Российской Федерации и должно оказать существенное влияние на ее укрепление.

Литература

1. 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.
2. Паршин С.А., Горбачев Ю.Е., Кожанов Ю.А. Кибервойны - реальная угроза национальной безопасности. М.: Изд-во КРАСАНД, 2011. 96 с.
3. Бородакий Ю.В., Лободинский Ю.Г. Информационные технологии в военном деле (основы теории и практического применения) М.: Горячая линия – Телеком, 2008. 394 с.
4. 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. М.: Изд. Управление делами Президента Российской Федерации, 2008. 400 с.
5. Бородакий Ю.В., Лободинский Ю.Г. Эволюция информационных систем - М.: Горячая линия – Телеком, 2011. 368 с.
6. Научно-технический сборник ФГУП «Концерн «Системпром» / Под общей ред. Ю.В.Бородакия - М.: ФГУП «Концерн «Системпром», 2011. № 1 (1).
7. Научно-технический сборник ФГУП «Концерн «Системпром» / Под общей ред. Ю.В.Бородакия - М.: ФГУП «Концерн «Системпром», 2012. № 1 (2).
8. Научно-технический сборник ФГУП «Концерн «Системпром» / Под общей ред. Ю.В.Бородакия - М.: ФГУП «Концерн «Системпром», 2013. № 1-2 (3).
9. Бородакий Ю.В., Миронов А.Г., Добродеев А.Ю., Болдина М.Н. Проблемы и перспективы создания эволюционирующих интеллектуальных систем защиты информации для современных распределенных информационно-управляющих систем и комплексов специального и общего назначения // Научные проблемы национальной безопасности Российской Федерации. 2012. Вып. 5. С. 328.
10. Бородакий Ю.В., Миронов А.Г., Добродеев А.Ю., Болдина М.Н., Бутусов И.В. Перспективные системы защиты информации должны быть интеллектуальными // Защита информации. INSIDE. 2013. № 2. С. 48-51.
11. Бородакий Ю.В., Добродеев А.Ю., Иванова А.И., Куликов Г.В. Перспективная архитектура интеллектуальной системы обеспечения информационной безопасности распределенной автоматизированной системы // Приложение к журналу «Открытое образование». 2006. С. 141-142.
12. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Доверенная среда-основа гарантированной безопасности // «Information Security/Информационная безопасность». 2013. №2. С. 36-37.
13. Расторгуев С.П. Информационная война. Проблемы и модели (Экзистенциальная математика в информационной войне). М.: Гелиос АРВ, 2006. 240 с.
14. Расторгуев С.П. Информационная война. М: Радио и связь, 1999. 416 с.
15. Медин А., Маринин А. Особенности применения киберсредств в межгосударственных военных и во внутренних конфликтах // Зарубежное военное обозрение. 2013. № 3. С. 11-16.

Referens

1. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Kiberbezopasnost kak osnovnoy faktor natsionalnoy i mezhdunarodnoy bezopasnosti KhKhI veka (Chast 1), Voprosy kiberbezopasnosti (Cybersecurity Issues), 2013, No 1(1), pp. 2-9.
2. Parshin S.A., Gorbachev Yu.E., Kozhanov Yu.A. Kibervoyny - realnaya ugroza natsionalnoy bezopasnosti, Moscow, Izd-vo KRASAND, 2011, 96 p.
3. Borodakiy Yu.V., Lobodinskiy Yu.G. Informatsionnyye tekhnologii v voyennom dele (osnovy teorii i prakticheskogo primeneniya), Moscow, Goryachaya liniya - Telekom, 2008, 394 p.
4. 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, Moscow, Izd. Upravleniye delami Prezidenta Rossiyskoy Federatsii, 2008, 400 p.
5. Borodakiy Yu.V., Lobodinskiy Yu.G. Evolyutsiya informatsionnykh system, Moscow, Goryachaya liniya - Telekom, 2011, 368 p.
6. Nauchno-tekhnicheskiy sbornik FGUP «Kontsern «Sistemprom», By ed. Yu.V.Borodakiy, Moscow, FGUP «Kontsern «Sistemprom», 2011, No 1 (1).
7. Nauchno-tekhnicheskiy sbornik FGUP «Kontsern «Sistemprom», By ed. Yu.V.Borodakiy, Moscow, FGUP «Kontsern «Sistemprom», 2012, No 1 (2).
8. Nauchno-tekhnicheskiy sbornik FGUP «Kontsern «Sistemprom», By ed. Yu.V.Borodakiy, Moscow, FGUP «Kontsern «Sistemprom», 2013, No 1-2 (3).
9. Borodakiy Yu.V., Mironov A.G., Dobrodeyev A.Yu., Boldina M.N. Problemy i perspektivy sozdaniya evolyutsioniruyushchikh intellektualnykh sistem zashchity informatsii dlya sovremennykh raspredelennykh informatsionno-upravlyayushchikh sistem i kompleksov spetsialnogo i obshchego naznacheniya, Nauchnyye problemy natsionalnoy bezopasnosti Rossiyskoy Federatsii, 2012, Vyp. 5, p. 328.
10. Borodakiy Yu.V., Mironov A.G., Dobrodeyev A.Yu., Boldina M.N., Butusov I.V. Perspektivnyye sistemy zashchity informatsii dolzhny byt intellektualnymi, Zashchita informatsii. INSIDE, 2013, No 2, pp. 48-51.
11. Borodakiy Yu.V., Dobrodeyev A.Yu., Ivanova A.I., Kulikov G.V. Perspektivnaya arkhitektura intellektualnoy sistemy obespecheniya informatsionnoy bezopasnosti raspredelennoy avtomatizirovannoy sistemy, Prilozheniye k zhurnalu «Otkrytoye obrazovaniye», 2006, pp.141-142.
12. Borodakiy Yu.V., Dobrodeyev A.Yu., Butusov I.V. Doverennaya sreda-osnova garantirovannoy bezopasnosti, «Information Security/Informatsionnaya bezopasnost», 2013, No2, pp. 36-37.
13. Rastorguyev S.P. Informatsionnaya voyna. Problemy i modeli, Ekzistentsialnaya matematika v informatsionnoy voyne, Moscow, Gelios ARV, 2006, 240 p.
14. Rastorguyev S.P. Informatsionnaya voyna, Moscow, Radio i svyaz, 1999, 416 p.
15. Medin A., Marinin A. Osobennosti primeneniya kibersredstv v mezhgosudarstvennykh voyennykh i vo vnutrennikh konfliktakh, Zarubezhnoye voyennoye obozreniye (Foreign Military Review), 2013, No 3, pp. 11-16.