www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2018.2.5

УДК 681.518:004.75
ББК 32.816

РОБОТОТЕХНИЧЕСКАЯ СИСТЕМА АНАЛИЗА КИБЕРБЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ И СЕТЕЙ СВЯЗИ

Валерий Михайлович Московченко

Доктор экономических наук, профессор,
профессор кафедры информационной безопасности,
Южно-Российский государственный политехнический университет (НПИ) имени М.И. Платова
fvo.urgpu.npi@yandex.ru
ул. Просвещения, 132, 346428 г. Новочеркасск, Российская Федерация

Михаил Александрович Гудков

Кандидат технических наук, начальник отдела научно-исследовательского центра
Военной академии связи имени Маршала Советского Союза С.М. Буденного
gud-0207@mail.ru
просп. Тихорецкий, 6,194064 г. Санкт-Петербург, Российская Федерация

Олег Сергеевич Лаута

Кандидат технических наук,
преподаватель кафедры Военной академии связи имени Маршала Советского Союза С.М. Буденного
laos-82@yandex.ru
просп. Тихорецкий, 6,194064 г. Санкт-Петербург, Российская Федерация

Аннотация. В статье рассмотрены различные аспекты кибернетического противоборства, обоснована актуальность создания проактивной системы управления защитой и предложены реализующие ее аппаратно-программные решения, основанные на разработке мобильной робототехнической системы.

Представлено описание системы, предназначенной для аудита устойчивости сетевой инфраструктуры к существующим и перспективным киберугрозам, ее архитектура и функциональные возможности.

Ключевые слова: киберугроза, кибербезопасность, проактивная система управления защитой, мобильная робототехническая система, нечеткие нейронные сети, криптографический чип.

Кибернетическое противоборство знаменует собой новый уровень вооруженного противостояния. Насущным требованием времени, учитывая роботизацию вооружения и военной техники, становится пересмотр принципов построения автоматизированных систем управления, информационных систем (ИКС) и сетей связи, а также обеспечение кибербезопасности.

Коэволюция системы кибербезопасности должна обеспечить: обнаружение новых, ранее неизвестных киберугроз (кибератак) в ходе мониторинга (разведки) киберпространства; автоматический выбор параметров функционирования информационных систем и сетей связи в условиях деструктивных воздействий без ухудшения их основных характеристик (когнитивные платформы построения информационно-телекоммуникационных сетей).

Ведение разведки в киберпространстве требует цифрового проникновения в сети и системы управления потенциального противника и предусматривает использование совершенно новых источников, форм и способов сбора данных и информации, разработки подходящих разведывательных средств и технологий, тактических и технических приемов.

С учетом вышеизложенного система кибербезопасности должна предусматривать возможность проведения упреждающих аппаратно-программных воздействий (упреждающих ударов) и активных атак на информационные системы и ресурсы противоборствующей стороны, а также способность к дезинформации противоборствующей стороны об истинных свойствах и параметрах информационных систем и сетей связи.

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, определение номенклатуры потенциальных угроз кибербезопасности, создание и ведение банка критериев обнаружения кибератак на информационные системы, выявление и противодействие внедряемым боевым программным агентам и противодействия им.

Одной из причин недостаточного уровня эффективности функционирования существующей подсистемы кибербезопасности информационных систем и сетей связи является то, что она построена на основе сетевой модели, в которой принятие решений осуществляется на основе показателей работоспособности элементов сети или отдельных направлений связи, а также анализа сетевых ресурсов. Системы управления, построенные на основе сетевых моделей, включаются в процесс управления в тот момент, когда событие, требующее их реакции, уже произошло, то есть являются реактивными. Однако развитие информационных систем и требований, предъявляемых к ним, диктует необходимость создания проактивной системы управления, то есть «действующей до того, как ситуация станет критической».

Проактивное управление инцидентами и событиями безопасности должно основываться на автоматических (интеллектуальных) механизмах, которые используют информацию об «истории» анализируемых сетевых событий и прогнозе будущих событий, а также на автоматической подстройке параметров мониторинга последних к текущему состоянию защищаемой системы.

Для проведения интеллектуального анализа устойчивости инфокоммуникационных сетей к дестабилизирующим воздействиям (ДВ) из киберпространства необходимо разработать систему обнаружения ДВ, позволяющую осуществлять интеллектуальный анализ сценариев ДВ на элементы и узлы ИКС, а также оценку уровня устойчивости ИКС к ДВ из киберпространства. Логика работы такой интеллектуальной автоматизированной системы кибербезопасности (ИАСК) должна учитывать сетевую специфику киберпространства, модели атак, технологические особенности *web*-среды и достижения искусственного интеллекта [1].

С целью устранения вышеуказанной проблемы предлагаются аппаратно-программные решения, основанные на разработке мобильной робототехнической системы (см. рис. 1 и 2), предназначенной для аудита (киберразведки) устойчивости сетевой инфраструктуры и приложений к существующим и перспективным киберугрозам (стрессовой нагрузке, различным *DDoS*-атакам, вредоносному коду в общем трафике, спаму, червям, атакам типа «*zeroday*», атакам с применением технологии fuzzing, и т. д.), программно-математического воздействия на информационно-управляющие системы, физического уничтожения (или выводу из строя) объектов информационной инфраструктуры противника.

В соответствии с функциональной схемой роботизированная система должна состоять из нескольких частей:

BeagleBone Black – главный процессор роботизированной системы;

Mini Maestro 18 – Channel USB Servo Controller – драйвер-двигатель для подключения сервоприводов);

MG996R – сервоприводы);

блок питания;

Wi-Fi адаптер.

Корпус предлагается сделать в виде металлического скелета, который связывает и объединяет необходимую периферию в единое целое, обеспечивая при этом защиту и целостность компонентов [2]. Размеры этого устройства будут зависеть от выполняемых задач.

Кроме того, с целью доставки робототехнической системы до необходимого места планируется использовать 8 винтов, расположенных на ее корпусе, а для передвижения по горизонтальной и вертикальной поверхности – использовать 6 конечностей (ног). Для подключения к кабелю на корпусе будет расположен щуп (зонд).

Мобильная робототехническая система позволит реализовать следующие характеристики: скорость, мобильность, отсутствие преград

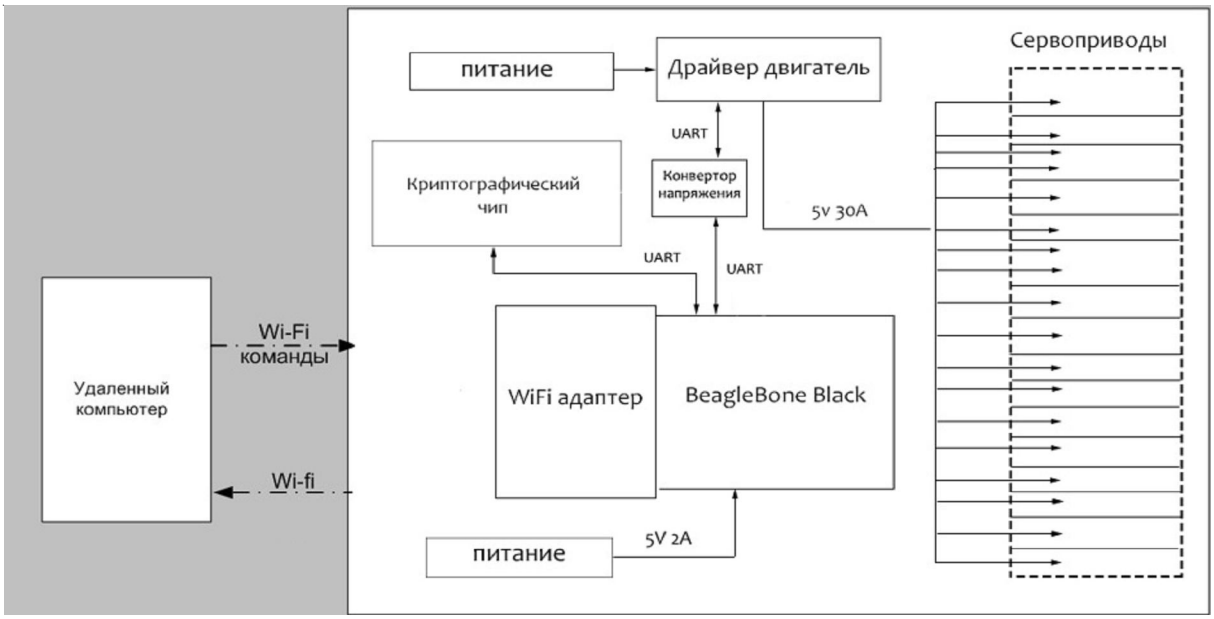

Рис. 1. Функциональная схема роботизированной системы

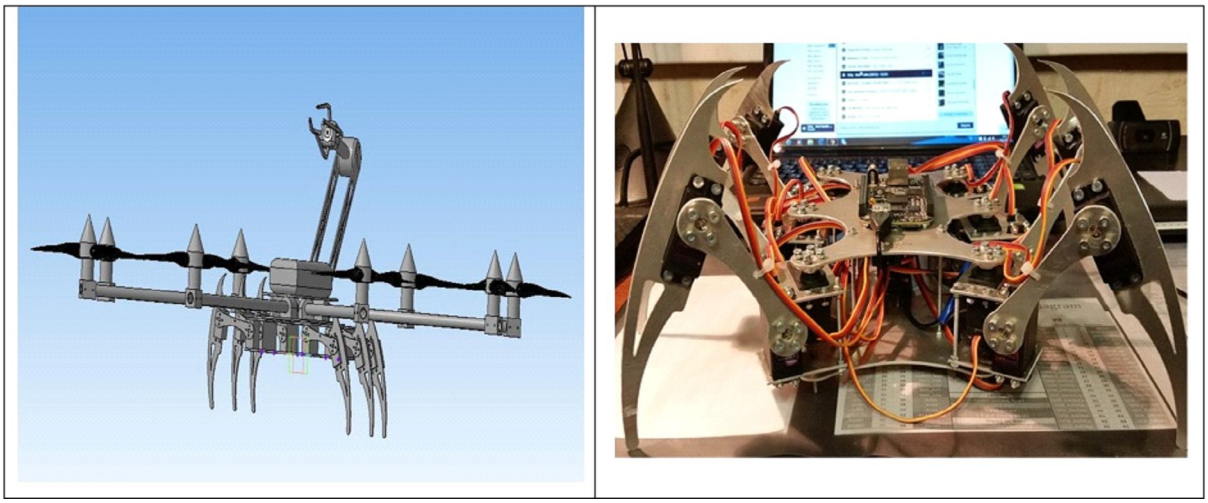

Рис. 2. Внешний вид роботизированной системы

для доступа, незаметность, низкая распознаваемость для средств противника, масштабируемость, пластичность состава роботов, входящих рой, высокий уровень координации действий, взаимная обучаемость за счет использования единой удаленной памяти, разнообразие реализуемых функций выполняемых задач.

В качестве каналов управления в робототехнической системе (РТС) предлагается применять: управление по радиоканалу (по каналу беспроводного широкополосного доступа), защищенного криптографическим алгоритмом AES; автономный режим работы [3; 9–13].

При автономной навигации роботизированная система должна использовать свой искусственный интеллект и сенсорные устройства (датчики различного типа) для следования по запрограммированному маршруту, а также избегать встречающиеся на пути непреодолимые препятствия, которые могут вывести роботизированную систему из строя.

Из-за динамического характера задач управления кибербезопасностью, их высокой размерности, сложности формирования полной системы показателей эффективности самой системы управления (из-за корреляции и нечеткого характера многих из них), неполноты и недостоверности контрольной информации целесообразно для одновременного обеспечения высокой функциональной гибкости и быстродействия РТС применять нечеткие нейронные сети, использующие нечеткое описание управляемого процесса и системы его управления в виде нечеткой базы знаний, а также преобразующей нечеткое описание в последовательность команд для достижения целей управления (рис. 3).

Особенностями предлагаемой схемы нечеткой системы управления являются: учет последовательности цикла управления, оценка ситуации, определение цели управления, выявление необходимости управления, поиск допустимых решений, способа достижения поставленной цели и его реализации.

Объединение двух независимых теорий –нейронных сетей и нечеткой логики – позволило создавать более универсальные интеллектуальные технологии, называемые нейронно-нечеткими системами, с традиционной экспертной системой, в которой знания представляются символически, с успехом используются в процессе принятия решений в сложных, многоразмерных системах для обработки различного вида знаний (см. рис. 4).

Полученная в результате интеграции технология объединяет соответствующим

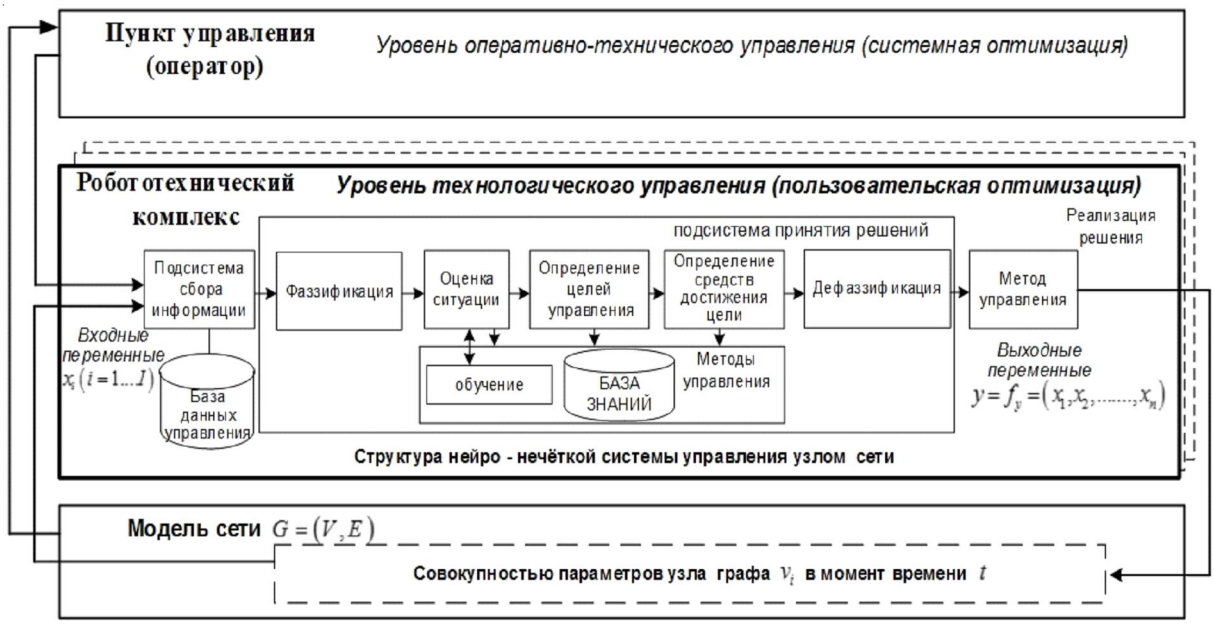

Рис. 3. Нейро-нечеткая система управления роботизированной системы (интеллектуальный агент управления)

образом способность нейронных сетей к самообучению и нечетких систем к обработке качественной информации, а также дает возможность использовать всю доступную информацию об объекте (как количественную, так и качественную). При данном подходе нейронная сеть состоит из специальных нейронов, которые представляют конкретные сущности систем с нечеткой логикой. Это позволяет представить систему в виде набора нечетких правил и при этом обучать ее как нейронную сеть [4–8].

Для одновременного обеспечения высокой функциональной гибкости и быстродействия системы управления кибербезопасностью предлагается использовать нечеткие нейронные сети, то есть алгоритмы управления реализуются программно в роботизированной системе с применением технологии распределенных интеллектуальных агентов (см. рис. 5).

Обладая вышеизложенными параметрами, представленная подсистема связи РТС будет иметь развитые интеллектуальные возможности по анализу и распознаванию обстановки, формированию стратегии целесообразного поведения, планированию последовательности действий, а также синтезу управляющих воздействий. Это позволит оптимизировать процесс управления подсистемой связи роботизированной системы, учитывая сложившуюся ситуацию в сети (уровень нагрузки в узлах, качество маршрутов передачи, остаточная емкость узловых батарей, расстояния между абонентами, скорость их передвижения, и др.), а также требования к передаче определенных типов трафика при групповом применении роботизированных систем [6].

С целью защиты канала управления предлагается в РТС внедрить криптографический чип, который будет поддерживать криптографический протокол AES и позволит шифровать открытые протоколы управления [6].

Автономный режим работы предлагается реализовать на основе средств искусственного интеллекта путем внедрения гибридной нейронно-нечеткой технологии моделирования и обработки информации.

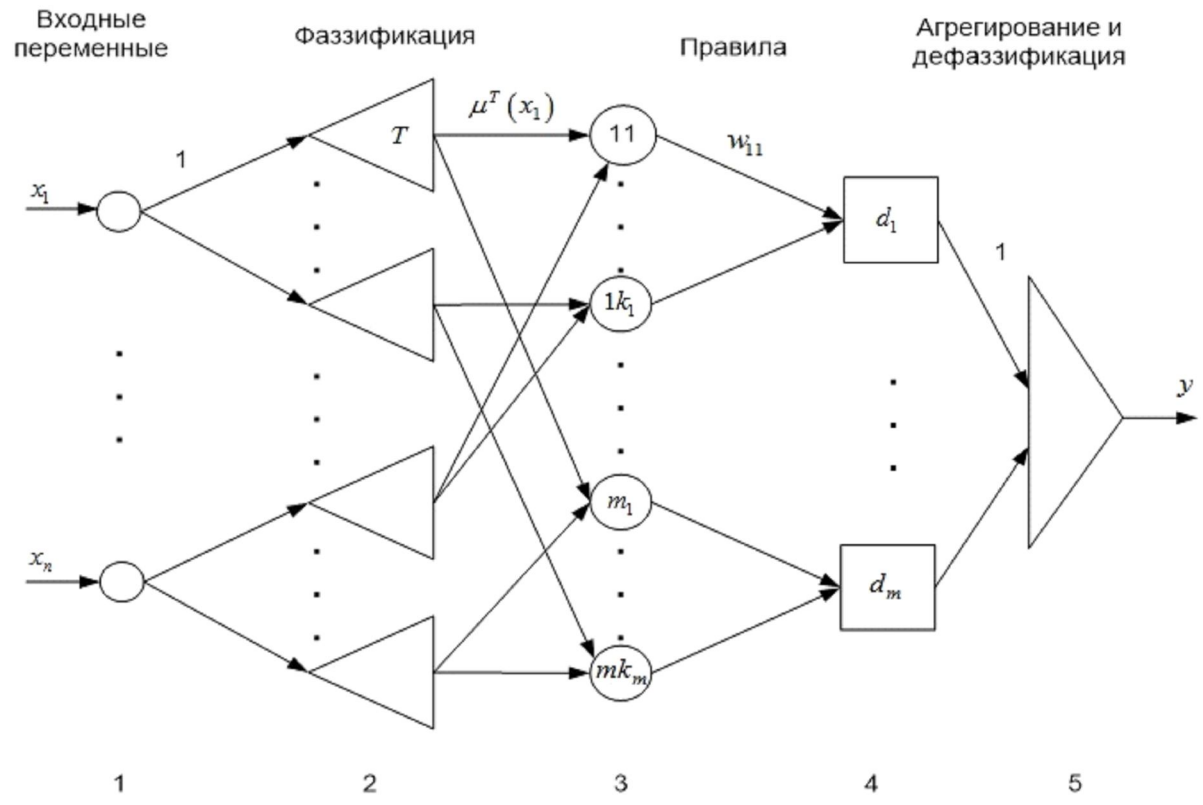

Рис. 4. Структура нейро-нечеткой сети

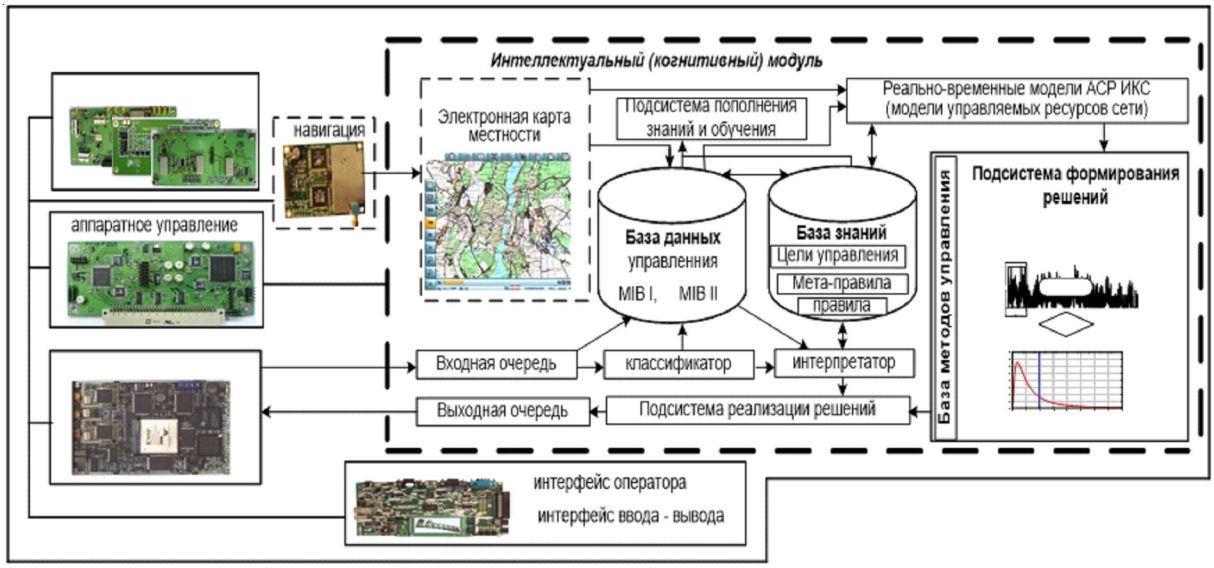

Рис. 5. Архитектура роботизированной системы кибербезопасности с интеллектуальной системой управления

Предлагаемая РТС позволяет осуществлять: анализ защищенности сетей; аудит безопасности сетей; выявление уязвимости сетей; анализ структуры сетей; ведение разведки; активное противоборство противнику; обход средств защиты; тестирование на проникновение беспроводных сетей; стресс-тестирование сетей.

СПИСОК ЛИТЕРАТУРЫ

1. Защита канала управления роботизированных систем / В. В. Баранов, М. А. Гудков, А. М. Крибель, О. С. Лаута, А. П. Нечепуренко // Актуальные проблемы обеспечения информационной безопасности труда. Труды Межвузовской научно-практической конференции : сб. тр. конф. – Саратов, 2017. – С. 32–37.

2. Кибербезопасность. Анализ нормативно-правовых документов Российской Федерации, регламентирующих политическую и военную деятельность в киберпространстве / М. А. Коцыняк, О. С. Лаута, В. О. Драчев, И. А. Клиншов // Материалы конференции ГНИИ «Нацразвитие». Ноябрь 2016 : сб. избранных статей. – СПб. : Нацразвитие, 2016. – С. 109–117.

3. Модель распределения факторов информационного воздействия по элементам информационно-телекоммуникационной сети / Д. А. Иванов, М. А. Коцыняк, О. С. Лаута, А. П. Нечепуренко //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017). VI Международная научно-техническая и научно-методическая конференция : сб. науч. ст. В 4 т. Т. 4 / под ред. С. В. Бачевского. – СПб., 2017. – С. 420–425.

4. Модель таргетированной кибернетической атаки / М. А. Коцыняк, Д. А. Иванов, О. С. Лаута, А. П. Нечепуренко // Радиолокация, навигация, связь. Материалы XXIII Международной научно-технической конференции : сб. тр. В 3 т. Т. 1. – Воронеж, 2017. – С. 90–98.

5. Методика обоснования мер противодействия радиолокационной разведке высокоточного оружия / М. А. Коцыняк, В. В. Карганов, О. С. Лаута, А. П. Нечепуренко // Вопросы оборонной техники. Серия 16, Технические средства противодействия терроризму. – 2016. – № 9–10 (99–100). – С. 54–57.

6. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия / В. В. Баранов, М. А. Коцыняк, О. С. Лаута, В. М. Московченко // Вестник Волгоградского государственного университета. Серия 10, Инновационная деятельность. – 2017. – Т. 11, № 2. – С. 11–15.

7. Методика оценки защищенности информационно-телекоммуникационной сети в условиях информационного противодействия / М. А. Коцыняк, Д. А. Иванов, О. С. Лаута, А. П. Нечепуренко // Радиолокация, навигация, связь. Материалы XXIII Международной научно-технической конференции : сб. тр. В 3 т. Т. 1. – Воронеж, 2017. – С. 83–89.

8. Методика оценки устойчивости информационно-телекоммуникационной сети в условиях информационного воздействия / М. А. Коцыняк, О. С. Лаута, А. П. Нечепуренко, И. Г. Штеренберг

// Труды учебных заведений связи. – 2016. – Т. 2, № 4. – С. 82–87.

9. Нормативно-правовые документы США, регламентирующие политическую и военную деятельность в киберпространстве / О. С. Лаута, В. В. Никитин, И. А. Клиншов, А. С. Лаута // Материалы конференции ГНИИ «Нацразвитие». Ноябрь, 2016 : сб. избр. ст. – СПб. : Нацразвитие, 2016. – С. 118–125.

10. Паращук, И. Б. Нейросетевые методы в задачах моделирования и анализа эффективности функционирования сетей связи / И. Б. Паращук, Ю. Н. Иванов, П. Г. Романенко. – СПб. : ВАС, 2010. – 104 с.

11. Применение метода топологического преобразования стохастической сети для моделирования системы воздействия / В. В. Баранов, Д. А Иванов, М. А. Коцыняк, В. М. Московченко, А. П. Нечепуренко // Актуальные проблемы обеспечения информационной безопасности труда. Труды Межвузовской научно-практической конференции : сб. тр. конф. – Саратов, 2017. – С. 38–43.

12. Робототехнические средства, комплексы и системы военного назначения: основные положения, классификация, методические рекомендации. – М. : ФГБУ «ГНИИЦ РТ» МО РФ, 2014. – 36 с.

REFERENCES

1. Baranov V.V., Gudkov M.A., Kribel A.M., Lauta O.S., Nechepurenko A.P. Zashchita kanala upravleniya robotizirovannykh sistem [Protection of the control channel of robotic systems]. *Aktualnye problemy obespecheniya informatsionnoy bezopasnosti truda. Trudy Mezhvuzovskoy nauchno-prakticheskoy konferentsii* [Current Problems of Information Security of Labour. Proceedings of the International Research and Practice Conference]. Saratov, 2017, pp. 32-37.

2. Kotsynyak M.A., Lauta O.S., Drachev V.O., Klinshov I.A. Kiberbezopasnost. Analiz normativno-pravovykh dokumentov Rossiyskoy Federatsii, reglamentiruyushchikh politicheskuyu i voennuyu deyatelnost v kiberprostranstve [Cybersecurity. Analysis of Legal Documents of the Russian Federation Regulating Political and Military Activities in Cyberspace]. Pavlov L.A., ed. *Materialy konferentsii GNII «NATsRAZVITIE» (Noyabr 2016)* [Proceedings of the Conference 'National Development' (November 2016)]. 2016, pp. 109-117.

3. Ivanov D.A., Kotsynyak M.A., Lauta O.S., Nechepurenko A.P. Model raspredeleniya faktorov informatsionnogo vozdeystviya po elementam informatsionno-telekommunikatsionnoy seti [Model of distribution of factors of information influence on elements of information and telecommunication network]. Bachevsky S.V., ed. *Aktualnye problemy infotelekommunikatsiy v nauke i obrazovanii (APINO 2017). VI Mezhdunarodnaya nauchno-tekhnicheskaya i nauchno-metodicheskaya konferentsiya: sb. nauch. st. V 4 t. T. 4* [Proceedings of the 6th International Research, Practice and Methodological Conference 'Current Problems of Info- Telecommunication in Science and Education (APINO 2017)'. In 4 vols. Vol. 4]. Saint Petersburg, 2017, pp. 420-425.

4. Kotsynyak M.A., Ivanov D.A., Lauta O.S., Nechepurenko A.P. Model targetirovannoy kiberneticheskoy ataki [Model of targeted cyber attack]. *Radiolokatsiya, navigatsiya, svyaz. Materialy XXIII Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii: sb. tr. V 3 t. T. 1.* [Proceedings of the 23rd International Scientific and Technical Conference 'Radiolocation, Navigation, Communication'. In 3 vols. Vol. 1]. Voronezh, 2017, pp. 90-98.

5. Kotsynyak M.A., Karganov V.V., Lauta O.S., Nechepurenko A.P. Metodika obosnovaniya mer protivodeystviya radiolokatsionnoy razvedke vysokotochnogo oruzhiya [Substantiation of Measures of Counteraction to Radar Reconnaissance of High-Precision Weapons]. *Voprosy oboronnoy tekhniki. Seriya 16: Tekhnicheskie sredstva protivodeystviya terrorizmu*, 2016, no. 9-10 (99-100), pp. 54-57.

6. Baranov V.V., Kotsynyak M.A., Lauta O.S., Moskovchenko V.M. Metodika otsenki ustoychivosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo vozdeystviya [Estimating Sustainability of Telecommunication Networks in Terms of Information Influence]. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Seriya 10: Innovatsionnaya deyatelnost* [Science Journal of Volgograd State University. Innovation Technology], 2017, vol. 11, no. 2, pp. 11-15.

7. Kotsynyak M.A., Ivanov D.A., Lauta O.S., Nechepurenko A.P. Metodika otsenki zashchishchennosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo protivodeystviya [Estimating the Security of Information and Telecommunications Network in the Conditions of Information Counteraction]. *Radiolokatsiya, navigatsiya, svyaz. Materialy XXIII Mezhdunarodnoy nauchno-tekhnicheskoy konferentsii: sb. tr. V 3 t. T. 1.* [Proceedings of the 23rd International Scientific and Technical Conference 'Radiolocation, Navigation, Communication'. In 3 vols. Vol. 1]. Voronezh, 2017, pp. 83-89.

8. Kotsynyak M.A., Lauta O.S., Nechepurenko A.P., Shterenberg I.G. Metodika otsenki ustoychivosti informatsionno-telekommunikatsionnoy seti v usloviyakh informatsionnogo vozdeystviya [Estimating the Sustainability of Telecommunication Networks in Terms of Information Influence]. *Trudy uchebnykh zavedeniy svyazi*, 2016, vol. 2, no. 4, pp. 82-87.

9. Lauta O.S., Nikitin V.V., Klinshov I.A., Lauta A.S. Normativno-pravovye dokumenty SShA,

reglamentiruyushchie politicheskuyu i voennuyu deyatelnost v kiberprostranstve [Regulatory Legal Documents of the USA, Regulating Political and Military Activity in Cyberspace]. Pavlov L.A., ed. *Materialy konferentsii GNII «NATsRAZVITIE» (Noyabr 2016)* [Proceedings of the Conference 'National Development' (November 2016)]. 2016, pp. 118-125.

10. Parashchuk I.B., Ivanov Yu.N., Romanenko P.G. *Neyrosetevye metody v zadachakh modelirovaniya i analiza effektivnosti funktsionirovaniya setey svyazi* [Neural Network Methods in Solving the Problems of Modeling and Analysis of Communication Networks Efficiency]. Saint Petersburg, VAS Publ., 2010. 104 p.

11. Baranov V.V., Ivanov D.A, Kotsynyak M.A., Moskovchenko V.M., Nechepurenko A.P. Primenenie metoda topologicheskogo preobrazovaniya stokhasticheskoy seti dlya modelirovaniya sistemy vozdeystviya [Application of the Method of Topological Transformation of the Stochastic Network for Modeling the System of Influence]. *Aktualnye problemy obespecheniya informatsionnoy bezopasnosti truda. Trudy Mezhvuzovskoy nauchno-prakticheskoy konferentsii* [Current Problems of Information Security of Labour. Proceedings of the International Research and Practice Conference]. Saratov, 2017, pp. 38-43.

12. *Robototekhnicheskie sredstva, kompleksy i sistemy voennogo naznacheniya: osnovnye polozheniya, klassifikatsiya, metodicheskie rekomendatsii* [Robotics, Systems and Systems for Military Purposes. Fundamentals. Classification]. Moscow, GNIITs RT Publ., 2014. 36 p.

ROBOTECHNICAL SYSTEM FOR ANALYZING CYBER-SECURITY OF INFORMATION COMMUNICATION SYSTEMS AND NETWORKS

Valeriy M. Moskovchenko

Doctor of Sciences (Economics), Professor,
Department of Information Security, South-Russian State Polytechnic University named after M.I. Platov
fvo.urgpu.npi@yandex.ru
Prosveshcheniya St., 132, 346428 Novocherkassk, Russian Federation

Mikhail A. Gudkov

Candidate of Sciences (Engineering), Head of Department of the Research Center,
Military Academy of the Signal Corps named after Marshal
of the Soviet Union S.M. Budenny
gud-0207@mail.ru
Prosp. Tikhoretsky, 6, 194064 Saint Petersburg, Russian Federation

Oleg S. Lauta

Candidate of Sciences (Engineering),
Teacher, Military Academy of the Signal Corps named after Marshal of the Soviet Union S.M. Budenny
laos-82@yandex.ru
Prosp. Tikhoretsky, 6, 194064 Saint Petersburg, Russian Federation

Abstract. The paper deals with the various aspects of cybernetic confrontation. The authors substantiate the urgency of creating a proactive protection management system and propose hardware and software solutions based on the development of a mobile robotic system. The paper describes the system designed to audit the stability of the network infrastructure to existing and prospective cyber threats, to its architecture and functionality.

Cyber warfare marks a new level of armed confrontation. An urgent requirement of the time, taking into account the robotization of weapons and military equipment, is the revision of the principles of building automated control systems, information systems and communication networks from the viewpoint of ensuring cybersecurity.

The co-evolution of the cybersecurity system should provide: the detection of new, previously unknown cyber threats (cyber attacks) during the monitoring (exploration) of cyberspace; the automatic selection of the parameters of the functioning of information systems and communication networks under the conditions of destructive effects without deterioration of their main characteristics (cognitive platforms for building information and telecommunication networks).

Intelligence in cyberspace requires digital penetration into the network and control systems of a potential enemy and involves the use of completely new sources, forms and methods of data and information collection, development of new intelligence tools and technologies, tactical and technical techniques.

Thus, the system of cyber security should be provided for the possibility of pre-emptive hardware and software effects (pre-emptive attacks) and active attacks on information systems and resources of the opposing side, as well as the ability to misinformation by the opposing side of the true properties and parameters of information systems and communication networks.

Key words: cyber threat, cyber security, proactive defense management system, mobile robotic system, fuzzy neural networks, cryptographic chip.