УДК 004.056:004.738.5

С.П. Евсеев,
кандидат технических наук, доцент,
Ю.Е. Хохлачева,
кандидат технических наук,
О.Г. Король
кандидат технических наук, доцент

ОЦЕНКА ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОСТИ БИЗНЕС-ПРОЦЕССОВ В ОРГАНИЗАЦИЯХ БАНКОВСКОГО СЕКТОРА НА ОСНОВЕ СИНЕРГЕТИЧЕСКОГО ПОДХОДА[1]

Исследована задача обеспечения непрерывности бизнес-процессов в организациях банковского сектора в условиях увеличения киберугроз.

Проанализированы основные тенденции развития кибербезопасности в условиях совершенства средств и способов ведения террористических информационных атак на объекты критически важных инфраструктур. Определены превентивные меры снижения риска реализации кибератак на национальном и международном уровне, позволяющие обеспечить непрерывность работы объектов с критической кибернетической инфраструктурой.

Ключевые слова: *кибертерроризм, кибератака, критическая инфраструктура, непрерывность бизнес-процессов.*

Досліджено завдання забезпечення безперервності бізнес-процесів в організаціях банківського сектора в умовах збільшення кіберзагроз.

Проаналізовано основні тенденції розвитку кібербезпеки в умовах досконалості засобів і способів ведення терористичних інформаційних атак на об'єкти критично важливих інфраструктур. Визначено превентивні заходи зниження ризику реалізації кібератак на національному та міжнародному рівні, що дозволяють забезпечити безперервність роботи об'єктів з критичною кібернетичною інфраструктурою.

Ключові слова: *кібертероризм, кібератака, критична інфраструктура, безперервність бізнес-процесів.*

The issue of providing a continuity of business processes in the organizations of the banking sector in the conditions of increasement of cyberthreats is investigated.

The main tendencies of the development of cyber security in the conditions of perfection of means and ways of conducting the terrorist information attacks on the objects of crucial infrastructures are analyzed. The preventive measures of decrease in risk of realization of cyber attacks at national and international level allowing to provide a continuity of work of objects with critical cybernetic infrastructure are defined.

Keywords: *cyberterrorism, cyber attack, critical infrastructure, continuity of business processes.*

---

[1] Закінчення в наступному номері.

Введение и анализ литературы

Развитие общества в начале XXI столетия характеризуется, в первую очередь, переходом от информационного общества к обществу высоких технологий, обеспечивающих перенасыщенность новейшими информационными и коммуникационными технологиями, дальнейшее развитие глобализационных процессов в современной экономике, динамику информатизации таких областей деятельности общества, как сфера связи, энергетики, транспорта, системы добычи и хранения нефти и газа, финансовую и банковскую системы, оборонной и национальной безопасности, структуры обеспечения стабильной работы министерств и ведомств, повсеместный переход на методы электронного управления и документооборота [1–3]. Во вторую очередь, информационные процессы, происходящие повсеместно в мире, выдвигают на первый план важнейшую задачу обеспечения безопасности информации. Это объясняется особой значимостью для развития государства его информационных ресурсов, ростом стоимости информации в условиях рынка, ее высокой уязвимостью и нередко значительным ущербом в результате ее несанкционированного использования [1–7]. В третью очередь, бурное развитие Интернета и других информационно-коммуникационных технологий формирует глобальное информационное пространство, позволяющее создать новые угрозы и новые формы международных конфликтов, включая информационные войны, сетевые противоборства, хакерские атаки и т.п. Развитие компьютерных технологий и информационно-телекоммуникационных сетей дает большие возможности обществу, в тоже время порождает и новый вид преступлений – киберпреступность [4; 6]. В 2015 году террористическая организация “Исламское государство Ирака и Леванта” (ИГИЛ) обзавелась подразделением, занимающимся проведением компьютерных атак. В сети Интернет данное подразделение известно под названием Cyber Caliphate, основными целями которого является взлом и раскрытие конфиденциальной информации, атаки на интернет-ресурсы, в число которых входят сайты банков, научных центров, государственных предприятий и др. [8]. О степени опасности для общества электронных преступлений можно судить по тем расходам на средства защиты, которые считаются допустимыми и целесообразными. По оценкам специалистов по безопасности электронного документооборота США, общие затраты на защиту банковских или других финансовых учреждений могут составить всего около 510 тысяч долларов. Однако считающаяся надежной система защиты крупного финансового учреждения, которое обслуживает до 80000 клиентов, стоит не менее 15 миллионов долларов, причем в эту сумму входят только стоимости аппаратных и программных средств (без учета оплаты труда наемного штата собственных сотрудников безопасности компании) [7].

Целью работы является рассмотрение задачи обеспечения непрерывности бизнес-процессов в организациях банковского сектора (ОБС) в условиях увеличения киберугроз, на основе анализа способов совершения преступлений террористической направленности на объекты критической инфраструктуры.

Анализ способов совершения преступлений террористической направленности на объекты критической инфраструктуры

Информационные угрозы могут проявлять себя в разных формах. Кибертерроризм характеризуется стремлением к существенной дестабилизации общест-

венного порядка. Это явление неразрывно связано с развитием информационной инфраструктуры: при постоянно возрастающей зависимости общества от бесперебойного функционирования вычислительных систем действия, направленные на их разрушение, наносят все более значительный ущерб и вызывают серьезный общественный резонанс [7]. При этом под *кибертерроризмом* будем понимать целенаправленное запугивание населения и органов власти реальными или возможными и провозглашенными (заявленными) кибернетическими воздействиями на социум, социотехнические и технические системы, совершение которых приводит к возникновению (создание предпосылок для возникновения) опасности для граждан, общества, государства [1]. Особую озабоченность в последнее десятилетие вызывает использование международным терроризмом для осуществления террористических акций существующих информационных ресурсов, в первую очередь, сети Интернет. Глобальная сеть привлекает террористические группы следующими своими особенностями:

– оперативностью, экономичностью и доступностью;

– слабой цензурой или полным отсутствием ее и какого-либо контроля со стороны государства;

– наличием огромной потенциальной аудитории пользователей, разбросанной по всему миру;

– быстрым и относительно дешевым распространением специально подобранной информации, комплексностью ее подачи и восприятия (рассылка электронных писем, организация новостных групп, создания сайтов для обмена мнениями, размещения информации на отдельных страницах или в электронных версиях периодических изданий и сетевого вещания и др.);

– большинство серверов коммуникационных сетей позволяют пользователям работать относительно конфиденциально и анонимно;

– существует возможность использования специальных роботов (bots) для снижения времени и затрат на террористическую деятельность;

– высокой эффективностью последствий, которые могут иметь как локальный, так и глобальный характер;

– киберпреступления сложно отследить и собрать доказательства;

– неопределенностью места, времени и процесса подготовки к осуществлению кибертеракта;

– возможностью организации актов кибертеррора одновременно на различные объекты или субъекты с различных направлений без необходимости нарушения любых границ;

– возможностью несанкционированного подключения к компьютерным сетям управления стратегическими объектами, в том числе военными;

– высокой степенью анонимности при осуществлении кибертеракторов;

– пространственно-временной удаленностью от объекта или субъекта кибератаки. Все кибернетические влияния осуществляются в киберпространстве и непосредственно через киберпространство. Основные средства кибертерроризма представлены на рис. 1 [1; 6; 9].

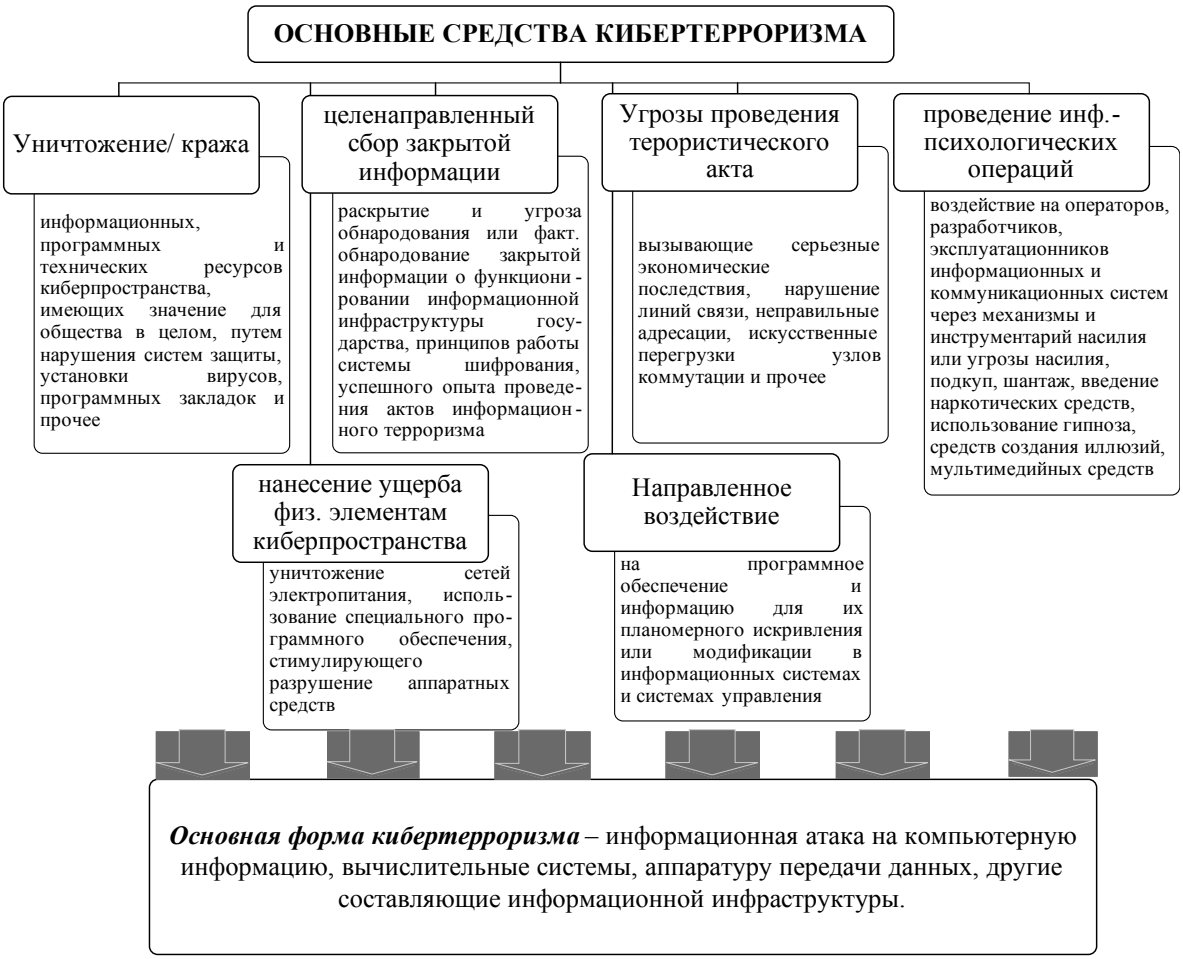

Рис. 1. Основные средства кибертерроризма

Анализ рис. 1 показывает что, терроризм все более становится информационной технологией особого типа, поскольку террористы все шире используют возможности современных информационно-телекоммуникационных систем для связи и сбора информации, большинство террористических актов рассчитаны не только на нанесение материального ущерба и угрозу жизни и здоровью людей, но и на информационно-психологический шок, воздействие которого на большие массы людей создает благоприятную обстановку для достижения террористами своих целей.

Таким образом, в условиях наращивания в мире процессов глобализации и формирования информационного общества терроризм стал выступать в качестве самостоятельного фактора, способного угрожать государственной целостности стран и дестабилизировать международную обстановку. Террористическими группами все чаще задействуются возможности новейших информационных технологий и сети Интернет для распространения пропаганды и обмена информацией, привлечения новых наемников, сбора финансовых средств в свою поддержку, планирования терактов, а также для осуществления контроля за их проведением [9].

Основные направления использования новейших информационных технологий и сети Интернет в террористических целях приведены на рис. 2.

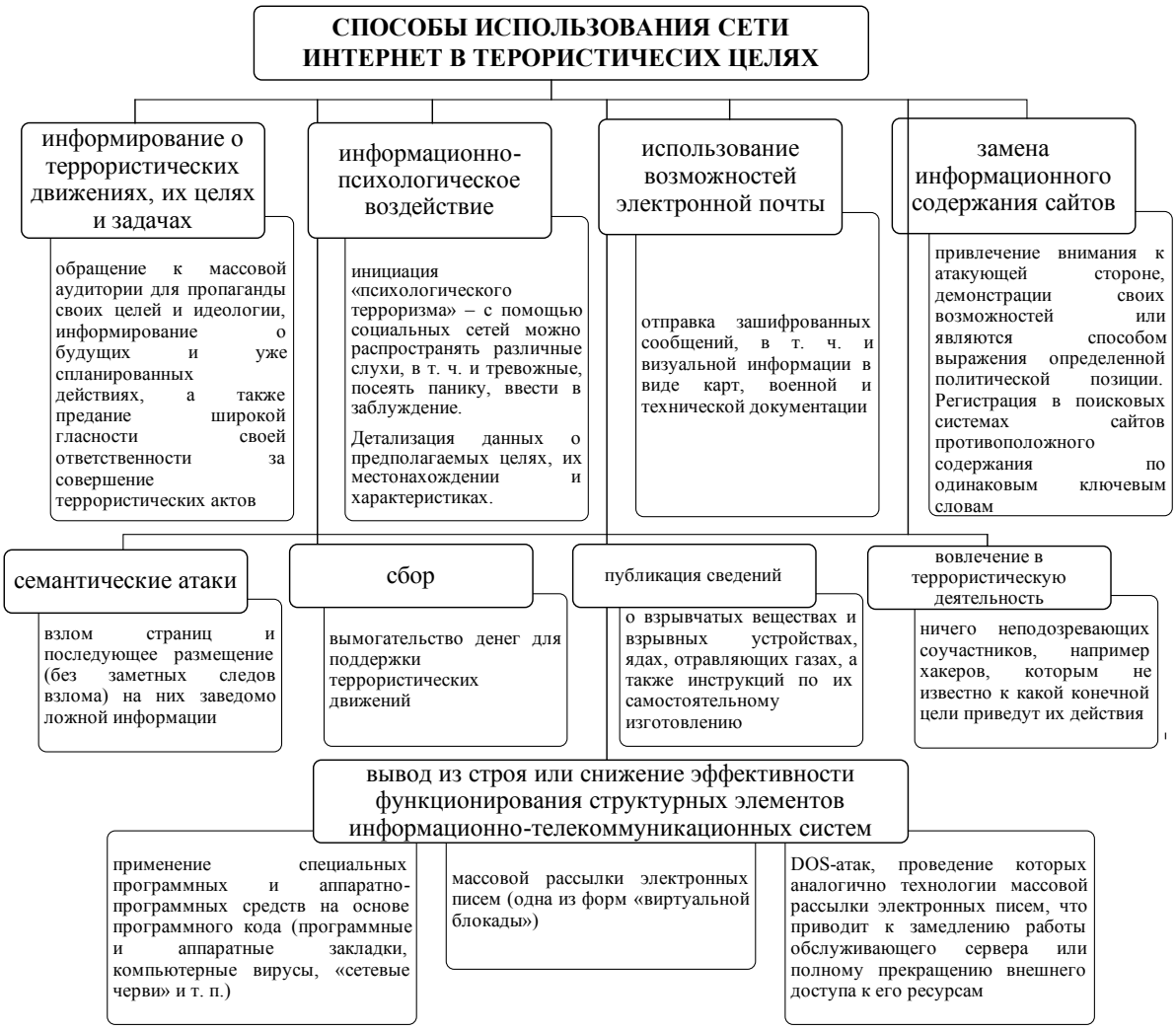

Рис. 2. Основные способы использования сети Интернет

Проведенный анализ рис. 2 показал, что социальные сети активно используются для пропаганды демонстрации якобы безбедной жизни боевиков, военного образа жизни и героизма боевиков, призыву бороться за свои идеалы с оружием в руках, трансляции сцен удачных боевых действий и актов устрашения. Фото и видеоотчеты сопровождаются джихадистскими песнями, которые занимают важное место в формируемой культурной матрице глобального террористического сообщества. У них есть собственное мобильное приложение и интернет-магазин, где можно купить футболку или худи с логотипом террористов. Вся эта опасная для сознания продукция распространяется на многих языках мира.

Активное использование ИГИЛ киберпространства в Европе показало следующую картину: 84 % – молодых людей пришли в ряды террористической организаций посредством сети Интернет; 47 % – обратили внимание на материалы (видео, текст), размещенные онлайн; 41 % – присягнули на верность ИГИЛ онлайн; 19 % – пользовались онлайн-инструкциями при подготовке теракта (изготовление самодельных взрывных устройств и бомб) [9]. Основная задача подобных продуктов – привлечь и заинтересовать любопытствующих, втянуть их в общение в формате вопрос–ответ с целью психологической обработки для последующей

изоляции человека от близкого окружения и социума в целом и вовлечения в ряды террористов.

Таким образом, в отличии от традиционного терроризма, который не угрожал обществу как таковому и не затрагивал основ его жизнедеятельности, современный высокотехнологичный терроризм способен продуцировать системный кризис в любом государстве с высокоразвитой информационной инфраструктурой. Развитие социальных сетей сопровождается все более широким использованием их возможностей для осуществления информационного противоборства, возрастанием координации, масштабов и сложности действий его участников, в качестве которых чаще всего выступают как государства, так и отдельные организованные группы, в т. ч. террористические. Объектом кибератак все чаще становятся информационные ресурсы, вывод из строя или "затруднение" функционирования которых может нанести противостоящей стороне значительный экономический ущерб или вызвать большой общественный резонанс [9; 10].

Критические информационные инфраструктуры

Использование террористами новейших разработок в сфере информационно-коммуникационных технологий позволяют радикально менять методы террористической деятельности, формировать гибкие и эффективные сетевые организационные структуры, объединяющие отдельные группы в транснациональные террористические группировки, которые очень трудно обнаружить к совершению террористического акта. Информационные атаки как правило подразделяются на две категории: вывод из строя информационного ресурса и разрушительные атаки. Разрушительные атаки – информационные (хакерские) операции против объектов, которые способны уничтожить информационный ресурс, линии коммуникации или вызвать физическое уничтожение структур, включающих информационные системы [3]. Если системы действуют в критических инфраструктурах, то при худшем развитии событий сетевые информационные атаки могут иметь масштабные последствия с человеческими жертвами, как и традиционные террористические акты.

Критически важная инфраструктура имеет ключевое значение для общественного порядка, экономической стабильности и национальной безопасности государств, ее защита затрагивает вопросы национальной безопасности, и потому входит в компетенцию государства. Тем не менее, большая часть инфраструктур находится в собственности частного бизнеса, поэтому государство и бизнес вынуждены совместно нести ответственность за безопасность и стабильное функционирование данных систем [5].

На сегодняшний день государства самостоятельно определяют, что относить к критически важным инфраструктурам, в зависимости от экономического состояния государства, политического руководства, географических и исторических особенностей. "Акт Патриота" (Patriot Act) США дает следующее определение – "критические инфраструктуры – это системы и ресурсы, физические или виртуальные, настолько значимые для США, что их разрушение или нарушение нормальной работы способно подорвать военно-политическую безопасность государства, экономическую стабильность, здоровье граждан и общественный порядок, или повлечь за собой несколько вышеуказанных факторов в любой комбинации" [11]. В Украине на законодательном и нормативном уровне не даны определения критически важных объектов и ключевых систем информационной

инфраструктуры. Учитывая анализ публикации специалистов из Российской Федерации, США, ряда стран Европы авторы предлагают обобщенные определения критически важных объектов (далее – КВО) и критически важной ключевай системы информационной инфраструктуры Украины (далее – КСИИ) [12].

Критически важный объект – объект, нарушение (или прекращение) функционирования которого приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок [12].

Ключевая система информационной инфраструктуры – это информационно-управляющая или информационно-телекоммуникационная система, которая отвечает одному из требований:

– осуществляет управление КВО (процессом);

– осуществляет информационное обеспечение управления КВО (процессом);

– осуществляет информирование граждан о чрезвычайных ситуациях [12].

Таким образом, главной характеристикой критической инфраструктуры является ее ключевое значение для безопасности общества и государства. Критически важные инфраструктуры могут иметь двойное назначение, и относиться как к КВО военного назначения, так и к КВО гражданского назначения. В табл. 1 приведены соотношения критических инфраструктур государств Украины и США.

Таблица 1

Критически важные инфраструктуры государств Украины и США

КВО Украины	КВО США	Назначение
здравоохранение	здоровье общества	гражданские объекты
сельское хозяйство	питание и сельское хозяйство	объекты двойного назначения
водоснабжение	вода	
государственное управление	государственное управление	
информационные и телекоммуникационные сети	информационные и телекоммуникационные сети	
энергетические системы	энергетические системы	
банковская и финансовые системы	банковская и финансовые системы	
химическая промышленность	химическая промышленность и взрывоопасные материалы	
теплоснабжение	–	
транспортная система	наземный и водный транспорт	
индустриальная промышленность	критически важное производство	
военно-промышленный комплекс	военно-промышленный комплекс	военный объект
гражданская оборона	службы экстренного реагирования	объекты двойного назначения

Таким образом, анализ табл. 1. показывает, что ОБС относятся к КВО, а АБС обеспечивают автоматизацию и непрерывность бизнес-процессов, обработку, хранение и передачу больших объемов Бин, необходимых для деятельности ОБС, следовательно, от надежности и безопасности функционирования информационной инфраструктуры АБС напрямую зависит непрерывность бизнес-процессов, доступность и целостность данных БИн, а значит и деятельность ОБС в целом.

Анализ и обобщение существующего опыта антитеррористической деятельности позволили сформулировать задачи по защите критической инфраструктуры от кибертерроризма, основные мероприятия, направленные на их решение, представлены в табл. 2 [1; 5; 6; 9; 12]. Комплексное решение перечисленных задач позволит принимать в централизованном порядке необходимые контрмеры для противодействия кибертерроризму, существенно снизить вероятность реализации его угроз в отношении критической инфраструктуры и обеспечить защиту своих национальных интересов.

Таблица 2

Основные мероприятия, направленные на предотвращение киберпреступности

на национальном уровне	*на международном уровне*
организация мониторинга и прогнозирования потребностей экономических и других структур в различных видах информационного обмена через сети Интернет	организация межгосударственного сотрудничества в работе международных организаций, общественных комитетов и комиссий в проектах развития мировых информационных сетей
координация мер государственных и негосударственных ведомств по предотвращению угроз информационной безопасности в открытых сетях. Разработка единой политики, предусматривающая защиту сетевого оборудования на территории страны от проникновения в него скрытых элементов информационного оружия	активное участие в разработке международного законодательства и нормативно-правового обеспечения функционирования глобальных сетей открытой инфраструктуры
разработка государственной программы совершенствования информационных технологий, обеспечивающих подключение национальных и корпоративных сетей к открытым сетям при соблюдении требований безопасности информационных ресурсов	создание единого антитеррористического пространства стран-союзников
совершенствование технологий своевременного обнаружения и нейтрализации несанкционированного доступа к информации, создание и использование опережающих технологий	разработка научно-методического обеспечения по пресечению транснациональных (трансграничных) террористических атак с использованием глобальных сетей, выработка единого понятийного аппарата, шкалы оценки киберугроз и их последствий
разработка национального законодательства в части правил обращения с информационными ресурсами, регламента прав, обязанностей и ответственности пользователей сетей открытой инфраструктуры	выработка механизмов взаимного информирования о широкомасштабных компьютерных атаках и крупных инцидентах в киберпространстве, а также способов совместного реагирования на угрозы кибертерроризма
установление перечня информации, не подлежащей передаче по открытым сетям, и обеспечение контроля за соблюдением установленного статуса информации	унификация национальных законодательств в сфере защиты критической инфраструктуры от кибертерроризма

Проведенный анализ табл. 1, 2 показал, что основные усилия каждого государства должны быть нацелены на обеспечение безопасности объектов с критической кибернетической структурой, входящих в состав сложной метасистемы государства, интеграционные действия, позволяющие объединить усилия мирового сообщества в борьбе с терроризмом в целом, и его проявлением в виде кибертерроризма в частности [1].

Выводы

Таким образом, проанализированы основные тенденции развития кибербезопасности в условиях совершенства средств и способов ведения террористических информационных атак на объекты критически важных инфраструктур. Определены превентивные меры снижения риска реализации кибератак на национальном и международном уровне, позволяющие обеспечить непрерывность работы объектов с критической кибернетической инфраструктурой.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. *Грищук Р.В.* Основи кібернетичної безпеки : монографія / Р.В. Грищук, Ю.Г. Даник ; за заг. ред. Ю.Г. Данника. – Житомир : ЖНАЕУ, 2016. – 636 с.

2. *Волковский Н.Л.* История информационных войн. В 2 ч. / Н.Л. Волковский. – СПб. : ООО "Издательство "Полигон". – Ч. 2. – 2003. – 736 с.

3. *Пелевина Е.С.* Информационные угрозы кибертерроризма / Е.С. Пелевина // Евразийский Союз Ученых (ЕСУ). – 2015. – № 11(20) Политические Науки. – С. 100–103.

4. *Бок А.А.* Некоторые вопросы борьбы с киберпреступностью в Германии / А.А. Бок, Д.А. Николаева [Электронный ресурс]. – Режим доступа : http://cj.isea.ru/pdf.asp?id=8613.

5. *Коротков А.В.* Безопасность критических информационных инфраструктур в международном гуманитарном праве /А.В. Коротков, Е.С. Зиновьева [Электронный ресурс]. – Режим доступа : http://cyberleninka.ru/article/n/bezopasnost-kriticheskih-informatsionnyh-infrastruktur-v-mezhdunarodnom-gumanitarnom-prave.

6. *Иванченко Е.В.* Тенденции развития кибертерроризма / Е.В. Иванченко, В.А. Хорошко // МНПК "Современные информационные и электронные технологии" Одесса, 26–30 мая 2014 г. – С. 105–106.

7. *Маслакова Е.А.* Кибертерроризм как новая форма терроризма / Е.А. Маслакова // Наука и Практика. – 2015. – № 2 (63). – С. 79–81.

8. Кибератаки исламского государства (ИГИЛ) на объекты и компании Российской Федерации [Электронный ресурс]. – Режим доступа : http://www.inside-zi.ru/pages/3_2015/22.html.

9. *Королев А.* Киберпространство и информационный терроризм / А. Королев [Электронный ресурс]. – Режим доступа : http://vpoanalytics.com/2016/02/15/kiberprostranstvo-i-informacionnyj-terrorizm/.

10. Некоторые аспекты кибертерроризма [Электронный ресурс]. – Режим доступа : http://nk.org.ua/geopolitika/nekotoryie-aspektyi-kiberterrorizma-16846.

11. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.

12. *Леоненко Г.П.* Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины / Г.П. Леоненко, А.Ю. Юдин // Information Technology and Security. – 2013. – № 1(3). – С. 44–48.

Отримано 10.02.2017

Рецензент Рибальський О.В., д.т.н.