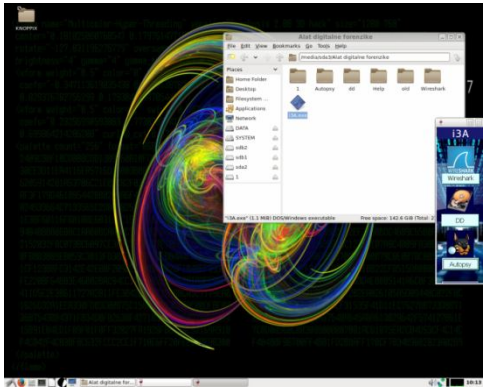

Fig. 6. Testing I3A on a Knoppix OS

The tool mentioned in this paper, SIFT workstation as integrated tool, is recognized and accepted by the courts of the USA on the basis of permanent positive Daubert test. In order to determine whether the forensic tool iA3, which is developed at the Academy of Criminalistic and Police Studies, is acceptable to the court, or whether the evidence obtained with this tool are admissible in court Daubert test was used.

Daubert process identifies four general categories that were used as the main evidence in assessing acceptability of the tool in court:

1. Testing: Can it be tested and whether the procedure was tested?
2. Expectancy: Is there a known probability of error of the procedure?
3. Publications: Is the procedure public?
4. Acceptability: Are the procedures generally accepted by the relevant scientific community?

The software solution has been done according to the regulations of the Ministry of Education, Science and Technological Development, and the tool iA3 is tested by the Ministry of Internal Affairs (the Cybercrime Department). The tool testing started in 2015 and it is still being tested. After completion of the test the evaluation and the possibility of its admissibility in court will be given.

The probability of error, which refers to errors known as “bugs” in the work tools where not noticed while working with these tools and in the previous test.

The tool has been published in several publications:

a) D. Randjelović, D. Delija, D. Stojković, M. Velicković, D. Erlevajn. COMPARING INTEGRATED AND NON-INTEGRATED DIGITAL FORENSICS TOOLS, Thematic Conference proceedings Archibald Reiss days, Vol. 3. Pp. 239–262. Belgrade, 2016;

b) T. Milanović, K. Kuk, D. Randjelović, P. Čisar Text mining techniques and identification of information by documents written (in Serbian) in High-end International Forum on Public Security Technology Informatisation, Shenyang, China, September 2015.

The tool is set up and is available on the website of the Academy of Criminalistic and Police Studies.

Based on everything mentioned above, we can say that iA3 is pretty good software solution that could be accepted in court and also from the technical standpoint it has best characteristics under Linux Ubuntu.

This work was supported by the Ministry of Science and Technology of the Republic of Serbia under the Project no. III 44007 and TR34019.

УДК 343.346.8:004:351.746:007

Ю.Г. Булай, Р.И. Булай, А.В. Патрашко

СЕТЕЦЕНТРИЧЕСКАЯ И КИБЕРВОЙНА – РЕАЛЬНЫЕ УГРОЗЫ БЕЗОПАСНОСТИ СОВРЕМЕННОГО МИРА

Существование современного мира немыслимо без информационных технологий, они стали неотъемлемой частью общества и каждого индивида в отдельности. Информационные технологии представляют огромные возможности для упрощения и улучшения всей жизнедеятельности человечества.

Стремительное развитие информационных технологий и информатизации общества привело к появлению новых видов преступлений и угроз, таких как киберпреступность, кибертерроризм, сетецентрическая и кибервойна.

Кибершпионаж, киберпреступность, кибертерроризм – феномены, получившие развитие в виде глобальной киберугрозы сетецентрической и кибервойны. При этом необходимо подчеркнуть, что как в материальном мире, так и в электронном пространстве все эти феномены тесно переплетены и взаимодействуют между собой. Такое взаимодействие характерно также для атакующих субъектов и объектов, подвергаемых атакам. Эти участники преступного поведения используют зачастую схожие программные средства, имеют сходные режимы их применения.

Боевые действия, к которым мы привыкли, меняют свое лицо, действующих агентов и саму логику. Помимо стандартных вооруженных конфликтов мы все чаще говорим о кибератаках, киберпреступности, кибершпионаже и кибертерроризме, информационной войне. Все эти процессы приводят к появлению новой терминологии: от гибридных и

асимметричных войн до сетецентричных операций и боевых действий вне условий войны. Такие причудливые определения пополняют новые военные доктрины различных стран.

Феномен сетецентрической войны и кибервойны – концепции, ставшие реальностью в XXI в. В оперативном искусстве и тактике за последние десятилетия произошли принципиальные перемены, которые требуют от государств радикального пересмотра прежних военных доктрин и критической переоценки всего спектра областей военного искусства. По сути дела, сегодня речь идет уже о появлении нового военного искусства, когда прежние оценки, опыт и знания требуют радикального пересмотра либо даже отказа от прежних взглядов.

Период глобализации с переходом от промышленной к информационной эре затрагивает все страны, что определяет информацию не только как важную составляющую этого процесса, но и наиболее эффективное оружие. А так как преобладающим типом человеческого поведения в информационную эпоху является сетевое поведение, то, по мнению некоторых авторов, сетецентрическая война подходит этому времени как нельзя лучше. Согласно доктрине Пентагона, ядро такой войны находится на пересечении социальной, физической, информационной и когнитивной областей. Если информация еще связана с определенной инфраструктурой, то когнитивная сфера наименее материальна из всех четырех областей, потому что существует в сознании человека.

Эксперт по безопасности правительства США Ричард Кларк пишет в своей книге «Кибервойна» (2010): «Кибервойна – действия одного национального государства с проникновением в компьютеры или сети другого национального государства для достижения целей нанесения ущерба или разрушения». Британский журнал The Economist описывает киберпространство как «пятую область войны, после земли, моря, воздуха и космоса».

На данный момент существуют феномены информационной войны и сетецентрической и кибервойны. Кажется, что они похожи, но они разделяются по объектам и средствам боевого воздействия.

Информационные войны – это войны, имеющие своей целью изменение массового, группового и индивидуального сознания. В процессе информационных войн идет борьба за умы, ценности, установки, поведенческие паттерны и т. п. Информационные войны велись задолго до интернета, они имеют историю, измеряемую даже не сотнями, а тысячами лет. Интернет просто перевел эти войны на качественно иной уровень интенсивности, масштабности и эффективности. Что же касается сетецентрической и кибервойны, то они предполагают целенаправленное воздействие информационных потоков в виде программ-

ных кодов на материальные объекты и их системы с целью разрушения, нарушение функционирования или перехвата управления.

В идеальной форме агентами сетевой войны являются сети небольших разнотипных объединений, напоминающие ячейки, которые рассредоточены, но взаимосвязаны. Сеть должна быть аморфной – без сердца и головы, хотя не все узлы сети должны быть эквивалентны друг другу. По мнению некоторых специалистов, наилучшая тактика ведения боя в прямом и переносном смысле – роение. Подобно рою пчел, группы лиц, объединенные общей идеей, синхронно начинают атаковать цель, будь то государство или транснациональная корпорация. Превосходящая по силе и потенциалу своих противников цель, тем не менее, вынуждена реагировать на каждый мельчайший «укус», а если атакующие обладают определенной техникой и искушены в конфликте, то исход практически предрешен. Эта тактика напоминает «волчью стаю» подводных лодок Германии времен Второй мировой воины.

Реальное существование киберугроз кибертерроризма, сетецентрической и кибервойны требуют от государств радикального пересмотра прежних доктрин кибербезопасности и критической переоценки информационных систем, обеспечивающих деятельность объектов критической инфраструктуры (предприятия топливно-энергетического комплекса, энергораспределяющих сетей, систем контроля и управления наземным, морским и в особенности воздушным трафиком), так как в случае поражения программными средствами они могут представлять угрозу национальной и международной безопасности.

Органы государственной власти и местного самоуправления подчас подвергаются еще большему воздействию киберпреступников и кибертеррористов, организующих шпионаж, хищение данных из государственных или частных стратегических информационных систем и/или препятствующих нормальной работе. Одна из первых подобных кибервойн произошла в апреле 2007 г., когда в связи с решением эстонского правительства о переносе памятника Воину-освободителю сайты государственных структур страны подверглись организованным атакам.

Крайне болезненным этот удар стал из-за наличия в Эстонии развитой системы так называемого электронного государства, к которой активно стремятся перейти не только европейские, но и ведущие азиатские страны.

В июне 2010 г. жертвой кибератаки стал Иран: когда в компьютерную сеть исследовательского ядерного центра в Натанзе был занесен компьютерный вирус Stuxnet, пострадали более 60 тыс. компьютеров. В марте 2013 г. были взломаны компьютерные сети ряда крупных банков Южной Кореи – Shinhan Bank, Woori Bank и Nonghyup Bank, а

также многих телерадиокомпаний – KBS, YTN и MBC, в общей сложности было затронуто более 30 тыс. компьютеров. Это была наиболее мощная кибератака в истории Южной Кореи.

С 2013 г. власти США и другие международные агенты официально считают именно кибератаки угрозой номер один (ранее эту позицию занимал международный терроризм).

В силу разного рода причин все труднее становится отделить военную кибербезопасность одного государства, региона от военной кибербезопасности других государств, что неизбежно ведет к региональной военно-политической интеграции. Угроза государству может исходить, как и повод для атаки, из того, что оно вследствие политического конфликта принадлежит к другому военному блоку, экономическо-политическому союзу. Создание блоков и военно-политических союзов и нахождение государства в сфере военного или экономическо-политического влияния представляет собой естественную политико-экономическую закономерность. На данный момент все развитые страны и некоторые другие создали и развивают кибервойска, расходуя многомиллионные, миллиардные средства в этом направлении, которые могли бы быть использованы в научных, учебных и других целях.

Существующая ситуация представляет возможность нам считать, что наилучший результат в борьбе против киберугроз дает развитие сотрудничества на национальном, региональном и международном уровне. Что-то можно реализовать на данном этапе, а что-то в перспективе.

На национальном уровне считаем необходимым предпринять следующие меры:

приступить к разработке международной стратегии противодействия киберугрозам, создавав единые международно-правовые механизмы регулирования виртуального пространства;

разработать и внедрить концепцию национальной стратегии кибербезопасности, которая должна основываться на законах, предусматривающих ее реализацию в различных сферах и направлениях.

На международном уровне необходимо разработать и внедрить соглашение по предотвращению и расследованию киберагрессии – киберкодекс.

Наибольшего продвижения на пути к созданию международного киберкодекса удалось добиться летом 2015 г., когда группа правительственных экспертов ООН по международной информационной безопасности (в нее входят представители 20 стран, включая Россию, США и Китай) сформировала основу глобального пакта об электронном ненападении. В соответствии с достигнутыми договоренностями государства приняли обязательство использовать кибертехнологии исключительно

в мирных целях. Предполагается, что атакам не будут подвергнуты объекты критически важной инфраструктуры друг друга (банки, АЭС, системы управления транспортом и т. п.), перестанут вставляться вредоносные «закладки» (вредоносный софт) в производимую IT-продукцию, государства воздержатся от необоснованного обвинения друг друга в кибератаках и начнут прилагать усилия в борьбе с хакерами, осуществляющими компьютерные диверсии как с их территорий, так и через них.

Теоретически меры предусмотрены хорошие, но в случае реального физического конфликта, сопряженного с использованием информационных методов войны, маловероятно, что всего этого будут придерживаться, так как главное правило войны – любые средства хороши в борьбе для победы над противником.

Проблема современного мира заключается в существовании двойных стандартов, в разделении по региональному, экономическому, политическому, религиозному, идеологическому критериям.

Действующие агенты так и не осознали, что мир принадлежит не нам, а следующим поколениям, что человечество – это единая цивилизация и процветание, что развитие этой цивилизации невозможно, пока идет противоборство на международном и региональном уровне за превосходство и контроль в политической, военной, экономической сфере.

Наша цивилизация имеет шанс выжить и возможность процветать, если предотвратить феномены войн, в том числе сетецентрической и кибервойны, если изменить мировые векторы: план противоборства «кто сильнее» на вектор «как сделать вместе», план «кто больше» на «как лучше», план «все лучшее и большее для себя» на «как нужно и как рациональнее для всех теперь и что наименее важно для будущих поколений».

Действующие мировые агенты напоминают подростков, которые стараются показать себя и стать сильнее, богаче, умнее, нередко за счет других. Предложенные изменения векторов мировой политики касаются и принятия мер в направлении структурного изменения, повышения ответственности, авторитета международных институтов ООН, в экономическом направлении – ВТО, идеологическом и т. д.

Для преодоления и минимализации противоборства нужно в корне изменить существующие международные и региональные структуры и механизмы, элементы мирового законодательства.

Начать надо с создания нового международного института, который не имел бы привилегированных и постоянных членов с правом вето. Необходимо видоизменить формат института и состав его членов, определить месторасположение международного института на нейтраль-

ной для всех территории, придать полномочиям, распоряжениям и санкциям этой организации статус уровня международного правительства в политической, идеологической, и экономической сферах.

При любой проблеме нужно устранять не только последствия, но и причины ее порождающие.

УДК 004.9

Р.М. Юсупов, В.В. Бондуровский, М.А. Вус

ПРОЕКТ МОДЕЛЬНОГО ЗАКОНА ОДКБ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ»

Гармонизация национального законодательства по вопросам обороны, военного строительства и безопасности является одним из направлений уставной деятельности Организации Договора о коллективной безопасности (ОДКБ) и важнейшей задачей законотворческой деятельности Парламентской Ассамблеи ОДКБ (ПА ОДКБ). В рамках ОДКБ действует Соглашение о взаимной сохранности государственных секретов. Рекомендации по сближению национального законодательства по вопросам защиты государственной тайны стали одним из первых законодательных актов, принятых ПА ОДКБ.

Проект модельного закона ОДКБ «О государственной тайне» разрабатывается в соответствии с Программой деятельности ПА ОДКБ по сближению и гармонизации национального законодательства государств – членов ОДКБ на 2016–2020 гг. Головным разработчиком выступает Санкт-Петербургский институт информатики и автоматизации Российской академии наук в содружестве с Институтом национальной безопасности Республики Беларусь.

Первая рабочая версия законопроекта представлялась на Экспертно-консультативном совете при Совете ПА ОДКБ в ноябре 2016 г. По материалам работы вышел в свет ряд публикаций. Постоянная комиссия по вопросам обороны и безопасности ПА ОДКБ 20 апреля 2017 г. одобрила проведенную работу по разработке законопроекта и приняла решение направить проект модельного закона ОДКБ «О государственной тайне» в парламенты государств – членов ОДКБ для получения экспертных заключений.

Правовой институт тайны является одним из важнейших институтов и определяет: соотношение интересов личности, общества и государства, частного и публичного права; основания и пределы вмешательства государства в негосударственную сферу. Институт государственной тайны является предметом разрабатываемого для ОДКБ законопроекта. Разработчики законопроекта подчеркивают, что «государственная тайна» и «государственные секреты» – суть различные правовые категории.

В настоящее время правовая категория «государственная тайна» как объект защиты представлена в национальных законодательствах всех шести государств – членов ОДКБ; вместе с тем в тексты конституционных актов она включена только в Российской Федерации и в Республике Таджикистан (в Конституции Республики Казахстан упоминается более широкая категория «государственные секреты»).

Институт государственной тайны призван обеспечивать безопасность государства, он носит публично-правовой ограничительный характер – ограничивает основные конституционные права и свободы граждан. Целями закона о государственной тайне являются установление критериев отнесения к государственной тайне тех или иных сведений, установление критериев их засекречивания и рассекречивания, а также регулирование обращения таких сведений.

Разработчики модельного законопроекта исходят из постулата, что общественные отношения, связанные с защитой сведений, распространение которых может нанести ущерб безопасности государства, являются разновидностью конституционных правоотношений. Значимость конституционно-правовых отношений подразумевает более высокий уровень их регулирования, чем уровень регулирования обычными законами. Вследствие этого, как отмечают исследователи, логичном считается, что законодательство о государственной тайне объективно носит межотраслевой характер и вправе называться государственным (общеправовым), а не административно-правовым, хотя административное право и соответствующий административно-правовой режим играют наиболее заметную роль в регулировании обращения государственной тайны.

Представленный на заседании постоянной комиссии по вопросам обороны и безопасности ПА ОДКБ законопроект состоит из преамбулы и 7 разделов, включающих 31 статью. С учетом вышеотмеченного и в целях усиления системообразующей роли самого закона о государственной тайне и большей системности правового регулирования ее оборота предполагается необходимым придать национальным законам, разрабатываемым на основе модельного закона ОДКБ «О государственной тайне», статус конституционных. Это положение нашло отражение в преамбуле законопроекта.

В обсуждаемом законопроекте в сравнении с национальными законодательствами государств – членов ОДКБ расширен понятийный аппарат. В перечень используемых в законопроекте понятий дополнительно