1 Правове забезпечення захисту інформації. Проблеми розвитку нормативної та методичної баз системи захисту інформації

Владимир Хорошко, Михаил Шелест
Национальный Авиационный Университет
УДК 351.86:004.056

КИБЕРТЕРРОРИЗМ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Аннотация: **Представлені аспекти привабливості телекомунікаційних мереж для кібертероризму. Сформульовані і наведені негативні наслідки від кібертероризму через нерозвиненість правового регулювання, пропозиції щодо вдосконалення формування інформаційної інфраструктури України. Спрогнозовані тенденції засобів захисту.**
Summary: **Presented aspects of telecommunications networks for the attractiveness of cyberterrorism. And also formulated and presented: the negative effects of cyber-terrorism due to the underdeveloped legal regulation, to improve the formation of the information infrastructure of Ukraine and predicted trends remedies.**
Ключові слова: ***Інформація, інформаційна безпека, кібертерорізм.***

I Введение

Развитие человечества последовательно приводит к новым формам передачи и распространения информации, наиболее популярными из которых в настоящее время являются различные телекоммуникационные сети. Использование этих сетей в различных отраслях деятельности человечества естественно привлекает различного рода преступников.

При этом следует учитывать, что за последнее время различные аспекты безопасности в информационной сфере приобретает все большую актуальность. Связано это с несколькими обстоятельствами.

Индустрия информационных технологий – одна из наиболее стремительно развивающихся сфер мировой экономики, способная конкурировать по доходности с топливо – энергетическим комплексом и автомобилестроением. Она сделала рынок значительно более масштабным, динамичным и конкурентным, дала стимул к зарождению множества новых сфер бизнеса.

Информационные технологии по своей природе являются уникальным средством обработки, хранения и передачи информации с выходом на практически неограниченную аудиторию. Эта возможность позволяет: правительствам предоставлять гражданам услуги в рамках программ электронного правительства; организациям – информировать о своей деятельности, внедрять в производственные процессы и процессы выполнения различного вида работ, оказания услуг безбумажных технологий, переходить на методы электронной нумерации; банковским и финансовым учреждениям – оказывать услуги управления банковскими счетами через Интернет, осуществлять, задействовав информационные каналы, платежи в режиме реального времени; гражданам - участвовать в процессах принятия политических решений, эффективно искать и получать информацию, распространять результаты своего творческого труда, вступать в виртуальные сообщества в соответствии со своими интересами.

Информационные технологии изменяют принципы взаимодействия в обществе, поэтому неудивительно, что они также изменяют понятия преступности как таковые. Компьютеры, компьютерные сети, Интернет становятся основной частью бизнеса и социальной активности. Объем информации, доступной с помощью информационных технологий, привлекает преступников, и эта привлекательность будет только возрастать по мере того, как информационные технологии будут развиваться и приобретать новые формы.

Можно выделить следующие аспекты привлекательности телекоммуникационных сетей для кибертерроризма [1]:

- большинство серверов коммуникационных сетей позволяют пользователям работать относительно конфиденциально и анонимно;
- существует возможность использования специальных роботов (bots) для снижения времени затрат на террористическую деятельность;
- киберпреступления сложно отследить и собрать доказательства;
- пострадавшие замалчивают киберпреступления;
- меньший риск в сравнении с обычными видами преступлений и более высокая эффективность;
- возможность совершать киберпреступления через границы стран и континентов;

- не требует физического присутствия.

Неудивительно, что со временем формы преступности и терроризма перемещаются в область киберпространства и требуют глубокого изучения с целью эффективного противодействия.

Цель работы – анализ сегодняшнего состояния кибертерроризма и его влияния на региональную, национальную и международную информационную безопасность, а так же на пути и методы борьбы с ним.

II Основная часть

Проблемы информационной безопасности многогранны и требуют решения многих вопросов от обеспечения безопасности отдельного рабочего места до функционирования локальных и глобальных сетей.

Активизируется киберпреступность, которая в настоящее время рассматривается различными экспертами [1,2] как стремительно нарастающая угроза безопасности как отдельным государствам, так и для мирового сообщества в целом. Несмотря на усилия правоохранительных органов и спецслужб, направленные на борьбу с киберпреступностью и кибертерроризмом, число преступных актов с использованием информационных технологий не уменьшается, а, напротив, постоянно увеличивается и возрастает их общественная опасность.

Меняется и сам облик терроризма, о чем наглядно свидетельствует появление информационного терроризма. Информационные технологии уже освоены международными террористическими и экстремистскими организациями.

Информационные технологии представляют террористам возможность скрытно, планомерно и эффективно воздействовать на индивидуальное и массовое сознание, общественное мнение, процессы принятия решений; распространять информацию для вербовки в свои ряды новых членов, пропаганды своих идей; проводить дезинформацию; вызывать панику, а также непосредственно совершать террористические акты. Эти технологии позволяют террористическим группам, большинство из которых сейчас имеют сетевую структуру организации, эффективно и скрытно осуществлять взаимодействие между ее разрозненными ячейками и отдельными членами, а так же проводить сбор информации о будущих целях.

Рассмотрение состояния и развития информационных технологий и кибертерроризма позволяет прогнозировать будущее [3].

1. Наиболее реальными целями кибертерроризма будут персональные мобильные средства телекоммуникации, процесс совершенствования и развития которых в настоящее время чрезвычайно динамичен. Развитие телекоммуникационных систем, реализующих IP–телефонию и прочие голосовые сервисы неминуемо приведет к попыткам кибертеррористов реализовать уязвимость данного сервиса для реализации незаконного доступа.

2. Вредоносные коммуникационные соображения в настоящий момент являются бичом практически всех телекоммуникационных систем и согласно прогнозам объем этих преступлений в общем количестве кибертерроризма будет сохраняться. Однако многие аналитики уже в настоящее время рассматривают снижение роли электронной почты, как средства доставки вредного кода на компьютеры, и рассматривают реальную возможность создания более изощренных систем для реализации данных функций.

3. Использование беспроводных методов коммуникации уже сейчас привлекает значительное количество киберпреступников.

4. Привлекательность для кибертеррористов банковских систем будет в дальнейшем все более возрастать, а соответственно возрастать и использование уязвимостей, направленных на получение банковских и идентификационных параметров пользователей.

Одной из наиболее опасных угроз безопасности является все более широкое использование кибертероррористами (наряду с традиционными средствами совершения противоправных действий) возможностей открытых телекоммуникационных сетей для оказания пропагандирующего воздействия на мировую общественность и координации своей деятельности.

Следует учитывать, что сайты террористического характера, содержащие призывы к национальной и религиозной розни, призывающие к осуществлению актов терроризма и диверсий, регулярно выявляются в сети Интернет. На территории Украины безотлагательно принимаются меры к их закрытию, в результате чего в настоящее время факты появления таких сайтов в украинском сегменте сети Интернет носят единичный характер. Вместе с тем, особенность современного информационного пространства состоит в том, что распространение информации в нем не ограничено национальными границами. Сайты, пропагандирующие идеи терроризма, в том числе на русском и украинском языках, создаются и функционируют на территории иных стран. Поэтому особое значение в борьбе с пропагандирующей деятельностью террористических организаций в сети Интернет приобретает международное сотрудничество, обсуждаемое на уровне спецслужб и правоохранительных органов. В результате взаимодействия целого ряда

стран в настоящее время, прекращена деятельность многих сайтов террористической направленности, действующих в зарубежных сегментах сети Интернет.

Совершенно очевидно, что решение вопросов информационной безопасности требует комплексного подхода, включая вопросы правового, методического, научно- технического и организационного обеспечения информационной безопасности сетей, создание соответствующих структур и подготовку кадров [4].

Кроме того, существует значительное число проблем в противодействии киберпреступности. В стороне от числа технических, правовых и финансовых аспектов определяющих защиту информационного пространства и инфраструктуры, существует также различное количество неурегулированных элементов между коммерческими структурами и государственными организациями относительно того, какие компоненты информационного пространства и инфраструктуры требуют защиты и методы действий по отношению к кибертеррористам. Эти процессы возникают у бизнеса, основными целями которого являются предупреждение и отражение атак, в отличии от государственных структур, целями которого является обнаружить, нейтрализовать и захватить кибертеррористов. Это вызывает различные концепции ответственности, распространения информации и уязвимости в национальном информационном пространстве. Другая проблема состоит в постепенном переходе контроля над элементами критической инфраструктуры от государства к коммерческим организациям, что, как следствие, ограничивает возможности обеспечения защиты данных элементов.

Транснациональность угроз информационному пространству и уровень ущерба при их реализации заставляет ставить проблему обеспечения информационной безопасности как глобальную, требующею усилий всего мирового сообщества.

Одним из основных рычагов государственного регулирования прав доступа к объектам, имеющим национальное значение, является наличие соответствующего правового обеспечения процесса информационного взаимодействия. Однако противоречивость и неразвитость правового регулирования общественных отношений в информационном пространстве приводит к серьезным негативным последствиям:

- не обеспечивается эффективная реализация и защита конституционных прав личности и неприкосновенность частной жизни, личной и семейной тайны, защиту чести и достоинства личности;
- слабо реализуется возможность как конституционных ограничений свободы массовой информации в интересах защиты конституционного строя, нравственности, здоровья, прав и законных интересов граждан, обеспечение обороноспособности страны и безопасности государства;
- не обеспечена защита прав участников электронной коммерции, они работают на свой страх и риск, особенно велик этот риск у покупателей;
- отсутствуют правовые механизмы противодействия манипулированию информацией, что проявляется с одной стороны, в невозможности легко проверить достоверность представленной информации, а с другой стороны, в распространении средств и методов манипулирования информацией, особенно в рамках избирательных компаний;
- увеличить масштабы нарушения прав интеллектуальной собственности, что связано с развитием Интернета, сложностью контроля за использованием в сети объектов интеллектуальной собственности, распространением электронным библиотек, деятельность которых не регулируется;
- отсутствует защита интересов государств и общества в сфере использования государственных информационных ресурсов, не определены принципы отнесения информационных ресурсов к государственному и национальному достоянию, не обеспечен беспрепятственный доступ к государственным ресурсам и порядок их создания, развития и поддержания.

Учитывая цели и приоритеты по вопросам информационного общества представляется целесообразным сформулировать и рассматривать следующие предложения по совершенствованию формирования информационной инфраструктуры в Украины с целью поддержки вопросов национальной безопасности [4, 5]:

1. Разработать и принять, после публичного обсуждения, государственную информационную политику, предусматривающую в том числе, комплексное, взаимосвязанное развитие законодательства в сфере информационной безопасности.
2. В целях повышения законодательного регулирования обеспечить пакетный принцип подготовки законопроектов и внесения их в законодательные органы власти с тем, чтобы к моменту принятия и утверждения законов были готовы проекты всех нормативных актов, необходимых для их применения. Причем, особое внимание уделяется законопроектам, отражающим вопросы национальной безопасности, как наиболее важным для Украины.

3. Рассмотреть возможность создания вневедомственного научно-исследовательского центра с функциями:

- координация законопроектной деятельности в данной сфере;
- экспертизы законопроектов;
- анализ правоприменения;
- сравнительного анализа национального законодательства и законодательства зарубежных стран;
- выработки предложений по актуальным направлениям совершенствования законодательства.

4. Определить приоритеты в законодательной работе.

Это прежде всего законопроекты, направленные на:

- правовую защиту персональных данных;
- обеспечение доступа к информации органов государственной власти;
- защиту конфиденциальной информации;
- правовую регламентацию электронного документооборота, включая электронную торговлю и распознавание электронных подписей.

Наряду с разработкой новых законов необходимо вносить изменения в национальные законы в целях адаптации традиционных правовых механизмов регулирования различных правоотношений к реалиям информационного общества.

Существует целый ряд проблем повышения безопасности информационной сферы, включая телекоммуникационные сети, противодействия угрозам информационной безопасности.

Особое внимание требуют проблемы подключения к глобальным сетям и, в первую очередь, Интернет.

Этот процесс следует рассматривать через призму информационной безопасности. Политика исключения информационных ресурсов Интернет, будучи открытой, должна в обязательном порядке предусматривать защиту сетевого оборудования от возможных атак и воздействий как внутренних, так и внешних [5, 6].

Трудно оценить ущерб в случае, если выводятся из строя стратегически важные сегменты информационной инфраструктуры государства, учитывая, что в современных коммуникационных и управляющих системах, а также во вспомогательных средствах, которыми оснащаются узлы связи и управляющие структуры организаций связи, основными компонентами которых являются микропроцессорные системы с поддерживающим программным обеспечением. При этом, особую значимость для объектов связи приобретает возможность предупреждения опасного воздействия или вирусной атаки на них.

Как показывают последние события, все чаще массированные атаки «хакеров» используются с цель блокирования и взлома Интернет сетей. Это вызывает повышенное беспокойство по поводу уязвимости от «компьютерной атаки» на системы жизнеобеспечения, закрытые источники информации, как со стороны злоумышленников-одиночек, так и кибертеррористов.

В связи с этим, следует особо подчеркнуть, что противоборство с кибертеррористами приобретает новые формы, перемещаясь все более в сферу информационных технологий и Интернета. Причем, развитие государств, деятельность которых строится на современных инфокоммуникационных и информационных технологиях, легко может стать жертвой «массированного информационного удара», способно сразу и резко дестабилизировать ситуацию в государстве. Поэтому проблеме защиты в развитых странах придается большое значение [7].

Исходя из всего вышесказанного, можно спрогнозировать следующие тенденции развития средств защиты от кибертерроризма.

1. Совершенствования сетевого оборудования - защитных сервисных коммутаторов, с помощью которых появляется возможность оказывать корпоративным абонентам широкий спектр услуг по обеспечению безопасности информационной сферы.
2. Формирование рынка услуг по защищенной доставке цифрового контента и рынка технологий такой доставки
3. Возрастание объема рынка управляемых услуг безопасности; при этом лидирующие положения на нем займут провайдеры, учитывающие интересы электронного бизнеса.
4. Формирование нового рынка услуг удаленной «точечной» сетевой защиты в рамках виртуальных частных сетей на основе IP-технологий. Его участники будут обеспечивать защиту удаленных объектов, которые используют для работы в Интернет.
5. Увеличение объемов рынка интеллектуальных услуг сетевой защиты по мере того, как его участники будут использовать предупреждающий процесс управления безопасностью, предоставляя пользователям возможность защититься от хакеров.

6. Интеграция систем управления безопасностью с платформами для управления сетями и расширение применения биометрических систем аутентификации для повышения достоверности электронных документов и придания им юридической силы.

7. Возрастет спрос на консалтинговые услуги в части подготовки концепций информационной безопасности, проектирование информационных систем с учетом требования защиты, построение систем управления информационной безопасностью.

Кроме того, проблему информационной безопасности обостряет фундаментальная зависимость украинской информационной сферы от зарубежных компьютерных средств, телекоммуникационного оборудования, запасных частей и комплектующих, используемые при его ремонте и обслуживании. Особенно следует учитывать, что зарубежное программное обеспечение широко используется на стратегических объектах и принимая во внимание реальные прецеденты закладки недокументированных программных модулей для осуществления вмешательства в работу программного обеспечения.

Эти негативные последствия представляют серьезную угрозу национальной и международной безопасности. Они стали важным фактором, непосредственно влияющим на формирование международных отношений и приобретают особую остроту в связи со значительным ростом международного кибертерроризма.

Опасный характер со стороны кибертеррористов информационной безопасности делает противодействие им принципиальным аспектом укрепления региональной, национальной и международной безопасности и стратегической стабильности, а вследствие этого – отдельным направлением внутренней и внешнеполитической деятельности всех государств, стремящихся интегрироваться в глобальное информационное общество.

III Выводы

Для решения всех перечисленных проблем принципиально важно исходить из следующего.

1. Вопросы регулирования терроризма в сфере информационного пространства в полной мере не попадают под действие ни одного из существующих на сегодня международных политико-правовых документов. Подход, предусматривающий многоаспектное и всестороннее обеспечение информационной безопасности на региональном, национальном и глобальном уровнях в привязке к кибертеррористическому характеру отсутствует.

2. Существующие многосторонние механизмы, направленные на обеспечение информационной безопасности, недостаточны для эффективного решения вопросов информационной безопасности, адекватных угрозам кибертерроризма в этой сфере.

3. Эффективность противодействия угрозам кибертерроризма в информационной сфере возможно за счет координации и прогрессивного развития соответствующих норм международного права для обеспечение эффективного регулирования отношений, возникающих в информационном пространстве, на базе продолжения консультативного и переговорного процессов на двухстороннем, региональном, национальном и международном уровнях, в том числе путем выработки и принятия многостороннего договора о борьбе с информационном терроризмом, а в перспективе – юридически обязательного международного договора, регулирующего отношения в области международной информационной безопасности.

4. Предпринимаются необходимые усилия на международном уровне в направлении снижения угроз от кибертерроризма национальной безопасности, которые имеют внешний характер и могут исходить как от террористов, так и от отдельных государств. При этом крайне важно вести работу внутри страны по укреплению национальной безопасности на национальном уровне.

Список использованной литературы: ***1.*** *Ільяшов О. А. Кіберзлочинність – як одна з найбільших загроз сучасності: прояви і тенденції її поширення, можливі заходи протидії / Ільяшов О. А., Бурячок В. Л. // Труди університету «Інформаційна боротьба: проблеми та шляхи їх вирішення, Вип.2 (101), 2011. – С. 129-131.* ***2.*** *Голубенко А. Л. Информационные технологии и киберпреступность / Голубенко А. Л., Хорошко В. А., Петров А. С., Белозеров Е. В. // Вісник СНУ ім. В. Даля, №4 (110), 2006, ч.1. – С. 7-10.* ***3.*** *Голубенко А. Л. Основные проблемы национальной безопасности в области информационных технологий / Голубенко А. Л., Петров А. С., Хорошко В. А., Белозеров Е. В. // Вісник СНУ ім. В. Даля, №5 (111), 2007, ч. 1. – С. 7-13.* ***4.*** *Дорошко В. А. Информационная безопасность Украины, основные проблемы и перспективы / Хорошко В.А. // Захист інформації, спецвипуск, 2008. – С. 6-10.* ***5.*** *Бурячок В. Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / Бурячок В. Л. // Сучасна спеціальна техніка, Вип. №3 (26), 2011. – С. 104-114.* ***6.*** *Голубенко А. Л. Информационное противодействие в*

компьютерных сетях / Голубенко А. Л., Петров А. С., Хорошко В. А. // Вісник СНУ ім. В. Даля, №15 (204), 2013, ч. 1. – С. 9-14. **7.** *Бурячок В. Л. Основи формування державної системи кібернетичної безпеки / Бурячок В.Л. – К.: Вид. НАУ, 2013. – 432 с.*

Сергій Довбня, Андрій Нікірін, Іван Четверіков
Київський Національний університет імені Тараса Шевченка

УДК 621.321

СТВОРЕННЯ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ МАТРИЦ НЕБЕЗПЕЧНИХ ФАКТОРІВ, ЩО ХАРАКТЕРИЗУЮТЬ ТЕХНІЧНІ КАНАЛИ ВИТОКУ

Анотація: **Наведено формальний опис технічних каналів витоку інформації та завдання створення системи технічного захисту інформації. Наведено метод рішення завдання створення системи захисту інформації.**
Summary: **A formal specification over of technical channels of source of information and task of creation of the system of technical defence of information is brought. A method over of decision of task of creation of the system of defence of information is brought.**
Ключові слова: **Технічній канал витоку інформації, технічні засоби розвідки, система технічного захисту.**

Вступ

Забезпечення захисту інформації спрямовується зокрема на те, щоб не допустити збитків від утрати конфіденційної інформації. Відповідно до цього, уже передбачається наявність цінної інформації, в разі втрати якої можуть бути понесені збитки. А якщо є цінна інформація, то звичайно ж є можливість здійснення будь-яких дій, які можуть нанести шкоду цій інформації. Усі шкідливі дії можуть бути здійснені тільки за наявності будь-яких слабких місць (уразливостей) (див. рис. 1).

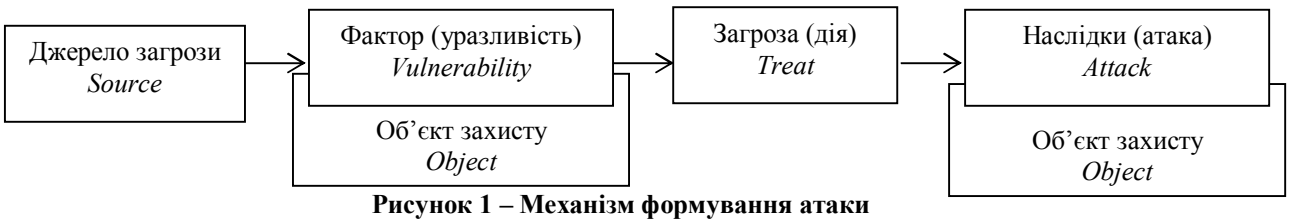

Рисунок 1 – Механізм формування атаки

А якщо є дії, то є найвища загроза їх здійснення, а також наявні джерела, з яких ці загрози можуть виходити.

Виникає наступний ланцюжок: джерело загрози – фактор (уразливість) – загроза (дія) – наслідки (атака).

Джерело загрози – це потенційні антропогенні, техногенні або стихійні носії загрози безпеці.

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке наносить збиток власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації.

Фактор (уразливість) – це властиві об'єкту інформатизації причини, які призводять до порушення безпеки інформації на конкретному об'єкті та зумовлені вадами процесу функціонування об'єкта інформатизації, властивостями архітектури інформаційно-телекомунікаційної системи, протоколами обміну та інтерфейсами, що застосовуються, програмним забезпеченням і апаратними засобами, умовами експлуатації.

Наслідки (атака) – це завжди пара "джерело-фактор", що реалізує загрозу та приводить до збитків.

Слід зазначити, що захист інформації відповідно до рекомендацій нормативних документів здійснюється за двома основними напрями: захист інформації від її витоку технічними каналами, що виникають в процесі її обробки, і захист інформації від несанкціонованого до неї доступу. У даній публікації мова піде про захист інформації від витоку її технічними каналами. При цьому під технічним каналом витоку інформації розуміється канал витоку інформації, несанкціоноване перенесення інформації в якому від джерела до зловмисника здійснюється з використанням технічних засобів. Основною класифікаційною ознакою технічного каналу витоку інформації є фізична природа носія інформації. За цією ознакою вони поділяються на оптичні, радіоелектронні, акустичні, матеріально-речові.