МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В ТЕОРИИ УПРАВЛЕНИЯ СЛОЖНЫХ ПРОЦЕССОВ

СОВЕРШЕНСТВОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ УПРАВЛЕНИЯ МЧС РОССИИ В СОВРЕМЕННЫХ УСЛОВИЯХ

О.Н. Савчук, кандидат технических наук, профессор,
заслуженный работник высшей школы Российской Федерации;
В.П. Крейтор, кандидат технических наук, профессор.
Санкт-Петербургский университет ГПС МЧС России

Рассматриваются вопросы информационной безопасности в условиях информационной войны и кибертерроризма, а также виды информационного оружия, которые могут воздействовать на системы управления органов МЧС России. Приводятся методы и способы обеспечения безопасности систем Центра управления в кризисных ситуациях МЧС России.

Ключевые слова: информационная безопасность, информационное оружие, электромагнитный терроризм, «логическая бомба»

PERFECTION OF INFORMATIVE SAFETY OF ORGANS OF MANAGEMENT MINISTRY OF EMERGENCY MEASURES OF RUSSIA IS IN MODERN TERMS

O.N. Savchuk; V.P. Kreytor.
Saint-Petersburg university of State fire service of EMERCOM of Russia

The article discusses the issues of information security in conditions of information war and cyberterrorism, as well as the types of information weapons, which can influence the systems of management bodies of EMERCOM of Russia. The methods and ways of safety systems Center for Crisis Management EMERCOM of Russia of EMERCOM of Russia.

Keywords: information security, information weapons, electromagnetic terrorism, «a logic bomb»

Анализ современной международной обстановки показывает, что США и ведущие европейские страны в основном делают ставку на применение военной силы при разрешении международных конфликтов. Эти страны, обладая военным превосходством, прежде всего, в развитии высокоточных, информационных и других высокотехнологичных средств ведения вооруженной борьбы, вмешиваются во внутриполитические конфликты более слабых государств, навязывая им свое мироустройство [1]. Особенно наглядно это проявилось при применении военной силы США в Ираке, Афганистане, сил НАТО в Югославии, Ливии, Сирии. В представленном Центром стратегических исследований гражданской защиты МЧС России ранжированном перечне стратегических рисков для устойчивого развития России военная угроза со стороны США и НАТО путем

возникновения региональных и локальных конфликтов занимает довольно высокое место по относительной значимости сферы 0,84.

В современных условиях развязывания вооруженных конфликтов одно из приоритетных направлений принимают нетрадиционные войны и, в том числе, информационная война. В настоящее время против России развязана широкомасштабная информационная война США и странами НАТО. Неслучайно недавно было принято решение о создании в рамках Вооруженных Сил Российской Федерации информационных войск.

В связи с этим в России с внедрением информационных систем возникают проблемы, связанные с надежным обеспечением работы элементов информационной инфраструктуры и сохранения достоверной информации.

Элементы ведения информационной войны использовались в русско-японской войне 1904 г., когда радиосвязь была нарушена с помощью радиопомех. В последующем значительное развитие получила информационная война с появлением радиоэлектронных средств. Во время войн в Корее и на Ближнем Востоке уже применялись радиопомехи, направленные на срыв радиосвязи противника, внесение дезорганизации оперативного управления войсками, нарушение работы систем противовоздушной обороны (ПВО) путем радиоподавления.

Например, в арабо-израильской войне 6 июня 1967 г. путем нарушения работы радиосети арабских войск было сорвано наступление четвертой танковой дивизии Египта. Применение информационных технологий вторжения в программу управления работой центрифуг со стороны США и Израиля была сорвана иранская программа реализации получения «ружейного плутония».

США и развитые страны с конца XX в. выделяют значительные суммы на совершенствование информационного оружия, способов его применения [2–4]. Только за последние 15 лет США увеличили в четыре раза расходы на покупку и создание новых средств информационной борьбы. С приходом президента Трампа в Белый дом военный бюджет США в 2017 г. увеличится на 10 % больше, чем в предыдущем году. В военных академиях США продолжается подготовка специалистов в области использования информационного оружия, создаются специальные центры и подразделения для проведения операций информационной войны.

Таким образом, информационная война – это такой вид войны, в которой происходят различные формы атак на информационные системы для воздействия на сознание людей или нарушения работы этих систем в органах управления противника.

По мнению американских военных экспертов [5, 6], информационная война состоит из действий, направленных на поражение информационных и компьютерных систем противника с обеспечением своей информационной безопасности.

В России уже появился ряд правовых документов, рассматривающих обеспечение информационной национальной безопасности. Так, в «Концепции национальной безопасности Российской Федерации» четко определены информационные опасности. В «Доктрине информационной безопасности Российской Федерации» [7] указаны причины, по которым информационная структура России, уязвима.

Совершенствование компьютерной и информационной технологий и создание единого информационного пространства способствуют совершенствованию и применению информационного оружия, которое предназначено, прежде всего, для вывода из строя компьютерных систем управления.

Информационное противоборство реализуется проведением мероприятий, которые наносят ущерб системам управления и принятию правильных решений, а также компьютерным и информационным сетям и системам. Основными элементами информационной войны являются [8, 9]:

– электронная война, цель которой затруднить получение противнику достоверной информации;

– дезинформация, цель которой предоставление противнику ложной информации;

– физическое разрушение, цель которого воздействие на элементы информационных систем и нарушение их работоспособности;

– прямые информационные атаки, цель которых искажение информации без видимого изменения ее сущности. Все это реализуется с помощью информационного оружия.

Информационное оружие – это такое сочетание программных и технических средств, которое способно контролировать, вмешиваться и воздействовать на работу информационных систем объекта.

Применение информационного оружия в информационных и телекоммуникационных системах носит скрытый характер и не сопровождается с объявлением войны или введением периода особых действий в локальных конфликтах. Наиболее уязвимыми для нападения являются те системы, которые должны сохранять непрерывную работоспособность в реальном масштабе времени.

В настоящее время в США завершено создание и принятие на вооружение ряда систем информационного оружия (ИНФОР) [10], которые по своему назначению и сферам воздействия подразделяются на следующие виды:

– ИНФОР-1 нарушает и выводит из строя информационные системы органов управления государственной службы, вооруженных сил, промышленных, транспортных, энергетических объектов, элементов связи и других объектов;

– ИНФОР-2 воздействует на психику людей, что позволяет манипулировать их поведением;

– ИНФОР-3 – это будет создано новое более эффективное и разрушительное оружие данного класса, которое пока держится в секрете. Информационное оружие по методам воздействия классифицируется как физическое, информационное, программно-техническое или радиоэлектронное [8].

Выход из строя компьютерных систем будет происходить путем применения информационного оружия физического воздействия: специализированных аккумуляторных батарей генерации электромагнитных импульсов, биологических и химических средств, уничтожающих электронные схемы, и программно-технического воздействия: компьютерные вирусы, «черви», логические бомбы.

Примером такого вида оружия может служить сверхвысокочастотное оружие (СВЧ-оружие), способное создавать направленный электромагнитный импульс, которое США впервые применило в Ираке в 2003 г. Применение его парализовало работу информационно-управляющей системы страны. Одним из представителей такого оружия является устройство типа MPS2, состоящее на вооружении США, которое снабжено антенной диаметром 3 м (мощность в импульсном режиме 1 ГВт, функциональное значение напряжения 265 кВ, величина тока 3,5 кА) [2]. Системой радиоэлектронной борьбы (РЭБ) «Хибины», установленной на бомбардировщике СУ-34, была выведена из строя информационно-управляющая система «Иджис» на военном корабле США «Дональд Кук» 12 апреля 2014 г., который приблизился к границе России в Черном море, что вызвало панику среди личного состава и привело к тому, что он покинул акваторию Черного моря. По оценкам специалистов потенциально уязвимы от СВЧ-оружия все компьютеры, используемые в системах обработки данных и отображения информации, системах промышленного контроля, включая управление всеми видами транспорта и электроснабжением [4].

Разрушающее воздействие на радиоэлектронное оборудование с использованием мощного источника электромагнитных излучений возможно по сетям электроснабжения нарушения работы управления объектов энергетики [2], а также по проводным линиям с использованием слаботочного сигнала [3], по эфиру с использованием электромагнитных импульсов малой длительности [6].

Воздействие по проводным линиям для передачи слаботочного сигнала [3] приводит к изменению параметров полупроводниковых приборов, микросхем запоминающих

устройств, интегральных схем с МОП-структурами (энергия импульса 1–100 мкдж, длительность импульса 10–1000 нс).

Наибольшую опасность представляет информационное оружие, воздействующее по эфиру на радиоэлектронное оборудование с использованием импульсов малой длительности [6].

Так, например, по оценкам западных специалистов, вероятность восстановления нарушенных функций компьютерных систем раннего предупреждения о ракетном нападении, систем противоракетной обороны будет довольно низкая. Последствия могут быть сопоставимы с последствиями применения оружия массового поражения.

Основными способами применения информационного оружия в этих целях являются:

– вывод из строя информационной инфраструктуры путем создания помех, использованием специальных программ, выводящих из строя аппаратные средства, применения биологических и химических средств поражения; внедрение вирусов и логических бомб, способных уничтожить или повредить информацию, программные и технические ресурсы противника, расстроить системы информационной защиты;

– способы воздействия с целью искажения программного обеспечения и базы данных компьютерных систем и систем управления;

– проведение информационно-террористических актов;

– воздействие на компьютерные системы с целью их искусственной перегрузки;

– воздействие на компьютерные системы с целью полного вывода их из строя.

Примером физического воздействия на компьютерное оборудование с целью выхода его из строя является применение современного лазерного оружия (отечественного комплекса «Гранит») по одному американскому космическому челноку «Шаттл», который летал над территорией страны, несмотря на протесты с нашей стороны. Тогда было принято решение произвести небольшое профилактическое воздействие по челноку из комплекса «Гранит» с помощью лазера и мазера (луч в радиочастотном диапазоне), такой интенсивности, чтобы не было жертв. Воздействие этих лучей приводит к выходу из строя радиоэлектронного оборудования противника на большом расстоянии и влияет на психику человека. В результате такого воздействия экипаж «Шаттла» в течение получаса потерял сознание, а почти вся радиоэлектронная аппаратура вышла из строя. Экипажу пришлось приземляться экстренно, используя ручное управление. После этого ни один челнок над территорией СССР не пролетал.

Кроме того, с помощью использования мультимедийных и программных средств возможно воздействие информации на сознание операторов, что приводит к расстройству их психического состояния или ухудшению здоровья, что скажется на принятии ими правильных решений при обработке информации. Так, например, «Вирус N-666» вызывает на экране цветовую комбинацию, что может привести оператора компьютерной системы в гипнотический транс и вызвать у него изменение функционирования сердечно-сосудистой системы, в частности сосудов головного мозга.

К средствам искажения и уничтожения информации компьютеров относятся вирусы, общее количество которых превышает 60 000 [4, 11]. Наиболее известными из них являются «троянский конь» («Trojan Horse») и «Червь» («Worm»). Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер, затрагивающие автоматизированную обработку данных или передачу данных. Это может привести к замедлению выполнения отдельных функций программ или к стиранию файлов и уничтожению программного обеспечения. Так, например, «троянский конь» активизируется по команде и может изменить или полностью разрушить информацию, а также снизить быстродействие информационной системы. «Червь» – это файл, образованный внутри базы данных компьютерных системы. Он способен сокращать ресурсы памяти, перемещать и искажать информацию.

К элементам информационного оружия, воздействующих на информационную инфраструктуру, следует отнести «логические бомбы», «бомбы электронной почты» и т.д.

«Логическая бомба» представляет скрытую внедренную программу в компьютерную систему, запускаемую ее кодовым сигналом, которая изменяет или полностью разрушает информацию. Примером ее воздействия может служить выход из строя системы ПВО Ирака во время вооруженного конфликта в Персидском заливе. Программное обеспечение систем ПВО, закупленное во Франции, содержало «логические бомбы», которые были задействованы с началом боевых действий. США добились выхода из строя системы ПВО путем активации микросхем-вредителей [10].

«Бомбы электронной почты» представляют большой объем информационных сообщений, поступление которых приводят к увеличению нагрузки на сервер, после чего он становится недоступным или его ресурсы не позволяют использовать его для нормальной работы [10].

В ходе информационной войны возможна подделка выходной информации при обработке исходных данных. Это достигается путем ввода в программу компьютера фальшивых данных при использовании сложных математических моделей.

Разработка систем информационной безопасности в настоящее время отстает, по мнению экспертов, от развития средств информационного оружия. Следует отметить, что весь компьютерный мир находится в зависимости от американской компании Билла Гейтса, чьей операционной системой пользуются 97 % обладателей персональных компьютеров. По оценкам специалистов ФСБ России «ни в одной стране в средствах связи нет такой высокой доли импортного оборудования с возможными «электронными закладками», как у нас». По их мнению, до 70 % сетей общего пользования России заражены «электронными закладками» обратной связи, которые могут быть задействованы по сигналу со спутника и вывести систему из строя.

Так, например, на американском мощном компьютере, установленном в г. Жуковский, на одном из промышленных оборонных объектов авиационного комплекса, произошел «сбой», приведший к аварии, связанный с внезапным выходом из строя такого компьютера. В Институте ядерной физики Сибирского филиала Российской академии наук и Институте им. Курчатова в Москве были зафиксированы факты передачи секретной информации через интернет в зарубежные страны.

Выявление последствий чрезвычайных ситуаций (ЧС) является одним из основных мероприятий защиты населения. Выявление последствий ЧС осуществляется с целью обеспечения органов управления Единой государственной системы предупреждения и ликвидации чрезвычайных ситуаций на всех уровнях информацией о масштабах последствий ЧС и вариантах действий личного состава сил, привлекаемых к ликвидации последствий, населения, персонала объектов экономики в очагах (зонах) поражения (заражения), при которых исключаются или снижаются до минимума возможные потери. От достоверности данных прогнозирования по возможным масштабам и последствиям зависит своевременное и наиболее адекватное принятие решения по обеспечению защиты населения и территорий (объектов экономики).

Масштабное применение информационного оружия может вывести из строя вычислительные комплексы в системе управления МЧС России, в том числе в подсистемах мониторинга и прогнозирования Центра управления в кризисных ситуациях субъектов Российской Федерации, что скажется отрицательно на принятии оперативных решений по возникающим ЧС.

В мирное время в условиях разгула терроризма возможно проявление его в виде электромагнитного терроризма [11]. Это может привести к росту техногенных катастроф.

Одним из направлений обеспечения информационной безопасности является информационно-техническое, которое отвечает за состояние защищенности информационно-технических систем. Методами обеспечения информационной безопасности, как правило, являются правовые, организационные и технические [12].

К правовым методам [12] относят разработку документов, устанавливающих наказания за преступления в информационной сфере, совершенствование законов

по обеспечению информационной безопасности, ратификацию международных договоров в этой области.

К организационным методам [12] относят: меры по охране информационных систем; разработку планов восстановления работоспособности информационных систем на период выхода их из строя; совершенствование организации сервиса информационных систем; разработку средств защиты информационных систем и т.д.

К техническим методам [12] относят: совершенствование защиты от несанкционированного входа в компьютерную систему с помощью кодовых сигналов; повышение надежности информационной безопасности путем резервирования компьютерных подсистем, источников электропитания; перераспределение ресурсов в компьютерных сетях, когда выходят из строя отдельные ее подсистемы; совершенствование конструктивной и физической защиты от диверсий, взрывов.

Одним из элементов усиления информационно-технической безопасности в случае информационной войны является применение способов и методов прогнозирования ЧС и на этой основе принятия оперативных решений по ликвидации последствий, базирующихся на использовании простейших методик, графиков, таблиц (экспресс-методик) без применения компьютерной техники.

Это в настоящее время актуально, так как США продолжают наращивать усилия по совершенствованию информационного оружия и методов его применения. Примером этого является развертывание ими системы HAARP на территории Норвегии, Аляске и Гренландии. Это также подтверждается высказыванием директора Агенства национальной безопасности США генералом Кеннет Минихэном, сделанным им в 1998 г.: «Теперь, когда мы вступаем в XXI в., информационные атаки становятся все более привлекательными для противника и нам, видимо, стоит подумать о том, чтобы добавить понятие угрозы для информационной инфраструктуры к нашему определению оружия массового поражения». Подобная угроза о проведении информационной атаки на органы управления Кремля и энергетики России прозвучала из уст пресс атташе Белого дома Дж. Кирби в период предвыборной кампании президента США в 2016 г.

Литература

1. Современные войны и гражданская оборона / под общ. ред. С.К. Шойгу. М.: ИПП «Куна», 2008. 296 с.

2. Carlo Copp. The E – bomb – a Weapon of Electronical Mass Destruction. URL: http.//dailyold/sec.ru:/www.gutenberg.org. (дата обращения: 20.03.2017).

3. Winn Schwartau. More about HERP than some – Information Warfane. URL: http://st.ess.ru/publications/ (дата обращения: 20.03.2017).

4. Расторгуев С.П. Информационная война. М.: Радио и связь, 1998. 416 с.

5. Войны XXI века. Теоретический труд. М.: Воен. акад. ГШ ВС РФ, 2000.

6. Shwartan W. Information Warfare, chaos on the electronic superhighway. New York: Thunder's mounth, press, 1994. 110 p.

7. Доктрина информационной безопасности Российской Федерации. М., 2016.

8. Почепцов Г.Г. Информационные войны. М.: Рефл. бук., 2000. 573 с.

9. R. Haeni Information Warfare. URL: http:// tangle seas gwu. edu/-retc/info-war. (дата обращения: 20.03.2017).

10. Сафина Е.О. Информационное оружие как средство ведения информационного противоборства // Рустрана.рф. URL: http: /article.php?nkj=10872 (дата обращения: 20.03.2017).

11. Кочнев И.М., Рыжова Л.А. Методы противодействия электромагнитному терроризму // Проблемы безопасности и чрезвычайных ситуаций. 2011. № 6.

12. Григорьев М. Методы ведения информационных войн. URL: http://mcpt. narod. ru/pr=war. Html (дата обращения: 20.03.2017).

References

1. Sovremennye vojny i grazhdanskaya oborona / pod obshch. red. S.K. SHojgu. M.: IPP «Kuna», 2008. 296 s.

2. Carlo Copp. The E – bomb – a Weapon of Electronical Mass Destruction. URL: http.//dailyold/sec.ru:/www.gutenberg.org. (data obrashcheniya: 20.03.2017).

3. Winn Schwartau. More about HERP than some – Information Warfane. URL: http://st.ess.ru/publications/ (data obrashcheniya: 20.03.2017).

4. Rastorguev S.P. Informacionnaya vojna. M.: Radio i svyaz', 1998. 416 s.

5. Vojny HKHI veka. Teoreticheskij trud. M.: Voen. akad. GSH VS RF, 2000.

6. Shwartan W. Information Warfare, chaos on the electronic superhighway. New York: Thunder|s mounth, press, 1994. 110 r.

7. Doktrina informacionnoj bezopasnosti Rossijskoj Federacii. M., 2016.

8. Pochepcov G.G. Informacionnye vojny. M.: Refl. buk., 2000. 573 s.

9. Haeni R. Information Warfare. URL: http:// tangle seas gwu. edu/-retc/info-war. (data obrashcheniya: 20.03.2017).

10. Safina E.O. Informacionnoe oruzhie kak sredstvo vedeniya informacionnogo protivoborstva // Rustrana.rf. URL: http: /article.php?nkj=10872 (data obrashcheniya: 20.03.2017).

11. Kochnev I.M., Ryzhova L.A. Metody protivodejstviya ehlektromagnitnomu terrorizmu // Problemy bezopasnosti i chrezvychajnyh situacij. 2011. № 6.

12. Grigor'ev M. Metody vedeniya informacionnyh vojn. URL: http://mcpt. narod. ru/pr=war. Html (data obrashcheniya: 20.03.2017).