Проблемы классификации кибероружия

В.В. Каберник

В статье поднимается проблема классификации существующих и перспективных видов кибероружия по нескольким основным типам. Предлагается базовый комплекс признаков кибероружия, описываются основные признаки, определяющие различие его типов с указанием примеров из спектра известных образцов. Определяются признаки, отличающие кибероружие от информационного, выделены ниши использования кибероружия различных типов. Предлагается также базис для отделения вредоносного программного обеспечения от разведывательных, криминальных и боевых систем.

Публикации последнего времени пестрят использованием терминов «кибервойна», «боевые действия в киберпространстве», «киберугрозы» и им подобными. Это происходит в основном из-за того, что журналисты быстро подхватили не самый удачный термин, используя его в отрыве от контекста. В результате кибервойной с равной вероятностью могут называться пропагандистские операции в информационном пространстве Интернета, попытки взлома банковских систем, операции по выведению из строя критической информационной инфраструктуры, а также любые действия, которые прямо или косвенно связываются с Интернетом, компьютерами и т.п. Точно так же размыто и понятие «киберугроза»: под него зачастую бездумно подводятся опасности, такие, как распространение определенных видов информации в сети, вопросы обеспечения безопасности информационных систем, противостояния вредоносному программному обеспечению (далее по тексту–ПО) и многое другое.

Настоящая статья ставит своей целью классификацию различных видов кибероружия и информационных воздействий, которые нередко ошибочно обозначаются различными терминами с модной приставкой «кибер». Разберемся сначала в терминологии. Термин «кибернетика» появился еще в 1830 г. в философских трудах Андре-Мари Ампера[1], который более известен как один из пионеров электродинамики. Кибернетика определялась Ампером как наука о рациональном управлении государством. В 1948 г. понятие «кибернетика» было использовано Норбертом Винером как наименование науки о закономерностях процессов управления и передачи информации в машинах, живых организмах и в обществе[2]. Объектом исследования кибернетики являются все без исключения управляемые системы, которым присуща обратная связь[3].

Иными словами, кибернетика вовсе не ограничена исследованиями современных информационных систем, алгоритмов и протоколов. Будучи междисциплинарной наукой, она охватывает системы электрических цепей, технологические процессы, логистику, эволюционную биологию, психологию личности, социологию, синергетику и т.п. Особо отметим то, что кибернетика, как наука об управлении, уделяет самое пристальное внимание методам управления государством и обществом[4]. Именно эта область внимания кибернетики и стала причиной ее критики в СССР с последующим объявлением «реакционной лженаукой» в 1950-х гг.

Кибернетика, как тогда казалось, претендовала на разработку научно обоснованного ап-

Каберник Виталий Владимирович – начальник отдела перспективных научно-образовательных разработок Управления инновационного развития МГИМО(У) МИД России. E-mail: vestnik@mgimo.ru

парата управления государством, стремилась «отбросить современную научную мысль, основанную на материалистической диалектике»[5]. Между тем наиболее интересные исследования кибернетиков относились именно к исследованиям политики, общества и способов административного управления. В области исследований информационных систем на смену «общей» кибернетике был создан специализированный высокоэффективный математический аппарат, опирающийся на хорошо разработанные теории систем, управления, автоматов, алгоритмов и т.п. В практическом решении прикладных задач, связанных с информационными технологиями, как правило, используется именно этот аппарат, а не «общая» кибернетика.

К определению кибероружия

Под термином «кибероружие» в настоящее время понимаются самые разнообразные технические и программные средства, чаще всего направленные на эксплуатацию уязвимостей в системах передачи и обработки информации или программотехнических системах. Так, под определения кибероружия подводят общедоступные утилиты работы с сетевой инфраструктурой и нагрузочного тестирования сетей на основании того, что их используют хакеры. Опираясь на масштабность воздействия, к кибероружию причисляют вирусы типа Flame[6] или зомби-сети, используемые для рассылки спама и организации распределенных атак, которые направлены на перегрузку информационных систем и следующий из нее отказ в обслуживании (DOS и dDOS-атаки)[7].

Эта ошибка стала столь расхожей, что назрела необходимость хотя бы минимально формализовать набор признаков, который делает отрывок программного кода оружием. И почему, собственно, именно программного кода? Ошибка, которая ведет к путанице в определениях, заключается в том, что авторы публикаций на тему кибервойн и других агрессий в киберпространстве постоянно смешивают понятия «оружие» и «орудие». Орудием является, например, мотыга. Можно ли ее использовать в качестве оружия? Несомненно, целый спектр видов холодного оружия древности ведет свое происхождение именно от сельскохозяйственных инструментов. Так «милитаризованная» мотыга превращается в клевец или чекан. Это уже оружие: устройство, которое конструктивно предназначено для поражения живой или иной цели, подачи сигналов[8] либо поражения объектов инфраструктуры противника.

Использование не предназначенных для нанесения ущерба орудий с разрушительными целями в агрессивных действиях (войнах) настолько же древнее, насколько старо и само человечество. Крестьянские армии и ополчение с успехом использовали привычные им серпы, мотыги, лопаты и вилы. Современные кибервоины, не обладающие высокой квалификацией и доступом к специализированным разработкам, точно так же используют доступное им несложное программное обеспечение, созданное вовсе не с какими-то разрушительными целями – начиная с имеющейся в каждой современной операционной системе утилиты ping. Принцип остается тем же самым: слабо подготовленное воинство, вооруженное подручными средствами, вполне способно одержать победу за счет своей массовости. Является ли утилита ping кибероружием? Сама по себе, безусловно, нет. Что не мешает ей оставаться примитивным средством (орудием) ведения кибервойны.

Попробуем формализовать признаки кибероружия. Начнем со второй типичной ошибки при использовании термина – прочной ассоциации кибероружия с программным кодом. Это в корне неверно: кибероружие воздействует на систему, которая совершенно необязательно является компьютером. Объектом воздействия кибероружия может являться любая система с обратной связью, например автомат. Необходимым условием при этом является управляемость объекта воздействия, предсказуемость его реакций. Компьютеры отвечают этому требованию. Но не только они.

Кибероружие первого типа: избирательная система

Рассмотрим пример воздействия на систему с обратной связью. На протяжении многих лет существуют самонаводящиеся ракеты с инфракрасным наведением. Не вдаваясь в тонкости конструкции системы наведения, такую ракету можно считать автоматом, функцией которого является наведение на источник ИК-излучения и его последующее поражение. Одним из способов противодействия ракетам с определенным типом системы самонаведения является использование устройства, генерирующего периодические или стохастические сигналы в ИК-спектре. В предельном упрощении это устройство является мигающей лампочкой. Создавая ложные сигналы для системы сопровождения цели, устройство вмешивается в систему обратной связи автомата. Нарушение нормального функционирования петли обратной связи (вызванное сбоем ожидаемой периодичности повторения импульсов) приводит к срыву наведения.

Обратим внимание на то, что и рассмотренная (ныне устаревшая) схема самонаведения, и устройство для создания помех являются аналоговыми. В них не использовались цифровые системы, компьютеры или программное обеспечение; они являются электронно-механическими приборами. В то же время воздействие помехи является однозначно информационным, происходит внутри некоторой замкнутой управляемой системы, функционирующей по предопределенным законам. Таким образом, задача срыва наведения автомата-ракеты является задачей кибернетики (с натяжкой ее можно считать нештатным способом программирования

этого автомата). Можно ли считать ситуацию, описанную в данном примере, применением кибероружия (мигающей лампочки)?

Как ни парадоксально это звучит, да. Несмотря на простоту помехопостановщика, мы имеем дело с устройством, специально предназначенным для нейтрализации технического средства противника. Это оборонительная система, действующая в пространстве решения кибернетической задачи нарушения функционирования некоторого конкретного автомата. И уже на этом примере мы можем выделить некоторые характерные черты первого типа кибероружия:

1. Воздействие на систему является информационным, отсутствует физическое вмешательство.

2. Воздействие происходит на строго определенную систему или на тип систем с эксплуатацией их уязвимостей.

3. Результатом воздействия является предсказанный и повторяемый результат.

4. Воздействие необязательно разрушительно, целью является прежде всего нарушение нормального функционирования.

Рассмотрим другой пример: использование широкополосной помехи для нарушения функционирования радиосвязи в некотором пространстве. Такое воздействие тоже является информационным и не нацелено на производство каких-либо разрушений. Возможно, нарушение радиосвязи приведет к нарушению управления войсками противника – тогда такое воздействие можно считать воздействием на кибернетическую систему в ее высокоуровневом рассмотрении. Но и в этом случае оно будет:а– нецелевым;б– опосредованным и в– непредсказуемым по конкретно достигаемым результатам. Не выполняется признак №3: точное предсказание результата воздействия невозможно. При детальном рассмотрении можно констатировать, что нарушается также и признак №2: воздействие не имеет конкретной цели. То есть предпринимается попытка нарушить функционирование всех радиосистем, включая собственные, вне зависимости от их типа. В зависимости от используемых способов передачи информации некоторые конкретные образцы могут оказаться слабо уязвимыми для такого ненаправленного воздействия.

В этом примере мы имеем дело с оружием информационным, но не кибернетическим[9]. Оно применяется как бы наобум, в расчете на какое-то заранее неизвестное негативное воздействие с заранее неизвестными последствиями. Именно к информационному оружию следует относить вредоносное программное обеспечение (в том числе известные вирусы и черви). Хотя и в этом случае причисление их к классу оружия является спорным. Предлагаемый комплекс признаков является на первый взгляд достаточным для определения кибероружия, но в то же время противоречит уже (к несчастью) сложившейся терминологии. Действительно, отделение информационного воздействия в пространстве решений кибернетической задачи от абстрактного информационного воздействия для неспециалиста является очень сложным.

Кроме того, в зависимости от уровня рассмотрения системы может меняться и классификация воздействия. Например, точно рассчитанное информационное воздействие может перейти в сферу кибернетики при рассмотрении последствий его влияния на более высокоуровневые схемы управления. Это относится к упомянутому выше срыву управления войсковыми структурами, нарушениям принятия стратегических решений, вопросам реакции масс и т.п. На достаточно высоком уровне рассмотрения любое информационное воздействие можно считать задачей общей кибернетики, но такое рассмотрение не имеет практической ценности. В примере со срывом наведения автомата-ракеты уже обозначено поле взаимодействия: замкнутая управляемая система, функционирующая по предопределенным законам.

Ограниченность этого поля порождает следующие уточняющие признаки кибероружия первого типа:

1. Воздействие кибероружия происходит внутри ограниченных систем.

2. Целью кибероружия являются системы и комплексы, действующие по однозначно установленным законам и алгоритмам.

С этими уточнениями комплекс признаков кибероружия приобретает необходимую сфокусированность. Обратим внимание на то, что под описанные признаки попадают не только программотехнические системы (которые принято выделять в современной практике), но и любые автоматы, функционирующие по известным законам. Казалось бы, этим мы избыточно расширяем спектр рассматриваемых систем. Тем не менее такое расширение является преднамеренным и обоснованным. Сравним два примера:

– в одном целью воздействия абстрактного кибероружия является программный комплекс управления атомным реактором, не подключенный к исполнительным устройствам, тестовый стенд;

– в другом целью воздействия является такой же комплекс, управляющий действующим реактором.

Результатом нарушения функционирования этого комплекса в первом случае будут сравнительно безобидные программные сбои. Во втором же случае результаты будут сильно варьировать в зависимости от спектра, схемы управления и способов функционирования подключенных к системе исполнительных устройств. В хорошо спроектированной отказоустойчивой системе программные сбои могут эффективно парироваться на уровне оконечных управляемых автоматов, которые имеют дополнительные (например, чисто механические) подсистемы обеспечения безопасности. Поэтому для целенаправленного

воздействия при его планировании необходимо также учитывать особенности работы этих конечных автоматов, возможные способы отключения предохранительных систем, изъяны конструкции, проектирования и т.п.

Из приведенного выше сравнения следует вывод о том, что для создания кибероружия первого типа необходимо глубокое знание и понимание способов функционирования объекта воздействия (системы). Исследование уязвимостей только программного кода может оказаться недостаточным: нарушение функционирования управляющей программы необязательно приведет к фатальным сбоям. Восстановление системы при отсутствии фатальных повреждений в этом случае может быть достигнуто простой переустановкой программного обеспечения. Еще более устойчивы распределенные системы, где необходимый уровень нарушения функционирования может быть достигнут только согласованным воздействием на несколько подсистем одновременно.

Отметим еще одну особенность. Кибероружие первого типа эксплуатирует известные уязвимости системы, которые могут быть устранены ее разработчиками при наличии информации о самом факте существования такого оружия. Нет сомнений, что эти уязвимости будут устранены в обязательном порядке при зарегистрированном факте применения оружия. Таким образом, кибероружие первого типа имеет практическую ценность только в том случае, если обеспечена секретность его разработки; сокрыт факт его наличия и внезапность его применения. Иными словами, кибероружие первого типа является едва ли не одноразовым. Если факт его использования или сам факт наличия известен противнику, он приложит все усилия для ликвидации уязвимостей систем, которые являются целью этого оружия. Такая характеристика позволяет говорить о том, что кибероружие первого типа чаще всего является наступательным, ориентированным на нанесение эффективного первого удара.

Примером кибероружия первого типа является ныне широко известный компьютерный червь Stuxnet. Обратим внимание на то, что его целью являлась совершенно конкретная система с известными уязвимостями, в том числе и на уровне конечных исполнительных устройств. Воздействие крайне избирательно: червь практически безвреден для других систем, используя их только как медиатор для распространения, а точнее, как способ доставки к заданной цели. Но попробуем рассмотреть и некоторые следствия прецедента Stuxnet[10]. Исследование уязвимостей цели воздействия не могло не требовать глубокого знания принципов ее функционирования. Из этого следует, что создание данного конкретного образца вредоносного ПО стало возможным только благодаря масштабной разведывательной операции одновременно с нарушением основных принципов построения системы безопасности на объекте, который стал целью воздействия. Сам же образец Stuxnet является в этом контексте лишь вершиной айсберга: специальным средством, разработанным в единичном экземпляре и использованным однократно для осуществления конкретной диверсии. Иными словами, Stuxnet следует сравнивать с заказными разработками разведывательного сообщества; это оружие никогда не предназначалось для массового использования.

Такие черты не могут быть признаны характерными для всех возможных образцов кибероружия первого типа, но их следует признать довольно типичными. Высокая стоимость разработки и предварительных НИОКР, однократность применения, беспрецедентная избирательность поражения и необходимость обеспечения секретности разработки и доставки делают подобные образцы кибероружия непрактичными для реального войскового применения. Они переходят в разряд специальных средств, арсенала спецслужб.

Кроме того, отдельные образцы (существование которых с высокой долей вероятности можно предположить, хотя оно никак не разглашается в открытых источниках) кибероружия первого типа могут быть использованы для нейтрализации критической инфраструктуры противника в целях повышения эффективности первого удара либо ослабления способностей противника противостоять ему. Фактически это те же диверсионные операции, предшествующие началу полномасштабных боевых действий. Интересно отметить, что способы массированного применения таких образцов сходны со структурой первого обезоруживающего ядерного удара, что в некоторых вариантах рассмотрения позволяет причислить такие (описанные абстрактно) разработки к стратегическим наступательным вооружениям. Однако, в отличие от СНВ, кибероружие первого типа не имеет никакого потенциала сдерживания. Практически мгновенное воздействие, отсутствие предупреждения при применении и необходимость обеспечения секретности разработки (и самого факта наличия) выводят такое оружие за рамки действующих соглашений.

Кибероружие первого типа, вероятно, едва ли окажет влияние на способы ведения боевых действий. Ниша такого оружия – диверсии, включая диверсии стратегического уровня. Для армейских формирований использование такого кибероружия непрактично: оно требует высокой квалификации персонала, излишне избирательно, не может применяться на тактическом уровне, крайне дорого во владении и в разработке. Оно войдет в арсенал спецподразделений, причем нередко это будут единичные образцы, создаваемые специально для выполнения конкретных задач. Для задач, решаемых классическими вооруженными силами, более приспособлены другие виды кибероружия.

Второй тип: адаптивные системы с внешним управлением

Выделенный выше признак № 2 характерен для несложных автономных систем. Запрограммированность действий не позволяет применять их против целей, которые значительно отличаются по структуре построения подсистем безопасности. В то же время, если мы рассматриваем модульную систему, этот признак необязательно должен выполняться. Абстрактно такой комплекс кибероружия может быть описан как информационная система, состоящая из четырех блоков: проникновения; сбора информации; связи и управления; мутации (модернизации). Схема воздействия такого кибероружия на целевую систему описывается в следующей последовательности:

1. Используя модуль проникновения, вредоносная часть оружия внедряется в систему.

2. Используя модуль связи и управления, червь предоставляет операторам дополнительную информацию.

3. Пользуясь полученной информацией, операторы выбирают оптимальные способы воздействия на эту конкретную цель.

4. Используя модуль мутации, вредоносное ПО модифицирует себя, приобретая новые свойства.

В описанной последовательности пункты 3 и 4 могут повторяться произвольное число раз. Таким образом, внутри целевой системы червь может проходить последовательную модернизацию, эффективно обходя вновь возникающие способы защиты. Описанная модульная система, очевидно, нацелена прежде всего на выполнение задач шпионажа на длительном отрезке времени. Однако принципы, использованные в ее построении, пригодны также для создания долгоживущей «закладки» в информационной системе противника. В то время как шпионский вариант такого оружия может выдать себя, как минимум, регулярно отсылаемой информацией, адаптивная «закладка» после проникновения в целевую систему может вообще не выдавать себя. Более того, пользуясь своей системой мутаций, она способна, к примеру, избавиться от ненужного уже модуля проникновения, который нередко является характерным признаком, по которому производится поиск вредоносного ПО.

Применение адаптивных систем с внешним управлением в разведывательных целях наблюдалось для червей Flame и комплекса Red October[11]. Технология создания таких комплексов – в упрощенном или, напротив, усложненном варианте – в настоящее время совершенствуется очень активно. Однако рассмотрение разведывательных операций выходит за рамки классификации кибероружия, поэтому мы отметим в первую очередь потенциал использования технологии для создания адаптивных долгоживущих «закладок» в критических информационных системах. Добавление вредоносного кода (изначально либо в угрожаемый период по необходимости) позволяет нарушить функционирование критической инфраструктуры противника по команде оператора. Таким образом, разведывательная технология превращается в эффективное оружие.

Тем не менее второму типу кибероружия присущ существенный недостаток: потребность в действующем канале связи. Это не только позволяет обнаружить присутствие «закладок», но и резко снижает ценность такой системы для проведения атак на цели, изолированные от общедоступных связных каналов (например, не имеющие выхода в Интернет, что характерно для практически всех армейских систем). Поэтому перспективы использования адаптивных систем с внешним управлением в качестве кибероружия ограничены. Дополнительно его масштабное использование осложнено необходимостью иметь квалифицированных операторов.

Но при этом нельзя не отметить важное преимущество систем второго типа: сравнительно низкую стоимость разработки и владения таким оружием. В отличие от автономных систем, система с внешним управлением требует для своей разработки вложений лишь в эффективный модуль проникновения и отчасти в модуль мутаций. Дополнительные вредоносные модули могут разрабатываться и внедряться по мере необходимости. Не исключено, что целевая система позволит ограничиться сравнительно простыми решениями, что будет выявлено на стадии ее анализа. Большая часть работы по фактическому взлому и управлению перекладывается на оператора, что избавляет от необходимости создавать сложный программный код. Человек может реагировать на ситуацию более гибко, и это несомненное преимущество перед заранее запрограммированным спектром реакций. Показательно то, что кибероружие второго типа наиболее часто ассоциируется с китайскими разработками, в то время как США и другие страны Запада больше полагаются на сложные и дорогостоящие автономные системы.

Третий тип: автономная адаптивная система

Для определенных классов целей возможно создание полностью автономной адаптивной системы, которая, опираясь на базу знаний об уязвимостях целевой системы, сможет самостоятельно выбирать оптимальный вариант воздействия. Очевидно, что спектр таких вариантов будет ограничен и уровень адаптивности оружия третьего типа тоже уступает системам второго типа. Но при этом появляется важнейшее преимущество: независимость от связи с оператором. Кибероружие третьего типа уже начинает в высокой степени соответствовать требованиям к классическому оружию поля боя: не предъявляет высоких требований к квалификации оператора, сравнительно просто в применении необученным персоналом, процедура применения может быть предельно автоматизирована.

Кибероружие третьего типа, по сути, является экспертной системой, опирающейся на базу знаний об объекте воздействия, накопленную разведывательными службами классическими методами. В этом его сходство с оружием первого типа, и из этого следует, что создание кибероружия третьего типа также сопряжено со значительными затратами. От оружия второго типа третий тип наследует модульную схему построения, позволяющую комбинировать различные способы воздействия на целевую систему и при необходимости способность изменять себя в зависимости от внешних факторов. Но при этом кибероружие третьего типа является завершенным комплексом, что не позволяет использовать многостадийные алгоритмы внедрения и мутации. Из этого, в частности, следует, что кибероружие третьего типа едва ли может быть компактным, а это, в свою очередь, предъявляет определенные требования к пропускной способности канала внедрения. Кибероружие третьего типа допустимо рассматривать как «обойму» из различных систем первого типа с дополнительным модулем автоматического выбора оптимального способа воздействия.

Наилучшим образом под определение третьего типа кибероружия попадает разработка, проходящая под кодовым названием Suter[12]. Это крайне продвинутая система радиоэлектронной борьбы, которая, предположительно, способна выбирать способ воздействия на системы ПВО противника без участия оператора, анализируя обстановку в реальном времени. Отметим, что описанная система не внедряется в инфраструктуру противника, то есть не является компьютерным червем, а воздействует на целевые системы в реальном времени, включаясь в механизмы обратной связи. Эта разработка засекречена, но, по косвенным данным, можно предположить наличие в ее составе сменных модулей (баз знаний), позволяющих использовать ее против различных классов целей. Накопление информации о способах воздействия, несомненно, требует значительного времени и ресурсов. Повторимся: кибероружие третьего типа является уже полноценным оружием поля боя, но крайне дорогостоящим. Его распространение и совершенствование пока остается практичным лишь в отдельных узких нишах высокотехнологичной войны, да и там еще очень ограниченно. Тем не менее, по мере появления новых разработок и систематического накопления данных об уязвимостях информационных систем, используемых в военных целях, логично ожидать появления новых образцов кибероружия третьего типа в среднесрочной перспективе.

Четвертый тип: автономная самообучающаяся система

Четвертый тип кибероружия пока существует лишь как умозрительная конструкция. Абстрактно его можно описать как систему искусственного интеллекта, которая способна произвольным образом модифицировать себя для автономного проникновения в целевую систему, ее анализа и последующего самостоятельного выбора оптимального способа воздействия, возможно вырабатываемого в реальном времени. Фактически такая абстрактная система является развитием вышеописанных второго и третьего типов, но не нуждается ни в операторе, ни в экспертной системе, поскольку способна вырабатывать решения самостоятельно.

С учетом довольно скромного прогресса в развитии систем искусственного интеллекта и высоких рисков разработки можно предположить, что в среднесрочной перспективе действующих образцов кибероружия четвертого типа создано не будет. Для разработчиков кибероружия еще довольно долго будет перспективнее совершенствовать системы третьего типа. Дополнительным сдерживающим фактором, ограничивающим разработку систем четвертого типа, является крайне узкая ниша их использования и непредсказуемое поведение автономной самообучающейся системы. В обозримом будущем не наблюдается таких задач, которые не могли бы быть решены с использованием других типов кибероружия.

Заключение

Объем статьи не позволяет подробнее рассмотреть подтипы внутри каждого из обозначенных типов кибероружия. Предложенная классификация является лишь базовой и не учитывает способов распространения, воздействия, модификаций, не рассматривает особенностей целевых систем и сред, в которых происходит воздействие. Это остается задачей для будущих исследований. Хотелось бы в то же время отметить крайне важную особенность всех без исключения типов кибероружия. Практически все созданные образцы предназначены для диверсий, обеспечения первого удара, превентивного нарушения связи и дезорганизации командования. Иными словами, мы рассматриваем оружие, являющееся наступательным, обладающее глобальной досягаемостью, практически мгновенным воздействием без какого-либо способа получить предупреждение о его применении. Такие характеристики позволяют приравнять его к стратегическим наступательным вооружениям. Но разработки и применение кибероружия никак не регламентированы международными соглашениями, что не может не вызывать обоснованных опасений. Хотелось бы верить, что такие соглашения будут выработаны раньше, чем новые образцы кибероружия будут испытаны в боевой обстановке.

Kabernik V.V. Approaches to cyber weapons classification problem.

Summary: *Article focuses on the problem of classification of modern and prospective cyber weapons. Suggested complex of characteristics, based on analytical approach allows for type determination for existing and future cyber weapons. Current wider-known samples are classified and their respective niches are pointed out among different aims for cyber weapons application. Working criteria for differentiation between information warfare and practical cyber warfare is suggested for proper classification of malware, espionage toolkits, hacking tools and combat software.*

Ключевые слова

Безопасность, кибероружие, кибервойна, классификация, систематизация, информационная война, международные отношения, информационные технологии.

Keywords

Cyberwar, cyber weapons, international security, information technology, information warfare, classification, international relations.

Примечания

1. Amper A.M. (1834). Essai sur la philosophie des sciences. (Essay on philosophy of science.) Part II. Paris.
2. Wiener N. (1948). Cybernetics; or control and communication in the animal and the machine. New York: Wiley.
3. Понятие «обратной связи» введено А.П.Анохиным в 1935 г. для описания физиологических процессов в монографии «Проблемы центра и периферии в физиологии нервной деятельности».
4. См., например: WIENER, N., The Human Use of Human Beings: Cybernetics and Society: Houghton-Mifflin, 1950.
5. Цитируется по статье «Наука современных рабовладельцев». Наука и жизнь. Июнь 1953. С. 42.
6. Комплекс вредоносных программ, использовавшихся для осуществления шпионской деятельности на Ближнем Востоке. Подробнее см.: http://www.securelist.com/ru/blog/207764007/The_Roof_Is_on_Fire_otklyuchenie_komandnykh_serverov_Flame
7. Подробнее о классификации компьютерных атак см., например: Анализ типовых нарушений безопасности в сетях = Intrusion Signatures and Analysis. — New Riders Publishing (англ.). СПб.: Издательский дом «Вильямс» (русск.), 2001.
8. Определение дано согласно Федеральному закону РФ «Об оружии», ст.1.
9. В задачах практического радиоэлектронного подавления применяются, конечно, и более продвинутые системы. Без пристального рассмотрения принципов действия каждой из них нельзя однозначно причислить их к кибероружию. Некоторые из них могут считаться кибероружием (их будет характеризовать в первую очередь как раз высокая избирательность), в то время как многие другие средства радиоэлектронной борьбы под эту классификацию не подпадут.
10. Stuxnet–специализированный компьютерный червь, предназначенный для нарушения функционирования SCADA-систем, работающих под управлением ПО Siemens SIMATIC. Использован спецслужбами США и Израиля для нарушения функционирования иранских центров обогащения расщепляющихся материалов. Подробнее о Stuxnetсм.http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
11. Подробнее см., например: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation
12. David A. Fulghum, Michael A. Dornheim, and William B. Scott. Black Surprises // Aviation Week and Space Technology – 16.08.2004