УДК 343.7

© Матвиенко Ю.А.
Matvienko Yu.

КОМПЛЕКСНАЯ ИНФОРМАЦИОННАЯ АТАКА ТИПА «КИБЕРСТАЧКА» НА ПРОМЫШЛЕННУЮ АВТОМАТИЗИРОВАННУЮ СИСТЕМУ: АНАТОМИЯ ЯВЛЕНИЯ И ПОДХОДЫ К ЗАЩИТЕ

COMPREHENSIVE ACTIVE INFORMATION ATTACK OF "CYBERSTRIKE" TYPES TO THE INDUSTRIAL AUTOMATED CONTROL SYSTEM: ANATOMY OF PHENOMENA AND APPROACHES TO THE PROTECTION

Аннотация. *В статье проведен анализ технологии подготовки экономического кризиса различного масштаба путём организации и проведения на автоматизированные системы, управляющие процессом производства товаров или услуг, комплексной активной распределённой информационной атаки, получившей название кибер-стачка. Предложены направления организации противодействия такого типа вторжениям с целью ликвидации угрозы экономической безопасности предприятия, отрасли или страны в целом.*

Annotation. *The article analyzes the various scale economic crisis prepare technology by organizing and conducting to the automated systems that control the production process of goods or services, integrated active distributed information attack, known as cyber-strike. Proposed the directions of combating organizations this type of invasion to eliminate the threat of economic security enterprise, industry or country.*

Ключевые слова. *Угроза информационной безопасности, уязвимость, информационное вторжение, экономическая безопасность, производственный процесс, критически важная составляющая, кибер-стачка.*

Key words. *Information security threats, vulnerabilities, information intrusion, economic security, industrial process, a critical component, cyber-strike.*

С военной точки зрения – союзники существуют, с экономической – союзников не бывает.

Один из принципов британской политики

Не в коммунизме дело, как мы теперь понимаем. Сегодня речь идёт о борьбе за ресурсы, влияние, коммуникации, в которых Россия выступает конкурентом.

Филипп Бобков

Самая лучшая война – разбить замыслы противника.

Сунь Цзы

Основой экономики любого государства является материальное производство, которое представляет собой сложный процесс превращения сырья, материалов, полуфабрикатов и других предметов труда в готовую продукцию, удовлетворяющую потребностям общества. Материальное производство состоит из разного рода производственных процессов, структуру которых образует объединение основных, вспомогательных, обслуживающих и других процессов в определенной последовательности [1].

В современных условиях, особенно в автоматизированном производстве, наблюдается тенденция к интеграции основных и обслуживающих процессов. В частности, в гибких автоматизированных комплексах объединены в единый производственный процесс основные, комплектовочные, складские и транспортные операции.

Основной частью производственного процесса являются технологические процессы, в ходе реализации которых как раз и происходит изменение геометрических форм, размеров и физико-химических свойств предметов труда. При этом в каждом процессе есть так называемые критически важные составляющие (КВС), нарушение функционирования которых приводит к срыву процесса производства в целом.

В условиях информационного общества большинство производственных процессов протекают на

Матвиенко Юрий Андреевич – кандидат технических наук, профессор, Академия военных наук, тел. 543-36-76.

Matvienko Juriy – candidate of engineerings sciences, professor, Academy of military science, tel. 543-36-76.

предприятиях с использованием различных автоматизированных систем (АС). Часть процессов (особенно вспомогательные и обслуживающие производственные процессы, связанные с обменом данными и логистикой) непосредственно замкнуты на глобальную АС каковой, по сути, является сеть Интернет. Такой подход позволяет повышать качество услуг и снижать себестоимость товаров.

В статье под автоматизированной системой понимается организационно-техническое объединение персонала предприятия, средств автоматизации его деятельности, размещенных в структурных подразделениях и объединённых между собой и с другими АС посредством линий связи различной физической природы.

Основная задача АС заключается в поддержке производственных и технологических процессов в заданных параметрах посредством своевременного предоставления органам управления и управляемым объектам необходимых информационных ресурсов. При этом в качестве информационного ресурса могут рассматриваться и управляющие воздействия согласно технологии производства товаров и услуг, и данные от различных сенсоров, контролирующих технологический процесс, и разного рода сведения экономического характера для руководства и соответствующих подразделений предприятия, и информация логистического характера, и многое другое, связанное с нормальным функционированием производства.

По аналогии с критически важными составляющими производственных и технологических процессов в информационных процессах, реализуемых автоматизированными системами, также можно выделить так называемые критически важные информационные сегменты (КВИС) [5].

В зависимости от масштабов предприятия и решаемых задач АС могут быть автономными, локальными, региональными, глобальными. Кроме того, АС отдельных предприятий могут быть объединены в отраслевую автоматизированную систему.

В общем случае любая АС вне зависимости от её масштабов и назначения может быть представлена в виде совокупности узлов различного ранга (уровня), взаимодействующих между собой с использованием каналов связи. При этом в каждом узле можно выделить [6]:

- средства аппаратного обеспечения;
- общесистемное программное обеспечение (ОПО);
- прикладное (специальное) программное обеспечение (СПО).

На каждом из узлов АС могут храниться и обрабатываться информационные ресурсы, доступ пользователей к которым может осуществляться посредством локального или сетевого взаимодействия.

В условиях, когда информация является неотъемлемой (а порой и основной) составляющей современного производства, одной из основных задач АС является защита её информационного ресурса от несанкционированного доступа (НСД), а критически важных информационных сегментов – от деструктивного воздействия. В статье под НСД к информационному ресурсу АС понимается преднамеренное целенаправленное нарушение одного из трёх свойств информации: её конфиденциальности, целостности или доступности, а также нарушение работоспособности программно-аппаратных средств её приёма, хранения, обработки, отображения и передачи.

Необходимо отметить, что несанкционированный доступ к информационному ресурсу АС через программно-аппаратные средства её узлов или каналы связи может быть осуществлён по причине наличия в любой технической системе некоторых производственных недостатков (недоделок) - так называемых «уязвимостей». Они могут быть следствием случайных или преднамеренных действий, осуществлённых на этапе разработки АС или её последующей эксплуатации. В этом случае под уязвимостью АС будем понимать недостатки в её программно-аппаратных средствах, линиях связи, в системе мер защиты информационного ресурса АС или же отсутствие таких мер, позволяющих нарушителю целенаправленно совершать действия, приводящие к успешной реализации той или иной угрозы информационной безопасности АС [6].

Существует целый спектр угроз информационной безопасности автоматизированных систем, используемых в промышленном производстве [2,4,7]. В статье рассматривается лишь одна из них – так называемая активная информационная атака, под которой понимается целенаправленное воздействие или последовательность связанных между собой единым замыслом действий злоумышленника, которые приводят к изменению состояния автоматизированной системы вследствие нарушения конфиденциальности, целостности и доступности информационного ресурса АС, а также нарушения работоспособности её программно-аппаратных средств или блокирования доступа к ним легальных пользователей путём преднамеренного использования в своих интересах обнаруженных в информационной системе дефектов или уязвимостей.

Согласно имеющейся классификации информационные атаки (ИА) могут быть подразделены на внеш-

ние и внутренние, однонаправленные и распределённые. Различаются атаки по уровню эталонной модели взаимодействия открытых систем, объекту атаки, по типу уязвимости, активизируемой атакой, этапу и фазе жизненного цикла и т. д. [2, 5, 7]. В частности, выделяют следующие фазы жизненного цикла ИА на ресурсы АС:

1. Рекогносцировка.
2. Вторжение в АС через уязвимости.
3. Атакующее воздействие на элементы АС.
4. Развитие атаки.
5. Завершение атаки.

На стадии рекогносцировки проводится поиск и анализ уязвимостей атакуемой АС, а также осуществляется сбор данных об объекте атаки, на основании чего планируется порядок проведения атаки с учётом имеющегося у злоумышленника замысла и материально-технического ресурса.

На стадии вторжения нарушитель проводит попытку несанкционированного доступа к информационным ресурсам и программно-аппаратным средствам АС.

В случае успеха проводится собственно атака, результатами которой является нарушение конфиденциальности, целостности или доступности информации АС, а также нарушение работоспособности её узлов в зависимости от целей злоумышленника.

В дальнейшем, при положительном результате задуманного воздействия, сфера атаки может быть расширена и на другие элементы АС. Кроме того, на этой стадии жизненного цикла ИА злоумышленник дополнительно может совершать следующие действия:

• устанавливать в АС по своему усмотрению вредоносное программное обеспечение с целью получения в дальнейшем удалённого канала управления информационным ресурсом;

• использовать успешно атакованный узел АС в качестве плацдарма для проведения атаки на другие узлы системы.

Этапом завершения атаки является «заметание следов» со стороны злоумышленника. Мероприятия по сокрытию следов своего присутствия в АС включают удаление соответствующих записей из журналов регистрации узла АС и выполнение ряда других действий, возвращающих атакованную систему в исходное состояние [2].

В настоящее время существуют достаточно обширные базы данных уязвимостей АС и информационных атак. Для систематизации различных критериев, при помощи которых можно описывать последствия атак, были разработаны различные типы их классификаций [2, 5–7].

Следует отметить, что в последнее время при описании информационных атак всё чаще используется термин «кибернетическое оружие». Согласно работе [9] к кибероружию можно отнести «любой инструмент или способ, в состав которого входит общее или специализированное программное обеспечение, применимый с целью нанесения ущерба компьютеру, сети или электронному устройству». При этом, чтобы классифицировать какой-либо продукт как кибероружие, необходимо наличие у него трёх основных компонентов, используемых для формирования его наступательных возможностей, а именно:

• средства доставки поражающего элемента;

• компонента преодоления системы безопасности объекта атаки;

• поражающего элемента – программного кода вредоносного компонента.

На сегодняшний день к кибероружию можно, к примеру, отнести следующие средства поражения АС:

• различные виды атак, позволяющие проникнуть в атакуемую АС или перехватить управление ею;

• компьютерные вирусы, в том числе сетевые («черви»), модифицирующие и уничтожающие информацию или блокирующие работу вычислительных систем;

• «логические бомбы» – наборы команд, внедряемые в программу и срабатывающие при определенных условиях, например, по истечении определенного отрезка времени или нажатии определенной клавиши;

•"троянские кони" – программы, позволяющие выполнять определенные действия без ведома хозяина (пользователя) зараженной системы;

• средства подавления информационного обмена в сетях и др.

Кстати, компьютерный червь Win32.Stuxnet полностью подходит под данное выше определение кибероружия, причём кибероружия нового поколения, так как он, по оценкам специалистов, уже способен «выйти за пределы цифрового мира» и уничтожить материальные объекты, а не только парализовать интернет-коммуникации. Специалисты фирмы «Symantec» выяснили следующее [13]:

• Win32.Stuxnet – очень сложная и виртуозно спроектированная угроза, использующая 4 «уязвимости нулевого дня» и украденные сертификаты безопасности;

• это – первый «червь», направленный на SCADA-системы (системы автоматизации производства), целью которого являлся шпионаж и перепрограммирование систем;

• злоумышленники не преследовали цели получить финансовую прибыль;

• для создания такого кибероружия нужен очень высокий уровень экспертизы и значительные ресурсы;

• над созданием Stuxnet работали как минимум 6-10 человек на протяжении 6–9 месяцев;

• теперь хакеры имеют возможности использовать код Win32.Stuxtet как шаблон для будущих информационных атак на промышленные объекты.

Таким образом, появление кибероружия, способного причинять вред процессам материального производства в физическом пространстве, в определённых условиях может представлять серьёзную угрозу экономической безопасности любого государства, в том числе и России. При этом наметившиеся тенденции развития деструктивных информационных технологий, направленных на нарушение функционирования не только самих АС, но и управляемых ими процессов производства различных товаров или услуг, позволили говорить и о новом типе активной распределённой информационной атаки – виртуальной забастовке или кибер-стачке [11].

Суть её заключается в том, что в результате скрытого для руководства предприятия информационного вторжения в автоматизированную систему управления неким производством товаров или услуг происходит остановка того или иного технологического или обеспечивающего процесса так, как если бы это сделал персонал организации, объявивший забастовку.

На самом же деле путём внедрения в автоматизированную систему (через Интернет или так называемых «инсайдеров») вредоносного программного обеспечения и его активации обеспечивается по сути «внешнее» управление нужными процессами материального производства (в первую очередь их критически важными составляющими). Это позволяет к определённому времени нарушить всю технологию производственного процесса и, как следствие, остановить производство в целом. При этом сам сотрудник, чья ПЭВМ участвует в процессе производства товаров или услуг, может и не подозревать, что его компьютер «бастует»: на мониторе он может наблюдать показатели, соответствующие нормальному протеканию всех процессов в технологической цепи. Факт же киберстачки в этом случае может быть обнаружен не сразу, хотя отдельные ПЭВМ могут даже зафиксировать некий системный сбой. Причину остановки производства из-за информационного вторжения можно вообще не обнаружить, если во вредоносном программном обеспечении предусмотрена функция самоуничтожения после проведения неких действий по намеченной злоумышленником программе.

Прототипом информационной атаки типа кибер-стачка можно считать так называемые атаки «отказ в обслуживании», проводимые как одиночно (DOS-атаки), так и комплексно (DDOS-атаки) [5, 7, 21].

В условиях продолжающегося финансово-экономического кризиса и роста конкурентной борьбы как на внутренних рынках, так и на мировой арене, последствия от реализации киберстачки в базовых производственных или жизнеобеспечивающих отраслях экономики могут привести к значительному материальному ущербу и непредсказуемым последствиям.

Так, по заявлениям некоторых иностранных экспертов, прекращение работы компьютерных систем приведет к разорению 20% средних компаний и около 33% банков в течение нескольких часов, 48% компаний и 50% банков потерпят крах в течение нескольких суток. Исчезновение на рынке товаров и услуг одних предприятий в эпоху глобализации экономики довольно быстро может быть компенсировано подобными товарами и услугами других торговых марок. Возвращение же в потерянную экономическую нишу предприятий, допустивших остановку производства, процесс довольно длительный и не всегда успешный. Разорение компаний и банков, в свою очередь, способно нанести урон не только владельцам, работникам и вкладчикам, но и экономике государства. Наиболее в этом случае пострадает мелкий и средний бизнес, но угроза банкротства будет велика и для крупных организаций. Такая ситуация как снежный ком может вызвать лавину банкротств и резкий рост социальной напряженности сначала в отдельных регионах или отраслях экономики, а затем и в стране в целом.

Анализ инцидентов, связанных с информационным вторжением, а также возможностей существующих технических и программных средств позволяет сделать неутешительный вывод, что в настоящее время информационная атака типа киберстачка может быть организована практически против любой компании по производству товаров или услуг, не исключая и промышленных гигантов – ТНК и им подобных [5, 7, 21]. Будут различны лишь масштаб, а также формы и методы организации атаки.

В частности, при оценке степени угрозы информационной атаки типа киберстачка для российской экономики необходимо учитывать следующее.

Несмотря на все попытки «перезагрузки», наиболее сложными на международной арене остаются отношения между Российской Федерацией и Соединёнными Штатами Америки. К сожалению, сегодня, как и десятилетие назад, остаются актуальными слова такой одиозной фигуры американской политики как Збигнев Бжезинский, ко-

торый однажды заметил: "Для Америки Россия слишком слаба, чтобы быть ее партнером, но, как и прежде, слишком сильна, чтобы быть просто ее пациентом...».

США по-прежнему, начиная с 90-х годов XX века, придерживаются концепции однополярного мира, открыто заявляя в доктринальных документах о том, что и "в обозримом будущем Соединенные Штаты сохранят своё экономическое и военное могущество". Для успешной реализации данной политической концепции в феврале 2011г. в США была принята обновлённая «Национальная военная стратегия». Практическая реализация данной стратегии, по мнению её авторов, призвана помочь сохранению американского глобального лидерства и доминирования в мире, правда, с учётом реальных условий существующей в настоящее время многополярности и ограниченных возможностей самой Америки, связанных с финансово-экономическим кризисом и участием США в агрессии против Афганистана и Ирака.

В Национальной военной стратегии «NMS-2011» прослеживается впервые обозначенный в «Стратегии национальной безопасности-2010» подход, предусматривающий комплексное использование всех инструментов воздействия: от дипломатии до военной силы, включая возможности, предоставляемые информационными технологиями. «Наша способность эффективно работать в киберпространстве становится все более важной для нанесения поражения агрессору... Мы должны нарастить наши способности к проведению операций в киберпространстве при непригодности или недоступности общего пространства».

Необходимо отметить, что в вопросах, связанных с информационными технологиями, в американской внешней политике силовой (военный) аспект становится всё более приоритетным. Так, в Минобороне США создано специальное «кибернетическое командование». Для этого ведомства принят основополагающий документ - «Стратегия Минобороны по операциям в киберпространстве» (DoD Strategy for Operating in Cyberspace), согласно которому киберпространство объявлено такой же «обычной средой деятельности ВС США, как суша, море или воздушное пространство». Данный документ также предполагает, что в ответ на реальные или виртуальные угрозы и вызовы США готовы использовать любые средства – дипломатические, экономические, кибернетические и чисто военные.

Одной из форм борьбы, активно практикуемой в последнее время США и их союзниками для достижения своих интересов, является концепция нацеленности на конечный результат или эффект – «Effects-Based Approach to joint Operations» [19, 20]. Данный тип операций не является новым классом военных операций, а представляет собой интегрированное применение всего арсенала государственных, экономических, военных и дипломатических средств и процедур по отношению к противоборствующей стороне при обеспечении тесного взаимодействия с государствами-союзниками. Впервые эта концепция была применена в 1999г. в отношении суверенной Югославии. Тогда комплексное применение политических, дипломатических и экономических мер в сочетании с действиями международных неправительственных организаций на фоне ракетных и бомбовых ударов авиации стран НАТО в условиях широкого проведения информационно-психологических операций принудило президента Милошевича подписать Дейтонское соглашение и в конечном итоге привело к распаду СФРЮ [20].

Дальнейшее развитие концепция «Операция на основе эффектов» получила в ходе военной агрессии США и их союзников по НАТО в Афганистан и Ирак. При этом для достижения своих конечных целей в Ираке США дополнительно использовали и такой экономический рычаг, как откровенный подкуп военной верхушки армии Ирака и части окружения Саддама Хусейна, проведя специальную операцию накануне вторжения.

Вообще, для ведения подрывной экономической деятельности в США в своё время был создан целый институт специальных экономических советников – «экономических киллеров» [16, 24]. Так, согласно «Исповеди...» [16], работа «экономических убийц» заключалась «в убеждении мировых лидеров становиться частью обширной сети продвижения американских коммерческих интересов. В конце концов, эти лидеры должны оказаться пойманными в ловушку паутины долгов, которая гарантирует их лояльность. Мы сможем опереться на них всякий раз, когда того пожелаем, – для удовлетворения наших политических, экономических или военных интересов. В свою очередь, они укрепят свои политические позиции тем, что дадут своему населению технопарки, электростанции и аэропорты. А владельцы американских инжиниринговых и строительных компаний станут баснословно богаты».

Ещё одним средством воздействия на органы власти противника, широко используемым в рамках концепции «Операция на основе эффектов» за счёт возможностей современных информационных технологий, являются так называемые «цветные революции», когда люди на основе информации, а чаще - дезинформации, размещаемой в различных социальных сетях, и других способов манипуляции сознанием прекращают работу и выхо-

дят на улицы городов под лозунгами борьбы «за свободу и демократию» [22, 23].

При этом в ходе «цветной революции» может дополнительно задействоваться и дипломатический рычаг, как это было в случае с Ливией, когда для свержения законного правительства весной 2011г. под нажимом США Советом безопасности ООН 18 марта была принята резолюция №1973. Эта резолюция позволила членам Североатлантического альянса в дальнейшем легитимно организовать в Ливии фактически военный переворот под прикрытием так называемых «повстанцев» и других противников лидера ливийской Джамахирии и установить в стране после уничтожения полковника Каддафи лояльный Западу режим.

С учётом изложенного возможность организации и проведения со стороны блока НАТО и, в первую очередь, США информационной атаки типа киберстачка против предприятий (и даже отдельных отраслей) промышленности России следует рассматривать как серьёзную кибернетическую угрозу экономической безопасности страны.

Реальность и масштаб угрозы могут быть понятны, если вспомнить, что в настоящее время военное ведомство Америки эксплуатирует более 15 тыс. информационных сетей, построенных на базе 7 тыс. компьютеров, размещающихся на сотнях объектов в десятках стран мира. При этом анализ возможных средств и технологий, практикуемых США и их союзниками для достижения своих политических целей, позволяет с высокой вероятностью предположить, что с позиций концепции «Операция на основе эффектов» успешно организованная массовая киберстачка при меньшем времени и затратах на её проведение по своему конечному результату может сравниться, а то и превысить эффект от долгосрочных действий так называемых «экономических киллеров» или быстротечной, но высокозатратной боевой войсковой операции, чреватой, помимо всего прочего, безвозвратными потерями личного состава, вооружения и техники.

Какие же меры для защиты экономического потенциала страны от угрозы организации виртуальных забастовок можно предпринять в современных условиях?

Специалисты по защите бизнеса на основе печального опыта приватизации промышленности СССР в конце XX века и рейдерских войн в начале XXI века в России пришли к следующим выводам: «Без понимания сущности стратегии нападения и основных технологий грамотную оборону не построить: только знание и прогнозирование действий противника позволяют быстро провести соответствующие контрприёмы» [17, 18].

Поэтому последуем мудрому совету великого китайского полководца Сунь Цзы, который много лет назад сказал: «Тот, кто знает врага и знает себя, не окажется в опасности и в ста сражениях. Тот, кто не знает врага, но знает себя, будет то побеждать, то проигрывать. Тот, кто не знает ни врага, ни себя неизбежно будет разбит в каждом сражении» и исследуем «анатомические» особенности распределённой активной информационной атаки, каковой, по сути, и является киберстачка.

На наш взгляд, в терминах информационно-психологической войны киберстачка представляет собой специальную информационно-психологическую операцию (ИПО), под которой следует понимать совокупность согласованных и взаимоувязанных по целям, задачам, месту и времени, объектам и процедурам видов, форм и способов информационно-психологического воздействия на сознание и подсознание сотрудников предприятия (в первую очередь обслуживающих КВС производственного процесса), а также информационно-технического воздействия на программно-аппаратные средства промышленной АС (в первую очередь на её КВИС), с использованием различных коммуникационных каналов и уязвимостей с целью прекращения производства товаров или услуг в течение определённого времени.

Такое комплексное использование в определенной последовательности информационных технологий против программно-аппаратных средств и психологических техник против обслуживающих их сотрудников промышленного предприятия или целой отрасли с целью прекращения производства, в первую очередь жизненно важных товаров или услуг, по своей сути представляет собой определенную методологию изменения картины мира у субъектов информационного воздействия (персонала) в требуемом для атакующего направлении [13]. А гражданами с изменённым сознанием легко манипулировать для достижения любых целей.

Как и любая информационно-психологическая операция, атака типа киберстачка включает фазы рекогносцировки и разведки; информационного вторжения в производственный процесс с использованием уязвимостей АС, нарушения работы или прекращения функционирования КВС и КВИС; сокрытия следов атаки и оценки её результативности.

В фазе разведки ведется поиск уязвимостей автоматизированной системы управления производством, которое выбрано в качестве цели, сбор различной информации об объекте предстоящей атаки и внедрение (при необходимости) инсайдеров в трудовые коллекти-

вы предприятий – потенциальных жертв будущей атаки. На этой же фазе параллельно ведётся подготовка отношений со СМИ, после чего запускается PR-кампания по формированию в глазах общественности негативного имиджа продукции или услуг предприятия-мишени (или целой отрасли) [18]. Ярким примером такого типа негативных PR-акций является ежегодная весенняя кампания по дискредитации традиционных мест отдыха россиян на Черноморском побережье Кавказа и в Крыму, проводимая в российских СМИ по заказу и в интересах туристических ведомств Египта и Турции. В итоге туриндустрия России терпит колоссальные убытки, а наши граждане гибнут за границей от некачественного алкоголя и в дорожно-транспортных происшествиях.

Можно сказать, что фаза разведки состоит из череды взаимообусловленных разовых акций, под которыми понимаются кратковременные целенаправленные действия, отличающиеся ограниченным характером (использованием отдельного типа информационного или психологического воздействия с задействованием ограниченного количества коммуникационных каналов) и осуществляемые в локальных масштабах [25].

Ядром операции «киберстачка», её ключевой фазой является собственно распределённая информационная атака с использованием вредоносного программного кода, способного нарушить нормальное протекание производственного процесса или полностью остановить его. На этом этапе последовательно сначала осуществляется информационное вторжение в АС (взлом её системы защиты), а затем проводится воздействие на критически-важные информационные сегменты АС и управляемые ею критически-важные составляющие процесса производства товаров или услуг. При этом стратегия атаки – то есть время, место и масштаб вторжения выбираются по результатам фазы рекогносцировки и разведки.

Отличительной особенностью атаки типа киберстачка является специальное воздействие на электронную вычислительную технику (ЭВТ) предприятия-мишени, направленное на дезинформацию пользователей (операторов): в процессе вторжения параллельно осуществляется сокрытие от персонала не только факта информационного нападения на АС, но и фактов нарушения режимов функционирования контролируемых ими технологических или обеспечивающих процессов, до тех пор, пока на предприятии не сработают системы и средства аварийной остановки.

Одновременно в рамках отдельной PR-кампании осуществляется манипуляционное воздействие на персонал предприятия-мишени с целью принудить его к реальной забастовке и формируется негативное общественное мнение, связанное с деятельностью руководства предприятия (и отрасли в целом) в складывающихся условиях, а также качеством производимых предприятием товаров или услуг.

После успешного информационного вторжения в промышленную АС и достижения цели киберстачки – остановки производства товаров и услуг, – начинается этап закрепления успеха с целью вытеснения атакованного бизнеса с рынка товаров и услуг. В этот период потребителям продукции начинают усиленно рекламироваться на выгодных условиях аналогичные товары и услуги возможных конкурентов: инициаторов киберстачки (или заказчиков). В это же время в соответствии с планом атаки против предприятия-мишени начинается агрессивная PR-кампания с использованием различных «грязных» технологий [18]: может быть организован рейдерский захват «бастующего» предприятия, особенно, если оно «ключевое» в данной отрасли производства; для «расшатывания» ситуации могут быть искусственно инициированы и нападения на предприятие со стороны так называемых «гринмэйлеров»; может быть искусственно создан конфликт собственника с руководством предприятия или одних акционеров с другими (в зависимости от формы собственности предприятия-мишени) и т.п.

На последующем, завершающем этапе информационной атаки в кибернетическом пространстве производится «заметание следов» информационного воздействия на АС предприятия [2, 7], а в физическом пространстве формируется положительное общественное мнение о результатах, полученных в результате атаки. Кроме того, организаторами атаки проводится оценка результативности предпринятых действий по критерию: «успех нападения определяется достижением цели», после чего принимается решение о продолжении действий против предприятия-мишени или атакующее воздействие следует прекратить [13, 17, 18].

Такова вкратце «анатомия» информационной атаки типа киберстачка.

При разработке методов борьбы с этой угрозой для промышленных предприятий необходимо помнить, что в условиях обострения борьбы ведущих мировых держав и межгосударственных союзов за лидерство на международной арене нарушение экономической безопасности России следует рассматривать как одну из основных предпосылок к изменению в дальнейшем и её геополитического статуса.

В то же время по состоянию на сегодняшний день приходится признать, что в большинстве традиционных

систем защиты от информационных атак реализована в основном рефлексивная модель управления: они вступают в действие только на второй фазе атаки – попытке непосредственного информационного вторжения в автоматизированную систему управления предприятия [2, 6]. Вместе с тем организацию противодействия атаке на техническую систему следует сравнивать с организацией лечения болезни живых организмов: чем раньше удаётся отследить первые симптомы болезни и начать реагировать, тем быстрее и с меньшим ущербом для здоровья пациента пройдёт лечение [18].

Поэтому противодействие информационной атаке целесообразно начинать ещё на этапе сбора злоумышленником информации о предприятии, о его средствах и системах автоматизации и их уязвимостях, то есть в фазе разведки и рекогносцировки при подготовке и планировании киберстачки. Уже на этом этапе желательно уметь оценить ожидаемый характер угрозы с атакующей стороны, что позволит понять, с каким типом противника возможно столкновение, какие цели им преследуются и какие ресурсы задействуются. Такой подход к организации системы защиты предприятия позволит существенно усложнить, а часто и нейтрализовать работу организаторов информационной атаки на АС производством.

Анализ существующих методов, систем и средств противодействия информационным атакам применительно к такой потенциальной угрозе как киберстачка позволяет сделать вывод, что для успешного противодействия ей система защиты предприятия должна быть комплексной (с использованием организационно-правовых мер, программно-аппаратных методов и инженерно-технических средств защиты) и строиться на основе генерирующей (творческой) модели управления защитой. При этом в рамках системы защиты информации АС предприятия должна быть реализована так называемая инфраструктура обнаружения атак (ИНФОБА) [2]. Что имеется в виду?

Целью нападающей стороны является нарушение функционирования производственных процессов с последующим прекращением работы предприятия. Желаемого результата можно достичь за счёт получения несанкционированного доступа к определённому информационному ресурсу АС или путём нарушения работоспособности определённых программно-аппаратных средств из её состава. Для этого у организаторов атаки должна быть собрана достаточно большая база данных о предприятии-мишени, что подразумевает проведение широкого и тщательного поиска уязвимостей АС.

Поэтому ИНФОБА должна быть настроена на обнаружение различного рода попыток анализа процессов функционирования АС (особенно её КВИС), проникновения в её узлы и проводить регулярный аудит АС с целью выявления уязвимостей системы, возникающих по тем или иным причинам в процессе её функционирования. При этом ИНФОБА не должна ограничиваться только внешними угрозами технической составляющей АС [2, 4-6]. Необходимо не забывать и о внутренних угрозах информационной безопасности АС предприятия [26]. Кроме того, в инфраструктуру обнаружения атак должны поступать данные и от службы связей с общественностью предприятия, особенно если в медиа-пространстве замечена негативная информация о его деятельности.

На наш взгляд, для успешного противодействия информационной атаке типа киберстачка необходимо осуществить следующие мероприятия.

Первое. Провести исследование по выявлению и классификации критически важных составляющих разного типа технологических процессов промышленного производства, в первую очередь обеспечивающих жизнедеятельность населения страны, и критически важных информационных сегментов автоматизированных систем, задействуемых в КВС процессов производства товаров и услуг.

Второе. Доработать законодательство в области информационных технологий в части обязательного наличия в КВС промышленного производства и КВИС промышленных АС, обеспечивающих жизнедеятельность населения страны, комплексных систем защиты технологий производства и информационных процессов и поддержания их в актуальном состоянии.

Третье. Совершенствовать системы анализа защищённости промышленных АС (системы поиска уязвимостей проектирования, реализации и эксплуатации), как средство определения потенциальных возможностей реализации информационных атак.

Четвёртое. Регулярно проводить на предприятиях, обеспечивающих жизнедеятельность населения страны, кризисный аудит КВС производства и КВИС АС с целью выявления уязвимостей, через которые может быть реализована угроза киберстачки.

Пятое. Пересмотреть на предприятиях и в организациях, участвующих в производстве жизненно важных товаров и услуг, политики и процедуры безопасности в направлении обеспечения противодействия информационной атаке типа киберстачка с обязательным обучением и подготовкой персонала.

Следует помнить, что киберстачка вне зависимости от того, кто является её организатором, может угро-

жать территориальной целостности, политической независимости или экономической безопасности любого из государств – объектов распределённой активной информационной атаки такого типа.

Сами американцы признают, что «кибератака, если в результате ее будет нарушена работа национальной энергосистемы, финансовых и правительственных органов, по степени разрушительного воздействия может стать следующим Пёрл-Харбором». В настоящее время в США приходит осознание того, что в недалеком будущем кибератаки будут направлены не только на извлечение из информационных систем Пентагона закрытых данных, но и на нарушение нормального функционирования оборонных систем различного назначения, а также на вывод из строя важнейших элементов национальной инфраструктуры, включая объекты атомной энергетики, что может привести к гибели нанесения Америки.

Возможным идеологам и организаторам киберстачки хочется напомнить слова американского журналиста Филиппа Найтли о том, что в условиях глобализации и интеграции «дестабилизация той или иной страны может угрожать мировой экономической системе в целом, и особенно в сфере погашения международной задолженности, ударяя, таким образом, и по интересам США».

Тем не менее в заключение хочется отметить следующее. В наше смутное время финансового кризиса, дефицита топливно-энергетических и питьевых ресурсов и обострения, в том числе и экономических противоречий между ведущими государствами мира, хочется напомнить всем тем, от кого так или иначе зависит экономическая стабильность и безопасность России, слова полководца древности Сунь Цзы: «Правило ведения войны заключается в том, чтобы не полагаться на то, что противник не придёт, а полагаться на то, с чем можно его встретить; не полагаться на то, что он не нападёт, а полагаться на то, чтобы сделать нападение на себя невозможным для него».

Поэтому одной из главных задач для властных структур России и «капитанов» российского бизнеса должна быть задача создания и внедрения в промышленности комплексных систем безопасности, способных противостоять, в том числе и такой угрозе как активная информационная атака типа «киберстачка».

Литература

1. Туровец О.Г., Родионов В.Б., Бухалков М.И. «Организация производства и управление предприятием». – М.: ИД «ИНФРА-М», 2007.
2. Лукацкий А.В. «Обнаружение атак». – СПб.: «БХВ-Петербург», 2001.
3. Малюк А.А., Горбатов В.С., Королёв В.И. и др. «Введение в информационную безопасность: учебное пособие для вузов под ред. В.С. Горбатова». – М.: «Горячая линия – Телеком», 2011.
4. Девянин П.Н. «Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов». – М.: «Горячая линия – Телеком», 2011.
5. Климов С.М. «Методы и модели противодействия компьютерным атакам». – Люберцы: КАТАЛИТ, 2008.
6. Сердюк В.А. «Новое в защите от взлома корпоративных систем». – М.: «Техносфера», 2007.
7. Сердюк В.А. «Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятия: учебное пособие». – М.: Изд. дом Гос. Ун-та – Высшей школы экономики, 2011.
8. Савенкова Т.И. «Логистика: учебное пособие для студентов». – М.: издательство «Омега-Л», 2011.
9. Паршин С.А., Горбачёв Ю.Е., Кожанов Ю.А. «Кибервойны – реальная угроза национальной безопасности?». – М.: КРАСАНД, 2011.
10. Гранатуров В.М. «Экономический риск: сущность, методы измерения, пути снижения: учебное пособие». – М.: «Дело и сервис», 2010.
11. Матвиенко Ю.А. «Варвары информационного общества. Кибер-стачка как угроза экономической безопасности России». Статья в журнале Академии военных наук «Информационные войны» № 4 (20) за 2011г.
12. Мельников В.П., Клеймёнов С.А., Петраков А.М. «Информационная безопасность: учебное пособие для сред. проф. образования под ред. С.А. Клеймёнова». – М.: Издательский центр «академия», 2005.
13. Матвиенко Ю.А. «Реконструкция информационных операций» в книге В.Б. Вепринцева, А.В. Манойло и др. «Операции информационно-психологической войны. Краткий энциклопедический словарь-справочник», М., «Горячая линия - Телеком», 2005г.
14. Башлы П.Н. «Современные сетевые технологии: Учебное пособие». – М.: «Горячая линия – Телеком», 2006.
15. Починок Н., директор отдела технических решений фирмы «Symantec» в России и СНГ. Доклад «Статистика 2010: Защита объектов критической инфраструктуры в России и мире. Угрозы и их последствия на примере кибер-атаки на ядерный завод в Иране», 2011.
16. Перкинс Джон «Исповедь экономического убийцы». – М.: Pretext , 2010.
17. Бианки В.А., Серавин А.И. «Убрать конкурента: PR-атака». – СПб.: «Питер». 2007.
18. Студеникин Н.В. «PR-защита бизнеса в корпоративных войнах: Практикум победителя». – М.: «Альпина Паблишерз», 2011.
19. Савин Л.В. «Сетецентричная и сетевая война. Введение в концепцию». – М.: «Евразийское движение», 2011.
20. Паршин С.А. «Современные тенденции в теории и практике совершенствования оперативного управления вооружёнными силами США». – М.: «Едиториал УРСС», 2009.
21. Мандиа Кевин, Просис Крис «Защита от вторжений. Расследование компьютерных преступлений». – М.: «ЛОРИ», 2005.
22. «Оранжевые сети: от Белграда до Бишкека / отв. ред. Н.А. Нарочницкая, ред и сост. Е.А. Бондарева». – СПб.: Алетейя, 2008.

23. Шарп Джин «От диктатуры к демократии / пер. с англ. Н. Макаровой». – Екатеринбург: «Ультра. Культура», 2005.
24. «Игры экономических убийц, тайный мир международных махинаций и сеть глобальной коррупции / под ред. Стивена Хайата». – М.: «Претекст», 2008.
25. Матвиенко Ю.А. «Аналитическая реконструкция информационно-психологической операции против кандидата на выборную должность как один из методов противодействия нелегитимным избирательным технологиям». Статья в журнале Академии военных наук «Информационные войны» № 3 (11) за 2009г.
26. Скиба В.Ю., Курбатов В.А. «Руководство по защите от внутренних угроз информационной безопасности». – СПб.: «Питер», 2008.

Материал поступил в редакцию 28. 11. 2011 г.