THE ANALYS OF CYBERATTACKS AGAINST THE INFORMATION AND TELECOMMUNICATION SYSTEMS

Larin V.V., Tarnapolov R.V.
Kharkiv Air Force University named after Ivan Kozhedub
77/79, Sumska Str., Kharkiv, 61023, Ukraine
Ph.: (+38 057) 7002165, e-mail: info@hups.mil.gov.ua

Abstract — At the present stage of our society development many of the traditional resources of the human progress gradually lose their original meaning. To replace them a new resource comes, the only product not diminishing, but growing with time, is information. Nowadays information becomes the main resource of scientific-technical and socio-economic development of the world community. The more and faster the quality information is implemented into the national economics and special applications, the higher the standard of life, as well as economic, defence and political potential of the country is.

АНАЛИЗ КИБЕРАТАК НА ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

Ларин В. В., Тарнополов Р. В.
Харьковский университет Воздушных Сил имени Ивана Кожедуба
ул. Сумская, 77/79, Харьков, 61023, Украина
тел.: (+38 057) 7002165, e-mail: info@hups.mil.gov.ua

Аннотация — На современном этапе развития нашего общества многие традиционные ресурсы человеческого прогресса постепенно утрачивают свое первоначальное значение. На смену им приходит новый ресурс, единственный продукт не убывающий, а растущий со временем, называемый информацией. Информация становится сегодня главным ресурсом научно-технического и социально-экономического развития мирового сообщества. Чем больше и быстрее внедряется качественной информации в народное хозяйство и специальные приложения, тем выше жизненный уровень народа, экономический, оборонный и политический потенциал страны.

I. Введение

Люди удаются к кибератакам по различным причинам. Например, террористы или правительства могут пробираться в компьютерные сети врагов и красть секретные данные или повреждать оборудование, которым руководят эти сети. В 2010 году зам министра обороны США Вильям Линн признал, что «враги» неоднократно атаковали засекреченные компьютерные сети США и воровали «тысячи файлов… в том числе проекты оружия, планы операций и данные разведки» [1].

Любая предпринимательская деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Целостность современного мира как сообщества обеспечивается, в основном, за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способно привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений. Поэтому в новых рыноч-но-конкурентных условиях возникает масса проблем, связанных не только с обеспечением сохранности коммерческой (предпринимательской) информации как вида интеллектуальной собственности, но и физических и юридических лиц, их имущественной собственности и личной безопасности.

II. Основная часть

В информационно-телекоммуникационной системе можно выделить три варианта воздействия на информацию:

1. Задержка в передаче информации. Телекоммуникационная система может обеспечить абсолютно достоверную передачу информации, но время ее передачи может оказаться столь длительным, что она потеряет свою актуальность для потребителя. В предельном случае задержка информации может привести к её полной потере.

2. Искажение или нарушение целостности информации. При этом часть информации может быть утеряна, подменена другой информацией, либо к исходной информации может быть добавлена информация, искажающая исходную (например, вирусы). В предельном случае искажение информации может привести к полной её потере.

3. Несанкционированный доступ к информации, т.е. нарушение конфиденциальности информации.

Задержка в передаче информации возникает, в основном, в сетях электросвязи. Усложнение применяемых технологий сетей электросвязи, процессов управления сетями и их технической эксплуатации объективно ведет к возникновению сбоев в функционировании этих сетей и, как следствие, к задержкам передачи информации [2].

Методами защиты являются: устранение возможных преднамеренных или непреднамеренных ошибок при проектировании сетей электросвязи, а также при настройке оборудования; защита от внедрения вредоносных программ и компонентов, реализующих не декларированные функции, на этапах создания и модернизации сетей электросвязи, а также в процессе технической эксплуатации; контроль за соблюдением правил технической эксплуатации сетей; повышение живучести сетей электросвязи; резервирование линий связи, каналов и трактов; создание системы оперативного управления сетями; создание препятствий для возможного вмешательства в процесс функционирования сетей электросвязи; обеспечение мониторинга состояния сетей электросвязи, своевременного обнаружения попыток деструктивного воздействия на сети электросвязи, локализации места воздействия и оперативной ликвидации последствий воздействия.

2013 23rd Int. Crimean Conference "Microwave & Telecommunication Technology" (CriMiCo'2013). 9—13 September, Sevastopol, Crimea, Ukraine
 ISBN: 978-966-335-395-1. IEEE Catalog Number: CFP13788

Искажения информации могут носить неумышленный или умышленный характер. Для защиты информации здесь используются методы, применяемые на верхних уровнях эталонной модели открытых систем. Для защиты информации важное значение имеет мониторинг нарушения целостности передаваемых сообщений.

Пять основных видов кибератак:

— *финансовые преступления и мошенничество.* Совершаются организованными и хорошо финансируемыми группами лиц, занимающимися хищением средств и прочих активов с помощью современных технологий.

— *шпионаж.* На сегодня корпоративная почта и файлы, а также традиционные объекты интеллектуальной собственности, такие как результаты научных исследований и разработок, представляют большую ценность для любой организации. Хищение интеллектуальной собственности – это постоянная угроза. Жертвы могут даже не догадываться о случившемся до момента внезапного появления пиратских копий на рынке или регистрации патента на результаты исследований и разработок третьими лицами.

— *военные действия.* Сюда относятся военные конфликты между разными странами, а также попытки завладеть организациями частного сектора, в особенности такими важными инфраструктурными объектами национального масштаба, как энергетическая, телекоммуникационная и финансовая системы.

— *терроризм.* Перекликается с угрозой военных действий. Атаки совершаются террористическими группами (с возможной поддержкой со стороны государства) с целью завладения стратегически важными частными или государственными инфраструктурными объектами.

— *активизм*. По своей природе напоминает некоторые другие категории, но атаки при этом совершаются сторонниками той или иной идеологии.

Считается, что для предотвращения или нейтрализации последствий применения кибератаки необходимо принять следующие меры [3]:

— защита материально-технических объектов, составляющих физическую основу информационных ресурсов;

— обеспечение нормального и бесперебойного функционирования баз и банков данных;

— защита информации от несанкционированного доступа, ее искажения или уничтожения;

— сохранение качества информации (своевременности, точности, полноты и необходимой доступности).

Создание технологий обнаружения воздействий на информацию, в том числе в открытых сетях, — это естественная защитная реакция на появление нового оружия. Экономическую и научно-техническую политику подключения государства к мировым открытым сетям следует рассматривать через призму информационной безопасности. Будучи открытой, ориентированной на соблюдение законных прав граждан на информацию и интеллектуальную собственность, эта политика должна предусматривать защиту сетевого оборудования на территории страны от проникновения в него элементов информационного оружия. Это особенно важно сегодня, когда осуществляются массовые закупки зарубежных информационных технологий.

Понятно, что без подключения к мировому информационному пространству страну ожидает экономическое прозябание. Оперативный доступ к информационным и вычислительным ресурсам, поддерживаемым сетью Internet, разумеется, следует приветствовать как фактор преодоления международной изоляции и внутренней дезинтеграции, как условие укрепления государственности, институтов гражданского общества, развития социальной инфраструктуры.

Стратегия кибербезопасности Украины имеет следующие цели:

— наравне с основными рисками и проблемами выявить экономические и геополитические возможности;

— сравнить между собой степень подготовленности и политическое внимание к проблеме безопасности Интернета в третьих странах;

— обозначить основные и важнейшие проблемы, которые требуют решения;

— оценить текущие и планируемые мероприятия, а также отметить те проблемные зоны, к которым государству следует уделить больше внимания.

В среде, где постоянно появляются и эволюционируют кибер-угрозы, государства при встрече с новыми, глобальными угрозами получат большую выгоду от гибких, оперативных стратегий кибербезопасности. Трансграничный характер угроз вынуждает страны вступать в тесное международное взаимодействие. Сотрудничество на пан-европейском уровне необходимо не только для эффективной подготовки к кибератакам, но и для своевременной реакции на них. Комплексная государственная стратегия кибербезопасности — первый шаг на этом пути.

Для реализации стратегий кибербезопасности частный и государственный сектора должны работать в тесном сотрудничестве. Сотрудничество должно осуществляться посредством обмена информацией, передовыми практиками (например, в сфере управления инцидентами), а также учениями на государственном и общемировом уровнях.

III. Заключение

1. Впервые изложены варианты воздействия на информацию в информационно — телекоммуникационной системе и методы защиты от них.

2. Дана классификация кибератак и угроз, которые они несут.

3. Изложены основные направления и цели Стратегия кибербезопасности Украины.

IV. References

[1] Baranov V.M. i dr. *Zashhita informacii v sistemah i sredstvah informatizacii i svjazi. Ucheb. Posobie* [Protection of information systems and means of information and communication. Tutorial]. Saint-Petersburg, 1996. 111 p.

[2] Barannik V.V., Sidchenko S.A., Larin V.V. Metodologija sozdanija kriptograficheskih preobrazovanij na baze metodov iskljuchajushhih izbytochnost' [The methodology for cryptographic transformations on the basis of methods of avoiding redundancy]. *Suchasna special'na tehnika,* 2009, No 4, pp. 5-17.

[3] Sokolov A.V., Stepanjuk O.M. *Metody informacionnoj zashhity ob#ektov i komp'juternyh setej. (Serija «Shpionskie shtuchki»)* [Methods of information protection facilities and computer networks. (Series "Spy stuff")]. Saint-Petersburg, Poligon, 2000. 272 p.