УДК 316

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Черепанова В.Н.[1], Устинова О.В.[2]

[1] Тюменский государственный архитектурно-строительный университет, Тюмень, Россия (625001, Тюмень, ул. Луначарского, 2), e-mail: veranikandrovna@mail.ru;
[2] Тюменский государственный нефтегазовый университет, Тюмень, Россия (625000, Тюмень, ул. Володарского, 38), e-mail: sema_79@bk.ru

Информационные процессы, происходящие повсеместно в современном мире, выдвигают на первый план, наряду с задачами эффективной обработки и передачи информации, важнейшую задачу обеспечения безопасности информации. Это объясняется ростом стоимости информации в условиях рынка, ее высокой уязвимостью и нередко значительным ущербом в результате ее несанкционированного использования. В статье рассматриваются научные подходы к понятию «информационная война», методы, которые используются в информационной войне и ее возможные последствия. Особое внимание в статье уделяется методам предотвращения угроз информационной безопасности. Представлены результаты авторского опроса пользователей сети Интернет, посредством которого выявлены основные угрозы информационной безопасности личности и методы их предотвращения; дана оценка эффективности используемых средств противодействия угрозам информационной безопасности.

Ключевые слова: информационная война, Интернет, средства массовой информации, информационная безопасность.

PROBLEMS OF INFORMATION SECURITY

Cherepanova V.N.[1], Ustinova O.V.[2]

[1] Tyumen State University of Architecture and Civil Engineering, Tyumen, Russia (625001, Lunacharskogo Street, 2), e-mail: veranikandrovna@mail.ru;
[2] Tyumen State Oil and Gas University Tyumen, Russia (625000, Volodarskogo Street, 38), e-mail: sema_79@bk.ru

Information processes occurring everywhere in the world, highlight, along with the task of efficient processing and transmission of information, the critical task of ensuring the security of information. This is due to the increase in the cost of information in the market, its high vulnerability and, often, significant harm as a result of its unauthorized use. The article deals with the scientific approaches to the concept of "information war", the methods used in the information war and the possible consequences. Special attention is paid to the prevention of threats to information security. Presents the results of a survey of Internet users by which identified the main threats to information security of the person and the prevention methods; evaluate the effectiveness of the used means of countering threats to information security.

Keywords: information warfare, Internet, media, information security.

Вооруженная борьба во все времена была неотъемлемым проявлением человеческих взаимоотношений. Развитие методов и технологий ведения войн происходит в тесной взаимосвязи с эволюцией человечества [10, С. 130]. Появление новых знаний и технологий существенно влияет на характер войн. Сегодня средства массовой информации – телевидение, СМИ, Интернет – все в большей степени оказывают влияние на население всех стран мира, формируя отношение к тем или иным событиям. Г.Вирен считает, что Интернет на сегодняшний день занял особое, исключительно важное место, причем его значение год от года возрастает, во многих странах и даже в целых регионах он близок к доминированию [2, С. 24]. В России большинство пользователей сети, и особенно молодежь, предпочитают Интернет газетам, телевидению, радио [13, С. 86]. Поэтому очевидно, что организаторы любой информационной войны будут использовать Интернет в своих целях. Тем более, что

целый ряд присущих ему специфических особенностей делает его особо привлекательным для противоборствующих сторон.

Что же такое информационная война? И.Н. Панарин под информационной войной понимает комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство, которое уже в мирное время приводило бы к принятию благоприятных для стороны-инициатора информационного воздействия решений [8, С. 202]. Н.В. Лопатина, О.Б. Сладкова рассматривают информационную войну как совокупность информационно-социальных технологий, в основе которых лежит целенаправленное изменение массового поведения и общественных настроений посредством манипулирования потоками новостной информации политического и экономического содержания [6]. Г.Вирен полагает, что информационная война – это комплекс мероприятий по информационному воздействию на массовое сознание для изменения поведения людей и навязывания им целей, которые не входят в число их интересов, а также защита от подобных воздействий [2, С. 30].

В ходе информационных войн важным является достижение информационного превосходства, которое определяется через способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать тоже самое. В ходе информационного противоборства предметом поражения и уничтожения являются уже не сами люди, а определенные типы сознаний.

Тактической задачей в информационной войне является затруднение доступа людей (или конкретного противника) к достоверной информации. Важность этого момента объясняется тем, что оперативность и качество оценки обстановки и принимаемых решений на всех уровнях общественной структуры непосредственно зависят от полноты и достоверности представляемой информации.

Можно выделить следующие основные методы, используемые сторонами в информационном противоборстве:

1. Сокрытие критически важной информации о положении дел в какой-либо области;
2. Погружение ценной информации в массив, так называемого, «информационного мусора» в соответствии с принципом «спрятать лист в лесу»;
3. Подмена понятий или искажение их смысла;
4. Отвлечение внимания на малозначимые события;
5. Применение понятий, постоянно используемых в медиапространстве, смысл которых претерпел качественные изменения;
6. Подача негативной информации, которая лучше воспринимается аудиторией по сравнению с позитивными новостями;

7. Обсуждение событий, не имеющих реальной общественной ценности, использование результатов некорректно проведенных социологических исследований для создания искаженного представления о ситуации в обществе;

8. Введение табу на определенные виды информации и разделы новостей в целях недопущения широкого общественного обсуждения критичных для определенных властных структур вопросов и тем;

9. Откровенная ложь в целях дезинформации населения своей страны и зарубежной общественности [4].

В отличие от традиционных вооруженных конфликтов, где круг участников в большинстве случаев четко ограничен и включает в себя специализированные военно-государственные структуры (вооруженные силы, иные военизированные формирования), для информационных войн свойственно активное участие негосударственных структур, при этом в последние годы все большую роль стали играть блогеры, хакеры, неструктурированные сетевые сообщества.

В качестве блогеров выступают частные лица, являющиеся продвинутыми пользователями сети Интернет и ведущими собственные блоги, которые добровольно или по команде вовлекаются в процесс информационной войны. Их основная роль сводится к размещению в своих блогах различной информации: видеозаписей, фотографий, статей, комментариев и прочего контента с целью причинения вреда атакуемому объекту, либо противодействия деструктивному психологическому воздействию с его стороны.

Хакеры – лица, использующие интернет-технологии для причинения ущерба компьютерным сетям и их пользователям. Они участвуют в войне посредством компьютерных атак на информационные ресурсы «вражеской стороны» с целью нарушения их работы и размещения пропагандистской информации на них после взлома.

Неструктурированные сетевые сообщества объединяют обе названные категории лиц под общим брендом и идеей. Несмотря на отсутствие официального статуса и четкой структуры такие сообщества имеют общую концепцию деятельности и занимаются ей на постоянной основе. Наиболее известными в мире сообществами являются «Anonimus, «WikiLeaks», «LulzSec».

Информационная война, реализуемая посредством Интернет, имеет ряд ряд преимуществ перед традиционными СМИ, в числе которых: прямой доступ к аудитории; широта распространения; отсутствие верификации (недостоверность информации, размещаемой в сети Интернет); анонимность; ограниченная юридическая ответственность и прочие [1, С. 111].

Реализация комплекса мероприятий в рамках информационных войн приводит к изменению сознания людей, их отношения к своему обществу, к государству, к самим себе. В результате люди могут потерять, сами того не осознавая, собственную волю, ценности, традиции, а государство – суверенитет.

Например, результаты исследований, проведенных Фарахутдиновым Ш.Ф., Дейнеко С.В., Устиновой О.В. показали, что наиболее значимую роль в девальвации духовно-нравственного развития общества играют средства массовой информации, сила влияния которых соизмерима с институтом семьи и педагогическим воздействием. Ученые отмечают, что общество под воздействием сторонних СМИ претерпевает девальвацию и подмену общечеловеческих ценностей. [12, 11, 9]

Потеря государственного суверенитета и гражданского единства является целью любой войны, но теперь на смену традиционным вооруженным, пришли «мягкие», но не менее опасные «информационные» войны. Как отмечает Н.В. Лопатина: «виртуализация способна создавать ситуации, когда даже ребенок может оказывать влияние на мировое сообщество. Чем не оружие массового поражения?» [5, С. 188]. Поэтому осмысление феномена информационных войн - это очень важная теоретическая и практическая задача [7].

Таким образом, информационное противостояние по значимости и масштабу ни в чем не уступает (а иногда и превосходит) традиционным методам ведения боя. Информационная война - это война технологий, в которой сталкиваются носители информации. Но она, как и любая война, олицетворяет собой борьбу за наиболее выгодные условия существования. А главное то, что в наше время информационное противостояние все чаще становится предпосылкой к реальным боевым действиям. И об этом не стоит забывать.

В контексте вышесказанного актуальным становится противостояние информационным угрозам. Угрозы информационной безопасности граждан представляют собой совокупность факторов и условий, способных оказать негативное влияние на реализацию гражданами своих интересов, связанных с имеющейся у них информацией, принадлежащими им информационными ресурсами и с использованием для обработки информации средств вычислительной техники [3].

Современное динамичное развитие Тюменской области отразилось на росте пользователей Интернет-ресурсами. Относительно высокий уровень благосостояния жителей региона, а также интенсивное развитие рынка информационных технологий, привели к тому, что большинство семей (особенно городских) имеют личные персональные компьютеры, оснащенные выходом в Интернет.

С целью выявления актуальных проблем в сфере обеспечения информационной безопасности личности, авторами статьи проведен анкетный опрос трудоспособного населения г. Тюмени, являющихся постоянными пользователями сети Интернет (всего 214 чел.). В рамках опроса ставились задачи: – выявление основных угроз информационной безопасности и методов их предотвращения; – оценка эффективности средств противодействия угрозам информационной безопасности.

По результатам опроса 40% респондентов стали «жертвами» компьютерных вирусов и атак на базовые узлы сетей; каждый третий столкнулся с активизацией спама; каждый десятый – со взломом систем на базе вредоносных программ (черви, троянские программы); 2-2,3% пользователей отмечают активизацию сетевых атак, административные привилегии, нелегальную перекачку виртуальных денег, подбор и захват паролей, включая личную информацию (рис. 1).

Рис. 1. Основные угрозы информационной безопасности для пользователей Интернет, %

Значительная доля респондентов дает средние и низкие оценки нанесения ущерба информационной безопасности (табл. 1). Это объясняется скорее тем, что в исследуемый период пользователи, либо не обладали ценной конфиденциальной информацией, либо уровень их технического оснащения был достаточно высок.

Таблица 1

Оценка пользователями ущерба, нанесенного в результате использования ресурсов информационных технологий, %

Перечень угроз	оценка ущерба				всего
	высокий	средний	низкий	нет	
Атаки на базовые узлы сетей, которые могут вызвать нарушение их работоспособности	14	50	28	8	100
Компьютерные вирусы	20	38	34	8	100
Взлом систем защиты с внедрением вредоносных программ (сниффер, rootkit, keylogger и т.д.);	17	39	37	7	100
Целенаправленная рассылка спама	12	30	43	15	100
Несанкционированное использование виртуальных денег	18	35	38	9	100
Сетевые атаки, на административные привилегии	0	33	42	25	100
Подбор и захват паролей и другой аутентификационной информации	28	18	43	11	100

Борьба с проявлением угроз информационной безопасности респондентов осуществляется посредством использования специализированных средств защиты информации и вычислительной техники. Эффективность такой защиты может быть оценена частотой использования респондентами наиболее распространенных специальных технических средств. Так, более 65% пользователей сети Интернет для обеспечения информационной безопасности применяют антивирусные средства. На втором месте по частоте использования - антиспамовые фильтры (21,7%); на третьем – применение открытых ключей шифрования и де шифрования информации при любом ее перемещении по сети (9,2%). Другие технические средства применяются значительно реже.

В целом, исходя из результатов исследования, авторы делают ряд выводов:

1) спецификой Тюменского региона являются высокие темпы развития рынка информационных технологий;

2) для пользователей сети Интернет основную угрозу информационной безопасности представляют: компьютерные вирусы и атаки на базовые узлы сетей; активизация спама; взлом системы на базе вредоносных программ (черви, троянские программы). Для обеспечения информационной безопасности применяются, в основном, антивирусные средства;

3) достижение высокого уровня информационной безопасности для пользователей сети Интернет представляется реальным, что объясняется, в первую очередь, высоким уровнем развития рынка программного обеспечения в Тюменском регионе;

4) в результате развития информационных технологий, постоянного роста уровня оснащенности и использования ИКТ пользователям сети Интернет необходимо пользователям уделять большее внимание повышению своего образовательного уровня в сфере обеспечения информационной безопасности.

Список литературы

1. Бибик, Л.Н., Дейнеко, С.В., Устинова, О.В. Роль средств массовой информации в современном обществе. [Текст] / Л.Н. Бибик, С.В. Дейнеко, О.В. Устинова // Вестник Челябинского государственного университета. 2014. №24 (353). С. 111-113.
2. Вирен, Г.В. Новые подходы к тематике и контенту информации российских СМИ. [Текст] / Г.В. Вирен / Альянс: Актуальные проблемы журналистиковедения и смежных областей знания: Сб. ст. / Отв. ред. В.И. Черед- ниченко. Краснодар: Кубанский гос. ун-т, 2009. 348 с. С. 23-38.
3. Горева, О.М., Гордиевская, Е.Ф. Общественная безопасность – системообразующий фактор социального самочувствия // Современные проблемы науки и образования. – 2014. – № 4; URL: www.science-education.ru/118-14156
4. Карякин, В.В. Наступила эпоха следующего поколения войн - информационно-сетевых. // Независимое военное обозрение. 22.04.2011. / [Электронный ресурс]. Режим доступа: http://nvo.ng.ru/concepts/2011-04-22/1_new_wars.html
5. Лопатина, Н.В. Информационная культура как условие эффективности социальных технологий. [Текст] / Н.В. Лопатина. М.: МГУКИ, 2002.
6. Лопатина, Н.В., Сладкова, О.Б. Информационная культура мегаполиса: единство многообразия. / [Электронный ресурс]. Режим доступа: http://www.i-nett.com/2012/11/28/kultura-megapolisa.
7. Миронов, С.М. Правда является самый крепкий бастионом в информационных войнах. 02 октября 2008 / Народы России: Единство в многообразии. / [Электронный ресурс]. Режим доступа: http://www.narodru.ru/article19179.html.
8. Панарин, И.Н. Информационная война и выборы. [Текст] М.: Городец, 2003. 416 с.
9. Устинова, О. В. Влияние средств массовой информации на духовно-нравственное развитие общества. [Текст] // Общество и человек. 2014. №2 (8). С. 132-133.
10. Устинова, О.В., Соболев, С.Е. Роль современных информационных технологий в жизни общества. [Текст] / О.В. Устинова, С.Е. Соболев // В сб.: Современные тенденции в образовании и науке сборник научных трудов по материалам Международной научно-практической конференции: в 26 частях. 2013. С. 130-131.
11. Устинова, О.В., Фарахутдинов, Ш.Ф., Дейнеко, С.В. Интернет как транслятор негативных социальных практик. [Текст] / О.В. Устинова, Ш.Ф. Фарахутдинов, С.В. Дейнеко // Историческая и социально-образовательная мысль. 2014. Т. 6. №6-1. С. 209-212.

12. Фарахутдинов, Ш.Ф., Дейнеко, С.В., Устинова, О.В. Роль СМИ в духовно-нравственном развитии общества. // Современные проблемы науки и образования. 2015. №1. / [Электронный ресурс]. Режим доступа: http://www.science-education.ru.
13. Шилова, Н.Н., Устинова, О.В., Дейнеко, С.В. Влияние средств массовой информации на духовно-нравственное развитие общества. [Текст] / Н.Н. Шилова, О.В. Устинова // Вестник Орловского государственного университета. Серия: Новые гуманитарные исследования. 2014. №5 (40). С. 85-87.

Рецензенты:

Силин А.Н., д.соц.н., профессор, Тюменский государственный нефтегазовый университет, г.Тюмень;

Линник Т.Г., д.э.н., профессор, Тюменский государственный архитектурно-строительный университет, г.Тюмень.