УДК [004:32.019.5]:340

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В КИБЕРПРОСТРАНСТВЕ

Ю.С. Дубова

Рассматривается глобальный спектр информационно-коммуникационных технологий, информационной безопасности человека и общества в киберпространстве.

Ключевые слова: информация; Интернет; кибербезопасность.

INFORMATION SECURITY IN CYBERSPACE

Iu.S. Dubova

The article considers the global spectrum of information and communication technologies, personal and human society information security in cyberspace.

Keywords: information; the internet; cybersecurity.

Глобальной тенденцией научно-технического прогресса в последние десятилетия является развитие и широкое применение всего спектра информационно-коммуникационных технологий (ИКТ). Информация становится для любого государства важнейшим стратегическим ресурсом, от рационального использования которого зависит безопасность государства и эффективная реализация намеченного внешнеполитического курса.

Можно выделить следующие основные этапы в информационном развитии общества:

- Первая информационная революция. Изобретение письменности позволило накапливать и распространять исторический опыт, знания и навыки. Цивилизации, освоившие письменность, развивались быстрее других и достигали более высокого культурного и экономического уровня. Например, это были такие страны, как Древний Египет, страны Междуречья, Китай.
- Вторая (середина XVI в.) – изобретение книгопечатания. Стало возможным не только сохранять информацию, но и сделать ее массово доступной. Все это ускорило развитие науки и техники, помогло промышленной революции, книги перешагнули границы стран, что способствовало началу сознания общечеловеческой цивилизации.
- Третья была связана с прогрессом средств связи (конец XIX в.). Появление телеграфа, телефона, радио позволило оперативно и четко передавать информацию на любые расстояния.
- Четвертая (70-е гг. XX в.) – появление микропроцессорной техники, электронно-вычислительных машин. Получают развитие компьютерные технологии, что в значительной степени упрощает процесс хранения и поиска информации.
- Пятым этапом информационной революции можно назвать современный этап развития общества. Он характеризуется развитием информационно-коммуникационных технологий, интеграцией в мировое информационное пространство, информатизацией всех сторон общественной жизни. В связи с этим возникает проблема информационной безопасности.

Под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. В свою очередь, защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности [1, с. 18].

Информация становится жизненно важным стимулом развития общества. Ее влияние используется на различных уровнях общественных отношений – межличностных, межгосударственных, межнациональных. Информация является и стратегически важным товаром. Развитие новейших достижений в области информационно-коммуникационных, психологических технологий требует непрерывного со-

вершенствования комплекса мер по обеспечению информационной безопасности, противодействию киберпреступности и шпионажу.

Данные меры состоят из:

- правовых (законодательных) мер;
- технологических;
- организационных (административных и процедурных) мер;
- технических (физических, аппаратных и программных);
- морально-этических.

Правовыми мерами защиты считаются действующие в стране законы, указы и другие нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее получения, обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя, тем самым, неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей. Правовые меры защиты носят в основном предупреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы [2, с. 3].

К технологическим мерам информационной безопасности можно отнести технологические приемы, основанные на использовании некоторых видов структурной, функциональной, информационной, временной избыточности. Данные меры направлены на уменьшение рисков и верификацию информационной безопасности. Примером может быть резервная копия данных, находящихся на главном сервере, защищенном двойным паролированием, инициализация ответственных операций только при наличии разрешений от нескольких должностных лиц, процедур проверки соответствия реквизитов исходящих и входящих сообщении в системах коммутации сообщений, периодическое подведение общего баланса всех банковских счетов и т. п.

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Они представляют собой меры административного и процедурного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей и обслуживающего персонала с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации [2].

Организационные меры необходимо поддерживать более надежными физическими и техническими средствами, так как им присущи определенные недостатки:

- относительно слабая надежность защиты информации без соответствующей поддержки физическими, техническими и программными средствами (любой регламент организации может быть в любой момент нарушен сотрудниками);
- большой объем формальной деятельности по установке правил и норм регулирования.

Технические средства защиты информации – совокупность физических, аппаратных и программных средств, обеспечивающих информационную безопасность. Они в свою очередь делятся на несколько видов.

К физическим средствам относятся механические, электромеханические, электронные, электронно-оптические, радио- и радиотехнические и другие устройства для воспрещения несанкционированного доступа (входа – выхода), проноса (выноса) средств и материалов и других возможных видов преступных действий.

Аппаратные средства – технические устройства, системы, предназначенные для защиты информации от разглашения, утечки и несанкционированного доступа.

Программные средства защиты информации представляют собой систему специальных программ, реализующих функции защиты конфиденциальной информации в киберпространстве: защита информации от копирования; защита информации от вирусов; программная защита каналов связи.

К морально-этическим мерам защиты относятся нормы поведения, которые традиционно сложились или складываются по мере распространения информационных технологий в обществе. Эти нормы большей частью не являются обязательными, как требования нормативных актов, однако их несоблюдение ведет обычно к падению авторитета или престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т. п.), так и писаные, то есть оформленные в некоторый свод (устав, кодекс чести и т. п.) правил или предписаний [3, с. 98–99].

Проблема обеспечения информационной безопасности в киберпространстве является, таким образом, наиважнейшей для современного общества. Ее недооценка приводит к непредсказуемым социальным, политическим, экономическим и материальным последствиям.

Кроме того, неотъемлемой частью инфраструктуры государств становится сеть Интернет

(глобальные и локальные вычислительные сети), компьютеры, факсы и факс-модемы, волоконно-оптическая связь, электронная почта, разветвленная сеть радио- и спутниковой связи, что значительно увеличивает объемы и скорость информационных обменов на транснациональном уровне [4, с. 56].

Количество нападений на инфраструктуру сети и ее объекты увеличивается. В напряженной международной обстановке террористы пользуются уязвимостью средств защиты киберпространства с целью разрушения и дезорганизации информационной инфраструктуры государств. Например, 12 января 2015 г. "Кибер-халифат" ИГИЛ взломал аккаунты соцсетей Пентагона. Особую иронию взлому придает тот факт, что сообщения с угрозами появились как раз в то время, когда президент США выступал с речью о важности кибербезопасности [5].

Широкое развитие получает не фактор силы, а именно информационный фактор воздействия, или так называемые "информационные войны". Ведущие мировые эксперты в данной области считают, что на данном этапе развития информационных технологий не создана пока надежная система преодоления и нейтрализации опасности, исходящей от информационных войн.

Информационная война является новым видом войны – это действия, предпринимаемые для достижения информационного превосходства и воздействия на информацию и информационные системы противника с одновременной защитой собственных информационных систем и информации.

Новым трендом также становится переход от информационных операций к операциям влияния. Для американцев это связано с изменением типа войны, которую они ведут. Это теперь: а) продолжительная война; б) партизанская война: в партизанских войнах существует достаточно серьезная зависимость от населения; в) следует добавить, что современные войны также зависят от поддержки собственным населением, с этим также связано использование некинетического оружия, которое не убивает [6, с. 78].

Например, гражданская война на Украине провоцирует множество внутренних и внешних информационных конфликтов. К внутренним можно отнести:

- Интерпретацию правительственными СМИ Украины событий на юго-востоке страны.

24 января 2015 г. в "КП в Украине" вышел материал, описывающий новые котлы, подобные иловайскому. Журналисты "Комсомолки" оказались правы: ситуация в дебальцевском направлении становится все мрачнее. Горячие бои начались в направлении Углегорска с 31 января, город превратился практически в руины, силовики контролируют только малую часть Углегорска. В штабе АТО информацию о котле не подтверждали и регулярно рапортовали о том, что к ребятам в Дебальцево силовики могут спокойно добраться [7].

Москва. 17 февраля, 2015 г. Interfax.ru – "В городе Дебальцево во вторник днем продолжается зачистка", заявил "Интерфаксу" замминистра обороны самопровозглашенной Донецкой народной республики Эдуард Басурин.

"Армия ДНР взяла 80 % города, осталось взять только частный сектор и Дебальцево будет полностью под контролем ДНР", – сказал Басурин. Кроме того, он подтвердил, что "ополченцы ДНР планируют отводить тяжелое вооружение от линии соприкосновения одновременно с украинскими военными в тех секторах, где соблюдается перемирие". "Еще в сентябре карта была разбита на сектора, и в тех, где не стреляют, где соблюдается тишина, там постепенно, одновременно с Киевом, должен начаться отвод. Но не по всей линии разграничения единомоментно", – заявил Басурин [8].

- Создание "образа врага" и постоянной угрозы для Киева от ЛНР и ДНР.

"Верховная Рада Украины определяет процедуру признания "ДНР" и "ЛНР" террористами, приняв поправки к ряду законов Украины, определяющие порядок признания организаций террористическими", – сообщило новостное издание Украины. За законопроект проголосовало 270 народных депутатов [9].

- Экономические интересы (нефтегазовая отрасль), ради которых разворачиваются достаточно серьезные информационные кампании.

В 2010 г. правительство Украины выдало американским и европейским компаниям лицензии на разведку сланцевого газа в стране. В 2013 г. Украина также подписала договор о добыче сланцевого газа на Юзовской площади с компанией Shell. Но работы на этом месторождении были приостановлены из-за боевых действий (Юзовская площадь находится на территории Харьковской и Донецкой областей). Однако компания Chevron решила в одностороннем порядке выйти из проекта по освоению Олесской площади [10].

К внешним факторам информационных конфликтов относится:

- Влияние извне на формирование политики Украины.

По сообщениям американских СМИ, "палата представителей конгресса США в понедельник, 23 марта 2015 г., большинством голосов приняла резолюцию, в которой президенту страны Бараку Обаме рекомендуется начать поставки боевого оружия Украине" [11]. За резолюцию проголосо-

вало 348 законодателей, 48 были против. При этом документ поддержали как республиканцы, которых в конгрессе большинство, так и демократы.

- Провокационные заявления стран Запада в отношении РФ как главного агрессора и провокатора нестабильности на Украине.

Примером может быть заявление репортеров авторитетной британской газеты "Guardian" о ситуации вокруг России и Украины. Издание пишет, что "в 2015 г. в российской экономике начнется серьезный кризис, и его масштабы будут зависеть от того, поднимутся ли цены на нефть и снимет ли Запад наложенные на Россию санкции". Кроме того, важным фактором остается и то, как Владимир Путин отреагирует на этот кризис. "Guardian" отмечает, что "россияне приняли этого жесткого лидера, поскольку взамен он дал им стабильность и повышение уровня жизни. Теперь этот "договор" нарушен, однако это вовсе не означает, что Кремль смягчит свою позицию по украинскому вопросу". "Путин, наоборот, может еще больше положиться на национализм и таким образом попытаться укрепить свои позиции, что лишь усугубит рецессию. А это, в свою очередь, окажет серьезное негативное влияние на соседние страны и всю еврозону", – провокационно заявляет британская газета [12].

В итоге можно констатировать, что наряду с политическими, экономическими, правовыми и другими факторами стабильности общества, информационная безопасность и надежность хранения и распространения данных, а также объективная их интерпретация, являются не менее важным приоритетом развития государства на пути движения к демократизации общественных отношений.

Слабость страны – это приглашение к агрессии, национальные интересы страны должна обеспечивать сильная политика во всех областях, которая проявляется в укреплении экономических и политических позиций значительного числа государств и их интеграционных объединений, в совершенствовании механизмов многостороннего управления международными процессами. При этом все большую роль играют экономические, политические, научно-технические, экологические и информационные факторы.

Литература

1. Об информации, информационных технологиях и о защите информации: закон Российской Федерации // Сборник Федеральных конституционных законов и федеральных законов. М., 2006. № 149.
2. *Безмалый В.Ф.* Основы защиты информации / В.Ф. Безмалый. М., 2010.
3. *Кирсанов К.А.* Информационная безопасность / К.А. Кирсанов. М., 2000. С. 98–99.
4. Критерии безопасности информационных технологий / Б. Скородумов // Вестник Ассоциации российских банков. М., 1999. № 5.
5. U.S. military social media accounts apparently hacked by Islamic State sympathizers. URL: http://www.washingtonpost.com/news/
6. *Почепцов Г.Г.* Информационные войны: базовые параметры / Г.Г. Почепцов. М., 2012.
7. Динамическая карта АТО: как менялась ситуация в "дебальцевском котле" день за днем. URL: http://kp.ua/incidents/489441-karta-ato-kak-menialas-sytuatsyia-v-debaltsevskom-kotle-den-za-dnem
8. Армия ДНР сообщила о взятии 80 % территории Дебальцево. URL: http://www.interfax.ru/world/424633
9. Парламент создает законодательную базу, которая определяет процедуру признания организаций террористическими. URL: http://zn.ua/POLITICS/rada-sdelala-pervyy-shag-k-priznaniyu-dnr-i-lnr-terroristami-165171_.html
10. Chevron отказалась от добычи сланцевого газа в Украине. URL: http://gordonua.com/news/money/SMI-Chevron-otkazalas-ot-dobychi-slancevogo-gaza-v-Ukraine-56288.html
11. House of Representatives and Democratic House members urged U.S. President Barack Obama to quickly authorize lethal weapons for Ukraine. URL: http://www.wsj.com/public/page/news-global-world.html/
12. В 2015 году судьбу мировой экономики решит Россия. URL: http://www.theguardian.com/world