ВЛИЯНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА НАЦИОНАЛЬНУЮ БЕЗОПАСНОСТЬ ГОСУДАРСТВА

А.О. Завьялова
(г. Томск, Томский политехнический университет)
e-mail: alena_04011@mail.ru

INFLUENCE OF INFORMATION TECHNOLOGY ON HOMELAND SECURITY

A.O. Zavyalova
(Tomsk, Tomsk Polytechnic University)
e-mail: alena_04011@mail.ru

Abstract: The modern world is a complexly organized system, a space of global information technologies (IT). Information today is the main determinant of society, and the rapid development of IT, which penetrate into all spheres of our life, opens up completely new opportunities for social progress, as well as certain problems and challenges. Since information technologies are widely used in business, politics, and national development, they have become an attractive target for hacker attacks; as well as a very powerful tool which can threaten state's national security.

This paper examines the issue of information technology and its role in homeland security protection, as well as the key problems associated with increasing their influence in the world.

Keywords: informatization, information society, information confrontation, information technology, national security, cyberterrorism.

Сегодня основным содержанием развития человечества считается переход от индустриального общества к постиндустриальной стадии развития в форме информационного общества.

Под информационным обществом понимают общество, в котором производство и потребление информации являются важнейшим видом деятельности, а информация признается наиболее значимым ресурсом, новые информационные и телекоммуникационные технологии становятся базовыми технологиями, а информационная среда наряду с социальной и экологической - новой средой обитания человека.

Информационное общество формируется в процессе информатизации, подразумевающей процесс внедрения информационных технологий во все сферы человеческой деятельности. Информационные технологии используются сегодня практически во всех сферах жизнедеятельности человека и общества и напрямую влияют на национальную безопасность, связанную с защитой жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, а также механизмы ее обеспечения.

В последнее время мы часто сталкиваемся с феноменом «информационного противоборства», целью которого служит завоевание и удержание информационного превосходства над противоборствующей стороной. Оно включает в себя: фабрикацию фактов; замалчивание информации; создание видимости плюралистичности мнений; а также изменение смысла слов и понятий, применяемых в освещении событий. Ярким примером информационного противоборства служит война в Ираке (2003 г.), где Соединенные Штаты создали структуру, разрушившую государственное устройство этой страны.

В условиях информатизации общества проблема обеспечения национальной безопасности не только сохраняется, но и приобретает ряд новых особенностей, связанных с возрастанием роли информации в обществе. Информационные технологии могут как обеспечивать стабильность и безопасность, так и угрожать этим двумя компонентам. С одной стороны, информационные технологии можно использовать для распространения и обмена идеями и стратегиями в области безопасности, для организации помощи в миротворческих миссиях, а также для осуществления и координации планов и операций по обеспечению безопасности. Они являются важной составляющей всех государственных операций по обеспечению без-

опасности, от сбора разведывательной информации до командования и контроля. Однако, с другой стороны, информационные технологии могут быть использованы таким образом, чтобы угрожать стабильности и безопасности государства. Противник может уничтожить коммуникационные системы при помощи физического оружия (бомбы, ракеты) и электромагнитного оружия (ЭМО); использовать средства массовой информации (СМИ) для распространения лжи по всему миру; а также проникнуть или атаковать компьютерные сети с целью получения секретной информации или повреждения данных и систем.

Глобальное использование информационных технологий, с одной стороны, приводит к зависимости национальной безопасности государства от защищенности информационной инфраструктуры. С другой стороны, решающее значение для национальной безопасности имеет уровень развития информационной инфраструктуры, который должен обеспечивать эффективность проведения государственной политики (обеспечение органов государственной власти полной и достоверной информацией; обеспечение современных информационных отношений в сфере бизнеса; реализация эффективного механизма включения информационного ресурса в хозяйственный оборот; обеспечение прав граждан на информацию и др.).

Информационные технологии оказывают существенное влияние и на характер угроз национальной безопасности. Данное явление четко прослеживается в развитии такой серьезной угрозы как международный терроризм. Террористические организации используют сегодня широкий спектр информационных технологий в процессе планирования и осуществления своих акций. Так, например, террористы Аль-Каиды манипулируют СМИ и Интернетом для вербовки сторонников из всемирной мусульманской диаспоры. Для них стратегическая пропаганда является неотъемлемым компонентом в кампании по ведению асимметричной войны. Таким образом, можно утверждать, что сегодня действия террористов все более перемещаются из силового поля в информационное.

В последнее время в обиходе начал широко использоваться термин кибертерроризм, т.е. террористические действия в виртуальном пространстве. Кибертерроризм включает в себя операции, которые компрометируют, наносят ущерб и уничтожают информацию, хранящуюся в компьютерных сетях; компьютерные вторжения и использование сетевых «снифферов» (Sniffers) для прослушки телефонов; использование вредоносного программного обеспечения, а именно компьютерных вирусов, червей и троянских коней. К ним относятся атаки типа «отказ в обслуживании» (DoS), которые останавливают или нарушают работу сетевых компьютеров, и «дефейс» (Deface), при которой страница веб-сайта заменяется на другую (как правило, вызывающего вида: реклама, предупреждение, угроза и т.д.).

Растущая угроза кибератак может быть связана с тенденциями и развитием информационных технологий. Основными тенденциями служат: распространенность, мобильность, инструменты взлома, уязвимость и безопасность.

Распространенность

Информационные технологии становятся все более всеобъемлющими и взаимосвязанными. Они распространяются по всему миру и интегрируются во всё возможное: от приборов и транспортных средств до процессов и инфраструктур. Автоматизация и подключение растут стремительными темпами, чему способствуют достижения в области вычислительной техники и телекоммуникационных технологий.

Данная тенденция к вездесущности усугубляет проблемы информационной безопасности. Увеличивается число преступников, целей, а также возможностей использовать, разрушать и саботировать системы.

Мобильность

Информация и информационные технологии становятся все более мобильными. Люди и устройства могут находиться где угодно, программное обеспечение и данные могут храниться и передаваться в любом месте и в любое время через электронную почту, Интернет и одноранговые сети.

Мобильность, как правило, затрудняет процесс защиты информации. Она расширила периметр сетевой безопасности от рабочего места до домов, аэропортов и гостиничных номеров. Информация, ограниченная офисными сетями, может попасть на домашние ПК, портативные компьютеры и карманные устройства, которые физически могут быть менее защищены. Каждый год десятки тысяч ноутбуков объявляются потерянными или украденными, многие из которых имеют конфиденциальную информацию, в том числе государственную секретную информацию.

Инструменты взлома

Инструменты и методы, используемые для атаки на компьютерные сети, становятся все более многочисленными. Они доступны на различных веб-сайтах. По некоторым оценкам, в настоящее время существует более 60 000 компьютерных вирусов.

Инструменты взлома стали более мощными, поскольку разработчики основываются на работе друг друга и программируют свои собственные знания в инструментах. Червь Nimda объединяет функции нескольких предыдущих вирусов и червей, чтобы создать мощный червь, который будет распространяться по четырем каналам: электронная почта, загрузка через Интернет, совместное использование файлов и активное сканирование для заражения уязвимых веб-серверов.

Уязвимость

Поскольку информационные системы становятся «умнее» и «похожими на нас», они также могут стать более уязвимыми для атак. Люди пронизаны уязвимостями. Мы можем быть ограблены, убиты, обмануты и подкуплены.

Суть в том, что у нас никогда не будет безопасных систем. Основная технология всегда будет иметь уязвимости. Кроме того, инсайдеры, имеющие доступ к информации, будут совершать умышленные действия шпионажа и саботажа. Таким образом, важным компонентом любой программы безопасности является способность обнаруживать и реагировать на возникающие бреши в безопасности.

Безопасность

Технологии обеспечения безопасности значительно продвинулись в таких областях, как криптография, биометрия, обнаружение вторжений, антивирусная защита, сканирование уязвимостей и др. Кроме того, многие компании сегодня предлагают услуги по управлению информационной безопасностью, включая удаленный мониторинг уязвимостей и вторжений. Хотя эти достижения, несомненно, помогли предотвратить многочисленные атаки, в целом они не справились с растущей угрозой.

Технологии обеспечения безопасности, в особенности те, которые скрывают информацию, также стали находкой для преступников и террористов. В марте 2000 года Джордж Тенет, тогдашний директор Центральной разведки, сообщил, что «террористические группы, в том числе «Хизбалла», ХАМАС, Организация Абу Нидаля (ОАН) и «Аль-Каида», используют компьютеризированные файлы, электронную почту и шифрование для поддержки своих операций».

Хотя технологии обеспечения информационной безопасности могут расстроить все планы в борьбе с терроризмом, они также играют ключевую роль в защите важнейших информационных инфраструктур.

Таким образом, если подобные тенденции продолжатся, мы можем ожидать больше нападений и больше массовых атак. Многие из этих атак будут финансово мотивированы. Они будут осуществляться преступниками-одиночками, а также террористическими группами, которые хотят финансировать свою деятельность. Атаки могут включать в себя банковское мошенничество, мошенничество с кредитными картами, вымогательство, кражу интеллектуальной собственности. Помимо прямых и косвенных издержек для жертв, эти преступления могут подорвать доверие к Интернету и электронной торговле, что в конечном итоге скажется на экономике.

Таким образом, особенностью современного общества является рост влияния информации и информационных технологий на все сферы жизни, а также перемещение центра борьбы в информационную область. Информация и информационные технологии становятся все более распространенными, мобильными и уязвимыми. Поэтому проблема обеспечения национальной безопасности в условиях информатизации общества становится еще более актуальной.

ЛИТЕРАТУРА

1. Бокстетте К. Террористы используют информационные технологии // per Concordiam. - 2010. - Т. 1. - С. 10-19.

2. Ветров К.В. Вопросы национальной безопасности в условиях информационного общества // Системы безопасности. - 2005. - № 1. - С. 28-29.

3. Дятлов С., Селищева Т., Марьяненко В. Информационно-сетевая экономика: структура, динамика, регулирование. - СПб.: Астерион, 2008. - 15 с.

4. Туронок С.Г. Терроризм в современном мире // Общественные науки и современность. - 2011. - № 4. С. 131-140.

5. George J. Tenet, Director of Central Intelligence, Statement Before the Senate Foreign Relations Committee on The Worldwide Threat in 2000: Global Realities of Our National Security, March 21, 2000.

6. Peter Mell, “Understanding the World of Your Enemy with I-CAT (Internet-Categorization of Attacks Toolkit),” Proceedings of the 22nd National Information Systems Security Conference, U.S. Dept. of Commerce, National Institute of Standards and Technology, Gaithersburg, MD, pp. 432-443.

ИНВЕСТИЦИОННЫЕ ИНСТРУМЕНТЫ ПРОГРАММЫ «ЦИФРОВАЯ ЭКОНОМИКА РОССИЙСКОЙ ФЕДЕРАЦИИ»

В.В. Зайцева, Е.Ю. Калмыкова
(г. Томск, Томский политехнический университет)
e-mail: Zaitseva_1205@rambler.ru, katerinapro@mail.ru

INVESTMENT THE TOOLS OF THE «DIGITAL ECONOMY OF THE RUSSIAN FEDERATION»

V.V. Zaitseva. E.Y. Kalmykova
(Tomsk, Tomsk Polytechnik University)

Abstract: the current stage of development of the Russian economy is associated with the introduction of digital technologies: services for the provision of online services, electronic payments, Internet Commerce, crowdfunding, blockchain, etc. The emergence of such software and financial technologies leads to the need for new tools to attract investment, which enable investors to receive income from investments much faster.

Keywords: digital economy, digitalization, investment tools, blockchain, crowdfunding,

1 Особенности внедрения программы «Цифровая экономика Российской Федерации» на предприятии

Цифровая экономика (интернет-экономика, новая экономика или веб-экономика) — это система экономических, социальных и культурных отношений, основанных на использовании цифровых технологий [1].

1 декабря 2016 Президент РФ в своем послании Федеральному собранию предложил: «запустить масштабную системную программу развитию экономики». 28 июля 2017 г. вы-