УДК [174:342.738]:004.056

О.В. Турута
Харьковский национальный университет радиоэлектроники
к.ю.н., доц. каф. философии, доцент

О.О. Жидкова
Харьковский национальный университет радиоэлектроники
ст. преподаватель каф. философии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ЧЕЛОВЕК, ОБЩЕСТВО, ГОСУДАРСТВО

В статье рассматривается и обозначается класс новых видов угроз и опасностей, связанных с применением новейших технологических средств. Среди них – искажение информации, фальсификация реальности виртуальными мирами, манипулирование сознанием людей, подмена целей и образа жизни навязанными стандартами. Акцентируется внимание на том, что наряду с позитивными результатами процесса использования информационных технологий уже проявились достаточно серьезные негативные эффекты, такие как «цифровое неравенство», компьютерная преступность, компьютеромания, формирование «машинного» стиля мышления, снижение у людей интереса к реальному миру. Поэтому, проблема обеспечения информационной безопасности является приоритетной среди других проблем национальной безопасности, носит всеобщий характер, касается всех: человека, общества, государства.

Ключевые слова: информационные технологии, информационная безопасность, информационно-психологическая безопасность.

Е.В. Турута, О.О.Жидкова
ІНФОРМАЦІЙНА БЕЗПЕКА: ЛЮДИНА, СУСПІЛЬСТВО, ДЕРЖАВА

У статті розглядається і позначається клас нових видів загроз і небезпек, пов'язаних із застосуванням новітніх технологічних засобів. Серед них - спотворення інформації, фальсифікація реальності віртуальними світами, маніпулювання свідомістю людей, підміна цілей і способу життя нав'язаними стандартами. Акцентується увага на тому, що поряд з позитивними результатами процесу використання інформаційних технологій вже проявилися досить серйозні негативні ефекти, такі як «цифрова нерівність», комп'ютерна злочинність, комп'ютероманія, формування «машинного» стилю мислення, зниження у людей інтересу до реального світу. Тому, проблема забезпечення інформаційної безпеки є пріоритетною серед інших проблем національної безпеки, має загальний характер, стосується всіх: людини, суспільства, держави.

Ключові слова: інформаційні технології, інформаційна безпека, інформаційно-психологічна безпека.

O.V. Turuta, O.O. Zhidkova
INFORMATION SECURITY: HUMAN, SOCIETY, STATE

Class of new kinds and dangers connected with application of new technological means are considered in this article. Among them are informational misrepresentation, falsification of reality by virtual world, manipulation of human minds, substitution of goals and life by force standards. Alongside with positive results of process of use of informational technologies there are serious negative effects such as "digital inequality", computer crime, computer addiction, creation of machine style of communication, decreasing of interest in real world. That's why problem of provision of

informational safety has priority among other problems of national safety, bears common character and concerns everyone: person, society and state.

Key words: informational technologies, informational safety and informational-psychological safety.

Единое планетарное сообщество сегодня становится реальностью. В обеспечении жизнедеятельности новой цивилизации особая роль принадлежит информации и знаниям, стабильность ее функционирования определяется качеством информационно-технологических решений. В тоже время данный процесс обладает двойственным характером: устойчивое развитие социума уже немыслимо без целенаправленной глобальной информатизации, с одной стороны, и повышением степени уязвимости социальных объектов от информационного воздействия – с другой.

Сегодня во всех сферах жизнедеятельности общества четко обозначился класс новых видов угроз и опасностей, связанных с применением новейших технологических средств. Среди них – искажение информации, фальсификация реальности виртуальными мирами, манипулирование сознанием людей, подмена целей и образа жизни навязанными стандартами, хакерство, пиратство и разработка вирусных программ, сбор различной информации без ведома лиц и компаний, о которых эта информация собирается, анонимность воровства, игромания, информационные войны и т. д.

Таким образом, наряду с позитивными результатами процесса использования информационных технологий уже проявились достаточно серьезные негативные эффекты, такие как «цифровое неравенство», компьютерная преступность, компьютеромания, формирование «машинного» стиля мышления, снижение у людей интереса к реальному миру. Человеческая деятельность, включая работу, досуг, социальные контакты и т.д. основанная в большей степени посредством телекоммуникаций, будет базироваться скорее на представлениях о действительности, чем на самой реальности, что порождает психологические проблемы, техностресс.

Созданное глобализацией общее информационное пространство размывает основы идентичности, ведет к потере отдельными странами своей автономности. Также, масштабное внедрение информационных технологий привели к трансформации системы ценностей, современное общество испытывает глобальный ценностный кризис. В подобных условиях совершенно очевидно, что роль информационной безопасности неизмеримо возрастает. Массовое внедрение информационных технологий должны сопровождаться оперативным контролем и гибкой реакцией на негативные социальные последствия.

Украинское государство включено в процесс всеобщей информатизации общества и формирования единого мирового информационного рынка. Такие преобразования привели к тому, что в настоящее время все более актуальный характер приобретает обеспечение информационной безопасности Украины как неотъемлемого элемента ее национальной безопасности, а защита информации превращается в одну из приоритетных государственных задач. Проблема создания и поддержки защищенной среды информационного обмена, которая обуславливает определенные правила и политику безопасности современного государства, является весьма актуальной, поскольку сегодня главным стратегическим национальным ресурсом, основой экономической и оборонной мощи государства становится информация и информационные технологии. Информация в современном мире является таким атрибутом, от которого в определяющем плане зависит эффективность жизнедеятельности современного общества. Информационные технологии принципиально изменили объем и важность информации, которая вращается в

технических средствах ее хранения, обработки и передачи. Всеобщая компьютеризация основных сфер деятельности привела к появлению широкого спектра внутренних и внешних угроз, нетрадиционных каналов потери информации и несанкционированного доступа к ней.

Информационная сфера Украины – это единое информационное пространство, которое формируется государственными органами, общественными, политическими и социальными организациями, а также гражданами и функционирует на основе правовых, организационных, научно-технических, экономических, финансовых, методических, гуманитарных и нравственных принципов с учетом требований и задач национальной информационной безопасности Украины.

Информационная безопасность является одним из видов национальной безопасности. Поскольку Проект Концепции информационной безопасности Украины и Проект Доктрины информационной безопасности Украины были наработаны Экспертным советом при Министерстве информационной политики Украины, прошли широкое обсуждение специалистами во многих регионах Украины и переданы на рассмотрение правительства, но в настоящее время эти документы так и остаются проектами. Поэтому Закон Украины «Об основных принципах развития информационного общества в Украине на 2007 – 2015 годы» от 09.01.2007 г., который, как ни странно, является действующим на данный момент и, практически единственным нормативным актом, который содержит следующее определение информационной безопасности: «состояние защищенности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесение ущерба из-за неполноты, несвоевременности и недостоверности используемой информации; негативное информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование, нарушение целостности, конфиденциальности и доступности информации» [1].

Политику национальной информационной безопасности нужно проводить только в тех формах и теми методами и средствами, которые присущи и приемлемые демократическому правовому государству, то есть основываются на принципах демократии и верховенства права. Информационное законодательство должно быть направлено на закрепление государственной информационной политики, которая предусматривает обеспечение гарантированного уровня национальной безопасности в информационной сфере, нормального развития информационных технологий и средств защиты информации, исключение монополизма в данной области, предотвращение разработки информационно деструктивных технологий воздействия на общество, защиту авторских и смежных прав и тому подобное. Система обеспечения информационной безопасности Украины создается и развивается в соответствии с Конституцией Украины и другими нормативно-правовыми актами, регулирующими общественные отношения в информационной сфере. Так Закон Украины «Об основах национальной безопасности Украины» различает две ключевые категории, обуславливающие содержание и направленность государственной политики в сфере информационной безопасности:

1) угрозы национальным интересам и национальной безопасности Украины в информационной сфере (ст. 7), к которым относятся:

– проявления ограничения свободы слова и доступа граждан к информации;

– распространение средствами массовой информации культа насилия, жестокости, порнографии;

– компьютерная преступность и компьютерный терроризм;

– разглашение информации, являющейся государственной и иной, предусмотренной законом, тайной, а также конфиденциальной информации, которая

является собственностью государства или направлена обеспечение потребностей и национальных интересов общества и государства;

– попытки манипулировать общественным сознанием, в частности, путем распространения недостоверной, неполной или предвзятой информации;

2) основные направления государственной политики по вопросам национальной безопасности в информационной сфере (ст. 8):

– обеспечение информационного суверенитета Украины;

– совершенствование государственного регулирования развития информационной сферы путем создания нормативно-правовых и экономических предпосылок для развития национальной информационной инфраструктуры и ресурсов, внедрения новейших технологий в этой сфере, наполнения внутреннего и мирового информационного пространства достоверной информацией об Украине;

– активное привлечение средств массовой информации к предотвращению и противодействию коррупции, злоупотреблению служебным положением, другим явлениям, которые угрожают национальной безопасности Украины;

– обеспечение неукоснительного соблюдения конституционных прав на свободу слова, доступа к информации, недопущение неправомерного вмешательства органов государственной власти, органов местного самоуправления, их должностных лиц в деятельность средств массовой информации и журналистов, запрещения цензуры, дискриминации в информационной сфере и преследования журналистов за политические позиции, за выполнение профессиональных обязанностей, за критику;

– принятие комплексных мер по защите национального информационного пространства и противодействию монополизации информационной сферы Украины [2].

Закон «Об основах национальной безопасности Украины» предусматривает разработку нескольких программных документов, которые должны определять конкретные направления проведения государственной политики безопасности в различных сферах. Одним из таких ключевых документов в сфере информационной безопасности является Стратегия национальной безопасности Украины, утвержденная Указом Президента Украины от 26 мая 2015 № 287/2015. Она определяет принципы, приоритетные цели, задачи и механизмы обеспечения жизненно важных интересов личности, общества и государства от внешних и внутренних угроз. Эта Стратегия является базой для разработки конкретных программ, проектов и планов мероприятий государственной политики национальной безопасности в информационной сфере и механизмов их реализации. Главной целью Стратегия определяет обеспечение такого уровня национальной безопасности, который бы гарантировал поступательное развитие Украины, ее конкурентоспособность, обеспечение прав и свобод человека и гражданина, дальнейшее укрепление международных позиций и авторитета Украинского государства в современном мире [3]. Одной из составляющих этой задачи является и обеспечение информационной безопасности. Стратегия национальной безопасности Украины среди угроз информационной безопасности Украины определяет:

– ведение информационной войны против Украины;

– отсутствие целостной коммуникативной политики государства, недостаточный уровень медиа-культуры общества [3].

Стратегия национальной безопасности Украины также определяет угрозы кибербезопасности и безопасности информационных ресурсов:

– уязвимость объектов критической инфраструктуры, государственных информационных ресурсов к кибератакам;

– физическая и моральная устарелость системы охраны государственной тайны и других видов информации с ограниченным доступом [3].

Поэтому приоритетами государственной политики обеспечения информационной безопасности Украины являются:

– обеспечение наступательности мероприятий политики информационной безопасности на основе асимметричных действий против всех форм и проявлений информационной агрессии;

– создание интегрированной системы оценки информационных угроз и оперативного реагирования на них;

– противодействие информационным операциям против Украины, манипуляциям общественным сознанием и распространению искаженной информации, защита национальных ценностей и укрепление единства украинского общества;

– разработка и реализация скоординированной информационной политики органов государственной власти;

– выявление субъектов украинского информационного пространства, созданных и / или используемых для ведения информационной войны против Украины, и невозможность их подрывной деятельности;

– создание и развитие институтов, отвечающих за информационно-психологическую безопасность;

– совершенствование профессиональной подготовки в области информационной безопасности, внедрение общенациональных образовательных программ по медиакультуре с привлечением гражданского общества и бизнеса [3].

Соответственно приоритетами обеспечения кибербезопасности и безопасности информационных ресурсов являются:

– развитие информационной инфраструктуры государства;

– создание системы обеспечения кибербезопасности, развитие сети реагирования на компьютерные чрезвычайные события (CERT);

– мониторинг киберпространства с целью своевременного выявления, предотвращения киберугроз и их нейтрализации;

– развитие способностей правоохранительных органов по расследованию киберпреступлений;

– обеспечение защищенности объектов критической инфраструктуры, государственных информационных ресурсов от кибератак;

– реформирование системы охраны государственной тайны и иной информации с ограниченным доступом, защита государственных информационных ресурсов, систем электронного управления, технической и криптографической защиты информации;

– создание системы подготовки кадров в сфере кибербезопасности для нужд органов сектора безопасности и обороны;

– развитие международного сотрудничества в сфере обеспечения кибербезопасности для усиления возможностей Украины в сфере кибербезопасности [3].

Все составляющие информационной безопасности являются системообразующими в других видах безопасности, таких как социальная, оборонная, экономическая и экологическая безопасность. Решению проблем обеспечения информационной безопасности так же способствует формирование новой информационной культуры в обществе. Информационная культура является важнейшим фактором преодоления и дальнейшей элиминации негативных эффектов информатизации, а также гуманистической ориентации данного процесса.

Информатизация общества и имманентно связанная с ней информационная безопасность обрели глобальные масштабы и превратились в фактор, влияющий на выживание человечества в условиях формирования единого мирового информационного пространства. Недооценка вопросов информационной безопасности может привести к трудно предсказуемым социальным, политическим, экономическим,

военным и другим последствиям. Поэтому сегодня назрела необходимость формирования системы глобальной информационной безопасности, а так же информационной культуры общества как составляющих всей системы общемировой безопасности.

Острота этой проблемы в сложившейся ситуации вызвана в значительной мере утратой гуманистических нравственных ценностей, идеалов и подчинением морали политико-идеологическим интересам. Роль этических норм в системе безопасности информационных технологий становится центральной для выживания и развития общества. Решающее значение в данной ситуации приобретает техническая грамотность, культура и этика поведения человека, которые должны соответствовать существующей модели информационной безопасности.

Важность института информационной безопасности способствовала появлению новой отрасли знаний – «информационной этики». Этот термин стал употребляться учеными и специалистами по компьютерной этике и смежным дисциплинам с 2002-го года. Информационная этика занимается изучением природы социального воздействия компьютерных технологий на общество, формированием на этой основе моральных норм и проведение политики их внедрения в сознание разработчиков и пользователей компьютерных технологий. Информационная этика – обширная дисциплина, включающая в себя профессиональную этику, потребительскую этику и некоторые вопросы политики государства. Естественно, что первоначально она возникла как элемент профессиональных знаний и культуры в области информационных технологий.

На сегодня 90% всех технологий, влияющих на уровень профессиональной этики любой отрасли знаний, связаны с информацией, т. е. с ее сбором, передачей, обработкой, хранением, техническими средствами и пр. Это обстоятельство определяет повышенный уровень требований к специалистам – программистам, системным администраторам, и, конечно, к аналитикам, связанным с информационно-аналитическим обеспечением безопасности. Поэтому вопросы профессиональной этики в современном обществе приобретают информационный оттенок, причем эта тенденция будет сохраняться [4].

Информационная этика выходит на первый план в свете обеспечения безопасности использования информационных технологий, повышения культуры на основе усвоения достигнутого человечеством, для информирования каждого субъекта о его правах и обязанностях в информационном сообществе, ответственности за использование информационно-компьютерных технологий и иных форм информации; формирование информационного общества создает новые информационно-этические проблемы: компьютерная преступность, манипулирование при помощи информационных технологий, воспитание технократического мышления, регулирование киберпространства, вопросы клонирования и генной инженерии. Все, что относится к теме обеспечения безопасности на всех уровнях использования информационных технологий, формирует задачи и решения этического характера.

Саморегуляция на основе нравственных норм является одним из естественных и эффективных способов защиты от антисоциального поведения участников информационного взаимодействия. Это связано с тем, что такой вид социальных норм, как нормы морали, является универсальным регулятором общественных, поскольку способен регулировать практически все существующие в обществе отношения (в отличие от правовых норм). В перспективе выработанные обществом нормы морали могут стать базой для формирования новых и совершенствования существующих правовых норм, обеспечиваемых силой государственного воздействия. Таким образом, обогатившись новым содержанием, адекватным новой реальности информационного общества, этические нормы могут стать гарантией обеспечения информационной

безопасности личности и общества. Именно они определяют границы должного и возможного поведения.

Социальные отношения в условиях информатизации общества складываются и изменяются непривычно быстро. Общество должно научиться адекватно реагировать на эти изменения, приводя социальные отношения в соответствии с реалиями, предупреждая появление нежелательных для общества процессов. Для государства важно иметь современную концепцию вхождения в информационное общество. Она должна принципиально отличаться от концепций предыдущих периодов развития государства, которые были ориентированы в первую очередь на техническое обеспечение общественных процессов. Теперь на первое место вышли вопросы социального характера, в их числе и проблемы информационной безопасности. Самая важная задача для государства на законодательном уровне – создать механизм, позволяющий согласовывать процесс разработки законов с прогрессом информационных технологий. Естественно, законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике помимо прочих отрицательных моментов это ведет к снижению информационной безопасности.

В течение последних десятилетий информация приобрела статус одного из важнейших национальных ресурсов, определяющих экономический, научно-технический и оборонительный потенциал страны. Под воздействием информатизации все сферы жизни общества получили новые качества – оперативность, гибкость и динамичность. В современных условиях проблемы информационного обеспечения во всех сферах деятельности по своей значимости и актуальности превосходят проблемы дальнейшей интенсификации производства, которые до недавнего времени считались одними из главных.

Высокие информационные технологии в настоящее время не просто сопутствуют и обеспечивают труд ученых и инженерно-технических работников, политических и военных деятелей, представителей искусства и образования, но, насквозь пронизывая всю жизнь общества, они являются определяющими условиями эффективной деятельности людей и всеобщего прогресса. Вместе с тем информационные технологии, как никакие другие, уязвимы и подвержены внешним и внутренним негативным воздействиям. Ущерб от таких воздействий, измеряемый натурными показателями потерь (экономических, социально-политических, военных), может быть сколь угодно велик.

Отсюда следует, что проблема обеспечения информационной безопасности является приоритетной среди других проблем национальной безопасности. Важно отметить, что проблема обеспечения информационной безопасности носит всеобщий характер, она касается всех: человека, общества, государства. Включает в себя не только организационно-технические вопросы, но и втягивает в свою орбиту правовые и социальные аспекты, а также задачи обеспечения информационно-психологической безопасности.

На уровне человека информационная безопасность должна обеспечить защищенность психики и сознания людей от опасных информационных воздействий: манипулирования, дезинформирования, побуждения к самоубийству. На уровне общества и государства информационная безопасность призвана обеспечить защищенность и, как следствие, устойчивость основных сфер жизнедеятельности (экономики, науки, сферы государственного и военного управления, а также общественного сознания) от опасных, дестабилизирующих и деструктивных информационных воздействий.

ПЕРЕЧЕНЬ ССЫЛОК

1. Закон Украины "Об основных принципах развития информационного общества в Украине на 2007-2015 годы" [Электронный ресурс]: документ от 9 января 2007 г. Режим доступа: www. URL: http://zakon3.rada.gov.ua/laws/show/537-16.
2. Закон Украины "Об основах национальной безопасности Украины" [Электронный ресурс]: документ от 19 июня 2003 г. Режим доступа : www. URL: http://zakon3.rada.gov.ua/laws/show/964-15.
3. Указ Президента Украины "О решении Совета национальной безопасности и обороны Украины от 6 мая 2015 года "О Стратегии национальной безопасности Украины" [Электронный ресурс]: документ от 6 мая 2015 г. Режим доступа: www. URL: http://zakon5.rada.gov.ua/laws/show/287/2015.
4. Минозов А.С. Профессиональная этика специалиста в области безопасности бизнеса / Под ред.Л.М. Кунбутаева. М.: Инд. МЭИ, 2005.