УДК: 930.1 (575.2) (04)

Шарипова Э.К.,
философия илимдеринин доктору, профессор
Шарипова Э.К.,
доктор философских наук, профессор
Sharipova E.K.,
doctor of philosophical sciences, professor

Камбарова Н. Н.,
изденүүчү
Камбарова Н. Н.
соискатель
Kambarova N. N.
competitor

Ош мамлекеттик университети
Ошский государственный университет
Osh State University

МААЛЫМАТТЫК КООПСУЗДУК: МАҢЫЗЫ ЖАНА КОРКУНУЧТАР
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СУЩНОСТЬ И УГРОЗЫ
INFORMATION SECURITY: ESSENCE AND THREATS

Аннотация. Бул макалада маалыматтык коопсуздук туруктуу социалдык өнүгүүнүн маанилүү фактору жана реалдуу тарыхый феномен катары каралат. Глобалдык маалыматтык тармактын функциялануу өзгөчөлүктөрү, маалыматты социалдаштыруу жана персоналдаштыруу, бирдиктүү глобалдык маалыматтык агымга социалдык-маданий жана цивилизациялык биригүү коом, инсан үчүн маалыматтык тобокелдерди жаратат, ал адамдын социумдан жана маалыматтык кайра түзүүлөрдөн алысташынан көрүнөт.

Негизги сөздөр: *к*оопсуздук, маалыматтык коом, маданият, цивилизация, ааламдашуу, тобокел, коркунуч, обочолонуу.

Аннотация. В данной статье информационная безопасность личности исследуется как важный фактор устойчивого социального развития и реальный исторический феномен. Особенности функционирования глобальной информационной сети, социализация и персонализация информации, социально-культурное и цивилизационное слияние в единый глобальный информационный поток порождают информационные риски для общества и личности, что выражается в отчуждении человека от социума и информационных новообразований.

Ключевые слова: безопасность, информационное общество, культура, цивилизация, глобализация, риск, угроза, отчуждение

Abstract. in this article, the information security of the individual is studied as an important factor in sustainable social development and a real historical phenomenon. Features of the functioning of the global information network, socialization and personalization of information, socio-cultural and civilizational merging into a single global information flow generate information risks for society and the individual, which is expressed in the alienation of a person from society and information neoplasms.

Keywords: security, information society, culture, civilization, globalization, risk, threat, alienation

Информационная безопасность представляет собой сложный, многогранный и многоуровневый феномен. Безопасность можно представить как ощущение безопасности на повседневном уровне в обыденной, привычной жизни, как отсутствие какой-либо внешней опасности по отношению к кому-либо, как состояние защищенности жизненно важных интересов личности, общества, государства от внутренних и внешних угроз, либо способность предмета, явления или процесса сохраняться при разрушающих воздействиях [1]. С правовой точки зрения она представляет собой государственную доктрину информационной безопасности, определяющую конституционные условия информационной безопасности государства. Существуют также социально-психологические аспекты информационной безопасности [2].

Безопасность как понятие характеризуется и как состояние некоторой системы, и как психологическое ощущение, и как идея или концепция, и как определенные меры, направленные на достижение данного состояния [3, с. 98].

В научном мире информация вполне обоснованно считается стратегическим национальным ресурсом. Политический вес страны, ее возможности влиять на мировые события зависят не только от вещественно-силовых факторов, но во все возрастающей мере от факторов информационных (возможности эксплуатировать интеллектуальный потенциал других стран, распространять и внедрять свои духовные ценности, культуру, язык, а также тормозить духовно-культурную экспансию других народов, трансформировать и даже подрывать их духовно-нравственные устои). В соперничестве и противоборстве государств, в реализации их политических планов происходит явное смещение центра тяжести с открытых силовых методов и средств к скрытым и более «тонким» информационным методам и средствам, подаваемым как следствия процессов глобализации.

В этих условиях роль информационной безопасности все более возрастает. Чем выше уровни интеллектуализации и информатизации общества, тем более значимой становится его информационная безопасность, поскольку реализация интересов, целей государств и народов все больше осуществляется посредством информационных, а не вещественно-энергетических воздействий.

Информация – не только мощный двигатель общественного прогресса, фактор многократного усиления совокупного потенциала государства, но и действенный инструмент манипулирования общественным сознанием. Речь идет о том, что не только сами государства, но и отдельные социально-политические силы внутри них, используя монополию на средства массовой информации, не знающие государственных границ и многих ограничений по расстоянию, способны формировать у широких масс определенные идеологические установки, оценки, настроения, ценностные ориентиры поведения.

Во многих странах для обеспечения информационной безопасности созданы специальные службы, которым выделяются значительные финансовые средства, развернута подготовка соответствующих специалистов. Достижения в области информатизации постоянно совершенствуются. Сегодня уже создано так называемое «информационное оружие», под которым понимаются устройства и средства, предназначенные для нанесения противоборствующей стороне максимального урона путем опасных информационных воздействий. Существует два типа такого оружия – информационно-техническое и информационно-психологическое. При использовании оружия первого типа (компьютерные вирусы, логические бомбы, программные закладки и т. п.) главными объектами воздействия являются информационно-технические системы (системы связи, телекоммуникационные системы, банки и т. д.). Примеров разрушения информационных ресурсов и телекоммуникаций, несанкционированного доступа к

ним, попыток хищения конфиденциальной информации или ее уничтожения в хорошо защищенных компьютерах – множество. С полным основанием можно говорить, что сегодня террористы и шпионы, мафия и хакеры полностью освоились в глобальных компьютерных сетях, шантаж и угрозы информационных диверсий стали привычным делом.

При воздействии информационно-психологического оружия главными объектами являются индивидуальная психика и общественное сознание. Цель такого воздействия – подрыв духовного, морально-психологического потенциала страны-конкурента и подготовка почвы для политико-экономического проникновения.

В настоящее время информация становится одним из главных рычагов в противостоянии на международной арене за новый передел мира в целях установления господства ведущих государств в глобальном информационном пространстве. В научном мире информация вполне обоснованно считается стратегическим национальным ресурсом.

С каждым годом информация в современном мире становится всё более доступной. С одной стороны, это может быть признано неоспоримым преимуществом: государство получает доступ к новейшим зарубежным технологиям и разработкам, а организациям обеспечивается возможность получения ценных сведений о конкурентах. Но, с другой стороны, свободно циркулирующая информация может оказаться заведомо ложной или искажённой, ставящей целью ввести в заблуждение её потенциальных пользователей. Последнее ведёт к девиациям общественного сознания, попыткам манипулировать им в сомнительных интересах разнородных политических и идеологических структур.

Кроме того, доступность информации привела к появлению одной из самых значимых проблем нашей современности - информационной избыточности или перенасыщению информацией. В случае переизбытка информации пользователь может либо анализировать сведения, поступающие к нему из различных источников, либо принимать в качестве достоверной наиболее примитивную информацию, изложенную самым простым языком. В таких условиях очевидной является потребность в критической рефлексии или, как минимум, в сомнении в качестве любой получаемой информации.

Следует также признать, что наибольшую угрозу информационной безопасности государства в эпоху глобализации, представляет собой возможность осуществления нового вида катастроф, наступающих по причине сбоев или нарушений в глобальных информационно-телекоммуникационных сетях.

Как следствие, возможности новой информационно-цифровой эпохи расширяются не только у конструктивных, но и у разного рода террористических и экстремистских организаций. Последние активно используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание. В результате нарастает межнациональная и социальная напряжённость, происходит эскалация конфликтов по разным основаниям, разжигаются этническая и религиозная ненависть и вражда. Опасность информационного терроризма зачастую недооценивается, в результате чего, граждане порой и сами не осознают, что становятся его жертвами.

Информационный терроризм предполагает особое психологическое воздействие на сознание человека с помощью ресурсов информационной сети, которое направлено на внушение требуемых идей, подавляющих собственное мнение, аналитическую способность и логическое мышление индивида [4, с. 113–114]. Основной целью информационных террористов является донесение заведомо ложной информации, которая впоследствии будет восприниматься потерпевшими как абсолютно достоверная. Главная опасность здесь кроется в том, что эта, как правило, негативная информация может повлечь за собой необратимые последствия,

например, пошатнуть целостность государства, привести к смене правительства и пр. Особенно эффективным инструментом террористической пропаганды является обыгрывание социально-политических проблем общества с разжиганием межэтнической и национальной розни.

В настоящее время можно выделить несколько разновидностей информационного терроризма.

Информационно-психологический терроризм. Связан непосредственно с самой информацией и её распространением, т. е. основное давление здесь оказывается на психику человека. Например, для того, чтобы запустить негативный слух в СМИ или интернете, используются методы насилия или подкупа, целью которых являются операторы, разработчики или представители телекоммуникационных систем.

Информационно-технический терроризм. Данный вид связан с нанесением ущерба непосредственно самой технике или с её помощью. Например, создание различных вирусов или помех с помощью других программ с целью разрушения систем управления или перехват управления техническими объектами.

Кибертерроризм. Направлен на выведение из строя компьютерных систем и их взлома, нападения на компьютерные сети.

Кибертеррористический акт, который проводится с помощью различных компьютерных технологий и является при этом политически мотивированным. Как правило, целью всего этого является максимальное привлечение внимания к политическим требованиям, выдвигаемым террористами.

Именно кибертерроризм считается самым опасным и масштабным видом информационных атак, т. к. как его крайне сложно обнаружить и предотвратить. Действия, совершаемые террористом, производятся удалённо через киберпространство. Они могут исходить даже с территории другого государства, что ещё больше усложняет ситуацию с выявлением киберпреступника [5, с. 98]. Таким образом, на сегодняшний день информационный терроризм становится угрозой для всего цивилизованного мира.

Ещё одним опасным последствием доступа террористических организаций к новым информационным технологиям является пропаганда экстремистской идеологии и вербовка в террористические группировки новых сторонников. В основном такими «новобранцами» становятся молодые, эмоционально нестабильные люди с подвижной психикой и неустановившейся системой ценностей. Вербовка молодёжи в экстремистские и террористические организации - одно из самых опасных последствий реализации угрозы информационной безопасности государства, поскольку, в свою очередь, создаёт угрозу всей системе национальной безопасности.

Глобализация имеет как положительное (например, увеличение доступного объёма информации о технологиях и стимулирование разработки российского программного обеспечения), так и отрицательное (например, рост киберпреступлений и зависимость от зарубежных программных продуктов) влияние на информационную безопасность. Приходится констатировать, однако, что современное глобальное информационное пространство представляет собой объект ожесточенной борьбы за информационное превосходство, политические, экономические и сырьевые преимущества, арену постоянного противоборства различных социальных структур. Причем в современных условиях наблюдается тенденция перехода от традиционных - силовых - методов борьбы государств при отстаивании своих национальных интересов к нетрадиционным, в частности информационным средствам воздействия на противника. Фактически речь идет о новом феномене глобализации - информационной войне, которая становится, по существу, новой формой противостояния государств, одним из видов «нетрадиционных» войн нового поколения. Поэтому в условиях стремительного формирования глобального информационного пространства (а также киберпростран-

ства) огромное значение в обеспечении национальной безопасности всех стран приобретает информационная безопасность.

Информационные войны являются частью нынешней информационной реальности. В век глобализации они представляют собой эффективное средство достижения превосходства в различных сферах жизни современного общества: политической, экономической, научно-технической, военной, социальной, духовной. Информационная война - это противостояние борющихся сторон, которые оказывают агрессивное воздействие на информационную инфраструктуру друг друга с целью достижения преимущества и победы над противником. Различают информационно-техническую и информационно-психологическую войну.

Главная цель такой войны заключается в информационном воздействии, которое позволяет без традиционных военных действий добиться победы над противником. Под информационно-психологической войной понимается информационное воздействие на сознание человека. Информационно-психологическое оружие направлено на «переформатирование» сознания людей (путем внедрения чуждых ценностей, традиций и культуры), а через него – на изменение существующей социально-политической системы. Диапазон информационно-психологического оружия чрезвычайно широк – от сокрытия важной информации и ее искажения до полной дезинформации населения. Опасность нового вида оружия заключается в том, что его воздействие приводит в конечном счете к кардинальной трансформации общественного сознания, влечет за собой социальный взрыв и свержение неугодного политического лидера или режима в стране-объекте.

Информационная безопасность государства заключается в создании условий для формирования эффективной информационной среды и информационной инфраструктуры, которые согласно действующему законодательству, Конституции и сложившейся социальной практике обеспечивают реализацию конституционных прав и свобод общества, общественных организаций и граждан в сфере доступа к открытым информационным ресурсам, свободы информационного взаимодействия, получения необходимой информации и пользования ею в целях обеспечения эффективного функционирования государства, сохранения незыблемости конституционного строя, государственного устройства и территориальной целостности, государственного суверенитета, достижения социальной и политической стабильности, защиты государственных информационных интересов и потребностей, обусловленных эффективным функционированием государственных структур, ориентированным на обеспечение законности и правопорядка, мира и согласия, бесконфликтного взаимодействия с гражданским обществом, равноправного и взаимовыгодного внутригосударственного и международного сотрудничества, обеспечивающих гармоничное и динамичное развитие государства.

Одним из главных направлений деятельности по поддержанию информационной безопасности государства является прежде всего защита информации. Защита информации есть системная совокупность государственных мероприятий, ориентированных на обеспечение целостности и конфиденциальности информации и при этом гарантирующих доступность информации общественным организациям и личности. При этом защита информации представляет собой деятельность, направленную на предотвращение утраты информации, несанкционированного проникновения в информационные ресурсы и нецелевого использования информации, в том числе использования с нарушением авторских прав и прав владельцев и собственников информации.

В мероприятия по защите информации включается собственно защита информации и защита прав на пользование и владение информацией, защита от незаконного рас-

пространения информации, от разглашения коммерческой, служебной и государственной информации, защита информационных ресурсов и информационных технологий.

Кроме информации, информационных ресурсов и информационных технологий, объектом защиты являются носители информации, информационные процессы, технические средства информации, системы информационной связи, материальные ресурсы, обеспечивающие информационное взаимодействие и хранение информации, а средствами защиты являются мероприятия правового порядка (указы, акты и нормы, законы, защищающие информацию), специальные действия и государственные акты, направленные на защиту информации, например лицензирование информации, сертификация информационных ресурсов, формулирование стандартов использования информации, а также государственная аттестация процессов информатизации в виде документов соответствия стандартам, различные государственные информационно-технические экспертизы. Итак, в условиях глобализации от надежности обеспечения информационной безопасности зависит национальная безопасность суверенных государств.

Список использованной литературы

1. Безопасность [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Безопасность

2. Грачев, Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты [Текст] / Г.В. Грачев. – М. : Изд-во РАГС, 1998. – 125 с.

3. Заплатинский, М. Терминология науки о безопасности [Текст] / М. Заплатинский // Zbornik prispevkov z medzinarodnej vedeckej konferencie «Bezhecnostna veda a bezpecnostne vzdelanie». – Liptovsky Mikulas : AOS v Liptovskom Mikulasi, 2006. – С. 98–103.

4. Колин, К.К. Информационная цивилизация [Текст] / К.К. Колин. – М.: Ин-т проблем информатики РАН, 2002. – 112 с.

5. Коротков, А.В. Цифровое неравенство в процессах стратификации информационного общества [Текст] / А.В. Коротков // Информационное общество. – 2003. – Вып. 5. – С. 24–35.