REPORTS OF THE NATIONAL ACADEMY OF SCIENCES OF THE REPUBLIC OF KAZAKHSTAN
ISSN 2224-5227
Volume 5, Number 315 (2017), 123 – 130

E.Zh. Aytkhozhaeva, N.A. Seilova

Kazakh National Research Technical University named after K.I.Satpayev, Almaty, Kazakhstan
ait_djam@mail.ru

DIGITAL SOCIETY RISKS

Abstract. Intensive development of information and communication technologies, as a technical basis, led to the creation and development of information society (digital society). Attention is drawn to the risks and threats of new technologies that threaten to the humanistic functioning of the information society: virtualization, cloud computing, Internet-to-Things (IoT), machine-to-machine (M2M), cyberphysical systems, etc. These new technologies improve the quality of life and economic efficiency of business; serve the development of a digital society. But these new technologies are fraught with new risks and threats to the security of citizens, enterprises and the state. The most difficult problems of risks are the problems associated with the human factor: moral, ethical, sociological, psychological problems. A decisive role in solving these problems belongs to digital sociology. One of the main, promising and effective methods, which create a threat to the electronic society, is social engineering. Social engineering is based on unpredictable human factor. The reasons for successful social engineering are indicated. There are different signs of classification of social engineering methods. A classification based on the manipulation of human traits is given. In the digital society the application of social engineering methods is facilitated by the fact that social networks, e-mail, online services are relatively anonymous. It is difficult to define a lie, since there is no direct contact with a person. The results of digital sociology researchers should be a platform for developing effective methods to combat cybercrime.

Key words: digital society, cyberthreats, digital sociology, social engineering.

УДК 316.4

Е.Ж. Айтхожаева, Н.А.Сейлова

Казахский национальный исследовательский технический университет
им. К.И.Сатпаева, Алматы, Казахстан

РИСКИ ЦИФРОВОГО ОБЩЕСТВА

Аннотация. Интенсивное развитие информационно-коммуникационных технологий, как технической основы, привело к созданию и развитию информационного общества (цифрового общества). Обращается внимание на новые перспективные информационно-коммуникационные технологии, которые несут новые риски и угрозы, представляющие опасность для гуманистического функционирования цифрового общества. Среди проблем рисков электронного общества, наиболее сложные связаны с человеческим фактором: морально-этические, социологические и психологические проблемы. Решающая роль в решении этих проблем принадлежит цифровой социологии. Одним из главных, перспективных и результативных методов, представляющим угрозу для электронного общества, является социальный инжиниринг. Указываются причины успешного социального инжиниринга. Приводится классификация методов социального инжиниринга по признаку манипулирования чертами человеческого характера. Для разработки действенных методов борьбы с киберпреступностью необходимы исследования цифровой социологии.

Ключевые слова: цифровое общество, киберугрозы, цифровая социология, социальный инжиниринг.

Концепция информационного общества

Считается, что идея информационного общества (ИО) 30 лет назад была высказана японскими исследователями. Но можно вспомнить теорию постиндустриализма, основу которой заложили З. Бжезинский, Д. Белл, Э. Тоффлер. Постиндустриальное общество – это информационное общество. Известный американский социолог, публицист-футуролог Э. Тоффлер в своей книге "Третья волна" в 1980 году писал о том, что человечество развивается «волнами» в соответствии с развитием науки и техники [1]. Цивилизация третьей волны перестроит систему образования и научных исследований, реорганизует средства массовой информации, принесет новые проблемы и риски. Информация приобретет большую ценность, чем когда-либо. Основоположником концепции информационного общества можно считать и канадского культуролога М. Маклюэна, введшим понятие "глобальной деревни".

Процесс формирования и развития информационного общества носит объективный характер. Представление информации в цифровой, электронной форме (электронные новости, электронные журналы, электронные документы, электронные книги и т.д.) привело к понятию цифрового, электронного общества. Технической предпосылкой создания цифрового общества является развитие информационно-коммуникационных технологий (ИКТ). Формирование ИО в каждой стране, в конечном итоге, ведет к формированию глобального информационного общества. При этом в каждой стране есть свои особенности этого процесса, вытекающие из исторических, политических, социально-экономических и культурных условий. Электронное общество (ЭО) разных стран находятся на различных этапах своего развития (начальная стадия - formative stage, стадия развития - developmental stage, зрелая стадия - mature stage) в зависисимости от развития ИКТ и их использования в различных целях всеми слоями общества [2]. Развитие электронного общества определяется развитием четырех ключевых доменов: электронное правительство (e-government, электронная коммерция (e-commerce), электронные сети (e-networking), электронная деятельность (e-working). Риски и угрозы существуют в любом домене и на любом этапе развития ЭО, имеют свою специфику, требуют социологических исследований с применением специальных методик.

Киберпространство цифрового общества

Сама по себе идея информационного общества имеет гуманистическую основу. ИО должно обеспечивать равные возможности для социального и экономического развития всех граждан страны, а в перспективе - и всех людей в мире. Все больше и больше информации и услуг становятся доступными гражданам в электронном формате. Информация будет доступна всем – нет государственных границ и различных барьеров для ее распространения. Но ЭО – это не только информационные ресурсы. Компонентами ЭО являются также организационные структуры, обеспечивающие его функционирование и развитие. Важной компонентой ЭО являются средства информационного взаимодействия, в том числе программно-технические средства, обеспечивающие доступ к информационным ресурсам на основе информационно-коммуникационных технологий. Индикаторы уровня развития электронного общества в 1980-х годах были ориентированы на перечисленные выше компоненты, так как это базис ЭО. К настоящему времени признанным, более реальным, показателем развития и зрелости ЭО является уровень использования этих компонент.

Ведь ЭО – это не только среда, которая формирует условия для развития и совершенствования человека, взаимного общения. Это глобальное киберпространство, в котором доступны различные виды деятельности: политическая, правовая, экономическая, финансовая, образовательная, экологическая и т.д. Эта деятельность может быть как легальной, так и противоправной, преступной, направленной на нарушение безопасности граждан, предприятий, государства, национальной безопасности страны. С этой точки зрения, ЭО является обществом риска, как и любое общество. Проблема в том, что в ЭО имеют место совершенно новые риски и угрозы, которые активно развиваются вместе с развитием ЭО.

В мире появляются новые технологии, являющиеся результатом развития информационно-коммуникационных технологий, которые способствуют формированию цифрового общества, развитию человечества. Растет ежегодно на 22% использование облачных сервисов, в основе которых лежат технологии виртуализации. Кроме виртуализации и облачных вычислений

появились интернет вещей (Internet of Things, IoT), межмашинное взаимодействие (Machine-to-Machine, M2M), киберфизические системы и т.д. Эти новые технологии повышают качество жизни и экономическую эффективность бизнеса, служат развитию цифрового общества.

Но эти новые технологии таят в себе новые риски и угрозы безопасности граждан, предприятий, государства. Современные информационно-коммуникационные технологии являются фундаментом для построения электронного общества и, одновременно, причиной необходимости обеспечения безопасности этого общества. Неправомерная деятельность в киберпространстве ЭО криминальных элементов или террористов способна приводить к огромным физическим, психологическим, и моральным разрушениям, деградации личности и государства.

Проблемы обеспечения безопасности электронного общества и социология

Задачи обеспечения безопасности ЭО носят комплексный характер. Все понимают необходимость решения правовых, организационных и технических проблем ЭО. Множество специалистов работает в этом направлении. Во всех странах разрабатывается правовая основа ЭО, обсуждается цифровой суверенитет страны. Как в развитых, так и в развивающихся странах принимаются законы: об информации и защите информации, об электронных документах, электронной цифровой подписи, о персональных данных и их защите и т.д. Разрабатываются новые методы и средства защиты информации. Появляются и развиваются новые сервисы обеспечения информационной безопасности.

Но к проблемам обеспечения безопасности ЭО относятся не только правовые, организационные, технические проблемы, но и экологические, морально-этические, социологические, психологические. Надо рассматривать экосистему: компьютер-человек. Современный человек, живущий в традиционном обществе, живет также и в цифровом обществе. События, происходящие в реальном мире и цифровом мире, воздействуют друг на друга. Появился термин "человек информационный" (Homo Informaticus) – продукт информационного общества. Постепенно информация и знание становятся основой всего общества вместо капитала и труда. Электронное общество характеризуется всепроникающим влиянием передовых информационно-коммуникационных технологий на умонастроения людей, их психику, привычки, менталитет, образ жизни. Идет формирование новой цивилизации.

Информация становится доступней, оперативней, наглядно показывает уровень жизни в благополучных странах, людей из разных слоев общества. Это касается и дезинформации, являющейся провоцирующим фактором, побуждающим к неверным действиям. Информация быстро оказывает большое воздействие на людей, заставляет их стремиться к определенному образу жизни, в том числе и противоправным путем, представляющим опасность для общества. Революция в средствах коммуникации приводит к революции в психике и умонастроении человека. Например, эксперты Лаборатории Касперского в результате опроса с участием 16,5 тысяч в 18 странах мира пришли к выводу, что для большинства интернет-пользователей жизнь в социальных сетях чревата расстройствами и депрессией. Эти проблемы не решаются правовым регулированием, организационными мероприятиями, техническими средствами. Определить и оценить риски, промоделировать ситуации, найти способы защититься в случае действия технических средств нарушения безопасности можно. В случае действий человека возникают проблемы гораздо сложнее. И работа в решении этих проблем только начинается.

Активную роль в решении обеспечения безопасности при существовании в электронном обществе должна сыграть цифровая социология, которая представляет собой направление социологической науки, призванное исследовать закономерности социальной жизни человека, живущего одновременно и в традиционном и в электронном обществе. В цифровой социологии, возникшей первоначально из применения методов на основе ИКТ для обработки социальных цифровых данных, объектом исследования является социальная жизнь электронного общества, социальные отношения, возникающие в цифровой среде. Появился термин "вычислительные социальные науки" [3].

Владельцы ресурсов социальных сетей и других онлайн-сервисов (IT-компании) имеют подразделения, которые занимаются анализом цифровых социальных данных, полученных из своих сетей. Но этим, в основном, занимаются не социологи, а IT-специалисты, математики, работающие в области Big Data (Большие данные), Data Mining (Добыча Данных). Из огромного

объема доступных цифровых данных посредством вычислений и интеллектуального анализа данных получают информацию, необходимую для продвижения и развития бизнеса, для развития ИКТ. Имеется тенденция вытеснения социологии, как самостоятельной науки, из области исследования социальной жизни цифрового общества. Но цифровые технологии и практики – это инструмент по поддержке социологических исследований. Новые инструменты всегда приводят к изменению теорий и методов любой науки, в том числе и социологических теорий и исследований [4]. Эти инструменты позволяют повысить уровень анализа в социологических исследованиях, являются, отчасти, точками роста социологических теорий. Но они являются всего лишь инструментами, несмотря на то, что инициируют пересмотр базовых социологических моделей [5]. «Иначе говоря, новые цифры – это еще не наука. Их надо сопоставить с данными других исследований, рассмотреть в динамике (во времени) и четко сформулировать научные выводы» [6]
.

При исследовании социальных проблем цифрового общества ведущую роль должны играть социологи со своими переосмысленными теориями и применением современных инструментов в социальных исследованиях.

Социальный инжиниринг. Одной из опаснейших угроз, которой подвергается любой из членов ЭО, является социальный инжиниринг – СИ (Social Engineering - SE). Методы социальной инженерии являются одной из составляющих многих кибератак, входят в ТОП-10 самых популярных хакерских методов (по данным международной компании BalaBit IT Security). На рисунке 1 представлено распределение типов атак, применяемых злоумышленниками [7]. Атаки методом социальной инженерии представляют 27% от общего числа атак. Следует учесть, что применение социального инжиниринга – это, чаще всего, подготовка к предстоящим атакам.

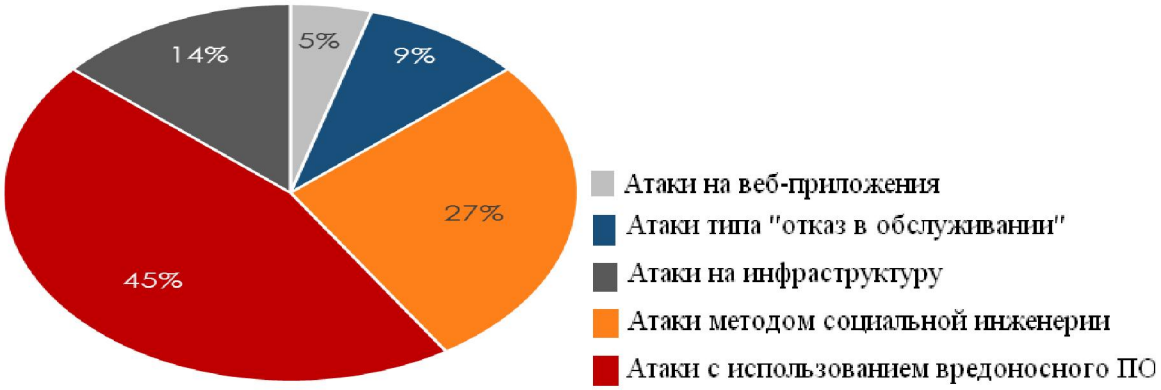

Рисунок 1 - Распределение типов атак

Чисто социологический термин обозначает совокупность подходов прикладных социальных наук, которые ориентированы на целенаправленное изменение человеческого поведения и контроль за ним. СИ основан на человеческом факторе, который имеет место всегда и везде. Человеческий фактор является причиной 70% случаев нарушений безопасности информации. Брюс Шнайер, всемирно признанный специалист в области информационной безопасности (в том числе и в криптографии) в своей книге “Секреты и ложь. Безопасность данных в цифровом мире” приходит к выводу, что не существует всеобъемлющего решения проблемы человеческого фактора в информационной безопасности [8].

Метод социальной инженерии направлен на то, чтобы обманным путем заставить человека выполнить опасные для него действия. Этот метод управления действиями человека без использования технических средств используется давно. Люди, умевшие ввести собеседника в заблуждение и убедить его в истинности того, что на самом деле является ложным, ценились еще в Римской империи.

В киберпространстве ЭО социальный инжиниринг приобрел новые формы и инструменты реализации. Особенно активно используются такие инструменты как электронная почта и сайты социальных сетей. Существует возможность стать другом любого пользователя социальной сети, используя методы социальной инженерии, и получить доступ к его личной информации. А

использование электронной почты уже давно практикуется в качестве инструмента социальной инженерии.

Человек под действием социального инжиниринга выполняет действия, необходимые злоумышленнику, считая эти действия осознанными, правильными и неопасными. На многие действия человека оказывает влияние подсознание. Исследования последних лет показывают, что подсознательное принятие решений опережает сознательное порой на 10 секунд. Учитывая психологические особенности человека, можно обойти многие технологичные решения безопасности: межсетевые экраны, системы предотвращения вторжений, устройства идентификации, средства шифрования, системы обнаружения сетевых атак и т.д. Социальный инжиниринг является самым быстрым и легким путем к нарушению безопасности и самым труднообнаруживаемым.

Социальную инженерию используют для получения закрытой информации или информации, которая представляет большую ценность для злоумышленника (или разведчика). Социальная инженерия всегда была главным оружием разведчиков. В настоящее время социальный инжиниринг является одним из главных, перспективных и результативных методов как киберразведки, так и киберпреступников любого направления. Метод социальной инженерии прост в реализации, требует незначительных финансовых вложений, имеет минимальную вероятность и относительную сложность в выявлении. Существуют специальные группировки профессионалов - социотехников, получающих и выполняющих заказы на поиск и сбор информации в киберпространстве, ее обработку и предоставление заказчикам. Эти профессионалы имеют свои закрытые форумы и закрытые сети.

При рассмотрении успешных примеров социального инжиниринга можно выделить несколько причин, благодаря которым социальный инжиниринг достигает своих целей. Основными из них являются:

- отсутствие (или незнание) достоверной информации, фальсификация, ложная информация и дезинформация;
- отсутствие информации о методах социального инжиниринга, их результативном использовании в преступных целях;
- неудовлетворительное физическое и психологическое состояние человека;
- отдельные черты характера человека (любопытство, доверчивость, беззаботность, невнимательность, лень, любезность, энтузиазм, желание понравиться, отблагодарить, разбогатеть и другие человеческие слабости).

Применение социального инжиниринга предполагает умение собирать о человеке необходимую информацию и знание психологии. Известные в прошлом хакеры, часто становятся консультантами по информационной безопасности. Они пишут книги, статьи и инструкции, дают интервью, проводят демонстрации, записывают видео, посвященные социальной инженерии и методам воздействия на человека. Существуют отдельные сайты, посвященные социальной инженерии. Эта информация в цифровом обществе доступна всем, любой желающий может использовать ее в своих целях. Без помощи социологов и психологов невозможно противостоять этой угрозе.

Злоумышленник, использующий методы социальной инженерии, убеждает человека выдать необходимую ему информацию с помощью психологических методов. Важны личностные качества социотехника. Он обычно коммуникабелен, приятен для других в общении, не навязчив, с чувством юмора, легко располагает людей к себе.

Методы социального инжиниринга можно классифицировать по различным признакам. Одним из важных признаков является классификация по использованию черт человеческого характера. Выделяют шесть методов, которые используются социотехниками.

Авторитетностный метод. Люди, обычно, не отказывают в услуге авторитетному или облеченному властью человеку. Социотехник, используя различные технологии социальной инженерии, достоверно представляется таким человеком и получает необходимую информацию.

Приверженностный метод основан на умении расположить к себе человека. Обычно социотехник узнает склонности человека, его интересы. Находит с ним общий язык и получает конфиденциальную информацию.

Взаимностный метод использует такую черту характера человека, как желание "отплатить" за услугу (подарок, помощь, совет, информацию и т.д.). Взаимная услуга – предоставление критической информации.

Ответственностный метод применяется к людям, которые привыкли выполнять свои обещания. Достаточно, используя методы социальной инженерии, заставить человека пообещать то, что нужно преступнику (информацию). Обещанное будет выполнено.

Социальностный метод эксплуатирует принадлежность человека к определенной авторизованной (социальной) группе. Все входящие в группу делятся между собой информацией. Необходимо лишь стать членом группы, в которую входят люди, владеющие необходимой информацией, войти к ним в друзья.

Ограниченностный метод основан на предоставлении человеку якобы ограниченной информации (по времени и/или по распространению, и/или по существованию). Для того чтобы получить доступ к этой информации, необходимо ввести идентификатор, пароль, адрес электронной почты. Очень часто люди используют одинаковые идентификаторы и пароли для доступа к разным информационным ресурсам, в том числе и конфиденциальным. Злоумышленник использует эти данные, чтобы получить закрытую информацию из конфиденциальных источников. Полученный адрес электронной почты используется для «маскарада». Можно получить необходимую информацию действуя от имени человека, которому доверяют.

В электронном обществе все эти методы, используя относительную анонимность сети, легко реализуемы на основе групп социальных сетей, электронной почты, онлайн сервисов. В Интернете существует множество фейковых аккаунтов, создаваемых социотехниками в противоправных целях. Функционирует большое количество фишерских web-сайтов, осуществляется множество фишинговых рассылок. Финансовый фишинг является одним из наиболее распространенных типов киберпреступной активности. На рисунке 2 представлен рост финансового фишинга от общего числа финансовых киберпреступлений [9].

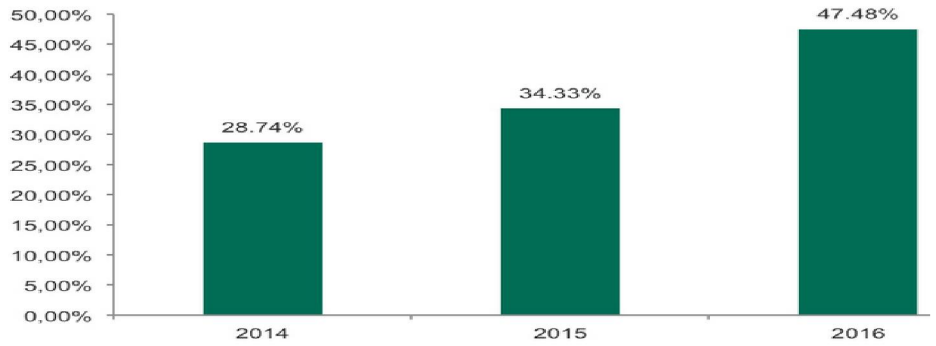

Рисунок 2 - Процент финансового фишинга, обнаруженного «Лабораторией Касперского» в 2014-2016 гг.

В ЭО никто не застрахован от социального инжиниринга. Кевин Митник - один из самых известных в прошлом хакеров, при расследовании своих преступлений в показаниях Конгрессу сказал, что наиболее уязвимое место в системе безопасности – «человеческий фактор». Являясь в настоящее время консультантом по компьютерной безопасности, он считает, что получить пароль путём обмана гораздо проще, нежели взломать систему безопасности. Причем, в киберпространстве это сделать легче, так как отсутствует непосредственное общение.

При непосредственном контакте с человеком, ложь можно определить по словам (оговорки, тирады), голосу (наличие пауз, речевые ошибки, тон и высота голоса), пластике (эмблемы, иллюстрации, манипуляции), мимическим признакам (микровыражения), признакам ВНС (вегетативной нервной системы) [10]. Чувства и эмоции людей, независимо от социального статуса и национальной принадлежности, проявляются в универсальных признаках. Они всегда выдают неискренность или свидетельствуют о преднамеренной лжи. Наблюдая за собеседником во время общения, можно по этим признакам получить достаточное количество информации и правильно ее

использовать. Но эту информацию невозможно получить, общаясь в социальных сетях или по электронной почте, используя онлайн-сервис.

Общеизвестные рекомендации для обеспечения собственной безопасности, безопасности предприятия, государства, которыми обычно руководствуются в традиционном обществе, в большинстве случаев игнорируются при общении в ЭО. Общение в социальных сетях, посредством электронной почты, использование онлайн сервисов создает иллюзию независимости, дружелюбности, взаимопонимания и взаимного доверия. И даже недоверчивые и осторожные люди становятся жертвами социальной инженерии.

Защититься от социального инжиниринга непросто. Люди могут не знать, что их обманули. К тому же многие предпочитают не рассказывать об этом. Модели, описывающей поведение людей в различных ситуациях, реакцию на то или иное воздействие или сложившиеся условия, не существует. Имеющиеся частные шаблоны поведения не охватывают все ситуации. Человек – это сложная и многогранная система. Разработка модели является проблемной задачей в силу необходимости учета очень многих индивидуальных параметров.

На данном этапе развития ЭО основным способом защиты от методов социальной инженерии является обеспечение людей информацией о методах социального инжиниринга, их результативном использовании в преступных целях, о частных шаблонах поведения. Необходимо вести обучение людей противодействию социальному инжинирингу. Для разработки действенных мер борьбы с этими преступлениями необходимы социологические исследования, направленные на изучение применения методов социального инжиниринга в преступных целях в ЭО.

Заключение

Информационное общество не знает границ. Используя сетевые технологии, киберпреступник может совершать преступления в любой точке земного шара, независимо от места своего нахождения. Киберпространство ЭО уже сейчас активно используется для реализации комплексного подхода к построению целевой кибератаки (APT-атаки), включающей активное воздействие на людей методами психологии и социальной инженерии.

Потенциальные последствия рисков в киберпространстве ЭО катастрофичны. Для безопасного существования в ЭО, противодействия его рискам необходимо объединение всех его членов. Успех зависит от объединения исследований социологов, психологов, математиков и IT-специалистов. Должны быть разработаны и на регулярной основе работать программы повышения осведомленности социума о киберугрозах, рисках цифрового общества, методах социальной инженерии и противодействия им. Результаты исследований цифровой социологии должны стать платформой для разработки методов борьбы с киберпреступностью. Это очень важно как для социума электронного общества каждой страны, так и мирового сообщества.

ЛИТЕРАТУРА

[1] Toffler A. The Third Wave. - New York: William Morrow & Company, ISBN 0688035973, 9780688035976, 1980. – 544 p.

[2] Becky P.Y. Loo. The E-Society. - Hauppauge: Nova Science Publishers, ISBN: 978-1-61209-831-9, 2011. – 266 p.

[3] Lazer D., Pentland A., Adamic L., Aral S., Barabasi A.L., Brewer D., Christakis N. et al. Computational Social Science // Science, 2009. - № 323 (5915). - P. 721-723. DOI: 10.1126/science.1167742.

[4] Дудина В.И. Социологическое знание в контексте развития информационных технологий // Социологические исследования, 2015. - № 6. - С. 13-22.

[5] Дудина В.И. Цифровые данные - потенциал развития социологического знания // Социологические исследования, 2016. - № 9. - С. 21-30.

[6] Тощенко Ж. Т. Об ответственности и взаимоответственности редакции и авторов // Социологические исследования, 2017. - № 1. - С. 3-4.

[7] Зиненко О. Анализ угроз информационной безопасности 2016-2017. //Аналитический центр Anti-Malware.ru. 2017. https://www.anti-malware.ru/analytics/Threats_Analysis/Analysis_information_security_threats_2016_2017.

[8] Schneier *B.* Secrets and Lies: Digital Security in a Networked World. - New York: John Wiley & Sons, ISBN: 0471253111, 2000. – 304 p.

[9] Ландшафт финансовых киберугроз в 2016 году. АО Kaspersky Lab. 2017. https://securelist.ru/analysis/obzor/30336/financial-cyberthreats-in-2016/.

[10] Ekman P. Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage. - New York: W.W. Norton & Company, ISBN 0-393-30872-3, 1985. – 366 p.

REFERENCES

[1] Toffler A (**1980**) The Third Wave. New York: William Morrow & Company, ISBN 0688035973, 9780688035976, 544 p.

[2] Becky PY Loo (**2011**) The E-Society. Hauppauge: Nova Science Publishers, ISBN: 978-1-61209-831-9, 266 p.

[3] Lazer D, Pentland A, Adamic L, Aral S, Barabasi AL, Brewer D, Christakis N et al. (2009) Computational Social Science [Science] No.323 (5915). 721-723. DOI: 10.1126/science.1167742.

[4] Dudina VI (**2015**) Sociological knowledge in the context of information technologies development [Sotsiologicheskie issledovaniya] 6: 13-22 (In Russian.).

[5] Dudina VI (**2016**) Digital data potentialities for development of sociological knowledge [Sotsiologicheskie issledovaniya] 9: 21-30 (In Russian).

[6] Toshchenko ZhT (**2017**) On responsibility and co-responsibility of editors and authors. [Sotsiologicheskie issledovaniya] 1: 3-4 (In Russian).

[7] Zinenko O (**2017**) Analiz ugroz informatsionnoy bezopasnosti 2016-2017. [Analiticheskiy tsentr Anti-Malware.ru] [https://www.anti-malware.ru /analytics/Threats_Analysis/Analysis_ information_security_threats_2016_2017] (In Russian).

[8] Schneier B (**2000**) Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, ISBN: 0471253111, 304 p.

[9] Landshaft finansovykh kiberugroz v 2016 godu. AO Kaspersky Lab (**2017**) [https://securelist.ru/analysis/obzor/30336/financial-cyberthreats-in-2016/] (In Russian).

[10] Ekman P (**1985**) Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage. New York: W.W. Norton & Company, ISBN 0-393-30872-3, 366 p.

Е.Ж. Айтхожаева, Н.А. Сейлова

Қ.И. Сәтпаев атындағы Қазақ Ұлттық Техникалық Зерттеу Университеті

САНДЫҚ ҚОҒАМ ҚАУІПТЕРІ

Түйін. Ақпараттық-телекоммуникациялық технологиялардың техникалық негіздері бойынша қарқынды дамуы, ақпараттық қоғам (сандық қоғам) дамуына және құрылуына әкелді. Жаңа ақпараттық-коммуникациялық технологиялардың қауіптеріне назар аударылады, олар гуманистік сандық қоғамның өмір сүруіне төнетін жаңа тәукелдер мен қауіптерді тудырады. Электрондық қоғам қауіптерінің ішіндегі проблемалардың аса күрделісі адами факторлармен байланысты: моральді-этикалық, социологиялық және психологиялық проблемалар. Бұл проблемаларды шешу үшін маңызды рөл атқаратын сандлық әлеуметтану. Электрондық қоғам үшін қауіп төндіретін негізгі, келешек және нәтижелі әдістердің бірі әлеуметтік инжиниринг болып табылады. Табысты әлеуметтік инжиниринг себептері көрсетіледі. Адам мінезінің белгілерін манипуляциялау арқылы әлеуметтік инжиниринг әдістерінің сипаттамасы келтіріледі. Киберқылмыспен күресу әдістерін тиімді құру үшін сандық әлеуметтануды зерттеу қажет.

Тірек сөздер: электрондық қоғам, киберқауіптер, сандық әлеумет, әлеуметтік инжиниринг.

Сведения об авторах:

Айтхожаева Евгения Жамалхановна - кандидат технических наук, ассоциированный профессор кафедры Информационной безопасности Казахского национального исследовательского технического университета имени К.И.Сатпаева, г. Алматы, ул. Сатпаева, 22, +7(701)7141752727), e-mail: ait_djam@mail.ru,

Сейлова Нургуль Абадуллаевна - кандидат технических наук, ассистент профессор кафедры Информационной безопасности Казахского национального исследовательского технического университета имени К.И. Сатпаева, г. Алматы, ул. Сатпаева, 22, +7(707)3505038, e-mail: seilova_na@mail.ru.