ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ МЕЖДУНАРОДНЫХ ОТНОШЕНИЯХ

Исамухамедов Темур Маратович
Независимый соискатель
Ташкентского государственного
университета востоковедения

АННОТАЦИЯ

В этой статье исследуется сложная сфера информационной безопасности в современного общества, рассматриваются его внутренние и международные аспекты. Используя два различных социологических подхода – структурно-функциональный и интерпретационный – этот анализ раскрывает сложную структуру информационной безопасности. Информационная безопасность стала одной из важнейших проблем современных международных отношений. Развитие информационных технологий привело к увеличению зависимости государств и международных организаций от информационных систем и сетей. В то же время кибератаки и другие угрозы информационной безопасности часты и могут подорвать стабильность и безопасность государств. В современных международных отношениях информационная безопасность является неотъемлемой частью национальной и международной безопасности. Государства и международные организации принимают меры по защите своих информационных систем и сетей от кибератак и других угроз.

Обеспечение информационной безопасности включает в себя ряд мер, например:

Разработка и реализация национальных стратегий и программ в области информационной безопасности.

Создание и сопровождение эффективных систем защиты информационных систем и сетей.

Развитие международного сотрудничества в сфере информационной безопасности.

Обучение и образование специалистов в области информационной безопасности.

Повышение осведомленности государственных органов, предприятий и граждан по вопросам информационной безопасности.

Обеспечение информационной безопасности — сложная задача, требующая постоянного мониторинга и адаптации к меняющимся угрозам.

Эффективные меры информационной безопасности служат стабильности, безопасности и благополучию государств и всего международного сообщества.

В наше время, когда информационно-коммуникационные технологии пронизывают все общество, появление информационного общества представляет собой важнейшую веху в развитии общества. Бесперебойный поток информации не только способствует выживанию человека, но и необходим для устойчивого роста. Следовательно, информационная безопасность приобретает все большее значение, привлекая все большее внимание как исследователей, так и практиков.В данной статье представлен всесторонний анализ информационной безопасности, рассматриваются ее сущность, различные проявления и последствия в современной цифровой среде. Кроме того, в нем рассматриваются различные стратегии и методологии, используемые для защиты критически важных данных и систем.

Кроме того, в этом исследовании расширен анализ потенциального влияния мер информационной безопасности на развитие общества, что позволяет глубже понять сложную взаимосвязь между этими мерами и развитием общества.

Ключевые слова: *цифровое общество, информационная сфера, информационная система, защита данных, коммуникация, информационный риск, структурно-функциональный анализ, социологическая парадигма.*

ВВЕДЕНИЕ

Проблема информационной безопасности становится все более значимой в сегодняшнюю эпоху, характеризующуюся широким влиянием информационных технологий. За последние несколько лет все больше осознается необходимость тщательного изучения как положительных, так и отрицательных аспектов этого развития, а также прогнозирования его будущего направления.

Важно признать, что, хотя развитие информационных технологий может принести многочисленные выгоды, оно не обязательно приводит к безоговорочным преимуществам для отдельных лиц, обществ, правительств и мирового сообщества. Тем не менее, существуют некоторые информационные тенденции, которые соответствуют принципам устойчивого развития и могут продолжиться в новой парадигме цивилизационного прогресса. К ним относятся: Растущий спрос на информацию со стороны отдельных лиц и

обществ; Информация[1], выступающая в качестве катализатора дальнейшего общественного развития; Интегрированная природа информационных технологий; Интеллектуализация и виртуализация социальных структур; Развитие информационной сферы; Обеспечение информационной безопасности; Создание глобального хранилища знаний и интеграция человеческого интеллекта; Формирование информационного общества.

В настоящее время информационная безопасность рассматривается как сложный и многогранный процесс, зависящий от множества внутренних и внешних факторов. Это обусловлено современным этапом развития общества, который характеризуется развитием и интеграцией различных информационных технологий, таких как сетевые коммуникации и биотехнологии.

МЕТОДОЛОГИЯ И СТЕПЕНЬ ИЗУЧЕННОСТИ

Специалисты, изучавшие тему "Проблемы обеспечения информационной безопасности в современных международных отношениях". Академические исследователи: Эдвард Сноуден, (Сиракузский университет), профессор Кристин Блэкберн, Школа передовых международных исследований им. Пола Х. Нитце Университета Джонса Хопкинса. доктор Томас Рид, Школа государственного управления Джона Ф Кеннеди Гарвардского университета, октор Мишель Чин-Ли, Школа общественных и международных отношений Колумбийского университета, Тимо Китцина, Институт международных отношений Финляндии. Эксперты из правительственных организаций: Генерал Кейт Александер (в отставке), бывший директор Агентства национальной безопасности США, Адмирал Майкл Роджерс (в отставке), бывший директор Агентства национальной безопасности США, Доктор Роланд Мюллер, бывший директор Германского федерального ведомства по информационной безопасности, Доктор Питер Фентен, бывший заместитель директора по вопросам кибербезопасности Центра правительственной связи Великобритании, Доктор Мишель ван ден Бош, бывший директор Национального центра кибербезопасности Нидерландов, Эксперты из международных организаций: Юрген Стольц, старший директор по кибербезопасности Организации по безопасности и сотрудничеству в Европе (ОБСЕ), Крис Кубекович, руководитель отдела кибербезопасности НАТО, Доктор Анурадха Миттал, генеральный секретарь Глобальной сети интернет-политики, Доктор Сесилия Муньос, директор Женевского центра политики

[1] Антипов А.А. Информационная безопасность как объект правового регулирования. URL://https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-obekt-pravovogo-regulirovaniya

безопасности, Доктор Кэтрин Уркарт, директор Женской программы по вопросам кибербезопасности в женском университете Джеймса Мэдисона и

ОСНОВНАЯ ЧАСТЬ

Анализ информационной безопасности. Развитие информационного общества в России представляет собой множество существенных проблем, решение которых оказывает существенное влияние на общее благосостояние общества. Глубокий анализ тенденций в процессе информатизации в России подчеркивает информационную безопасность как важнейший аспект в формировании современного информационного общества[2].

Недавние исследования начали изучать информационную безопасность через социокультурную призму, в то время как более широкая область знаний, связанная с различными социальными институтами, остается относительно неизученной. Многогранная природа информации проистекает из разнообразных контекстов, в которых она используется. Различия в способах распространения информации, потенциальных типах угроз и форматах готовых информационных продуктов порождают различные точки зрения на критические аспекты информационной безопасности.

Социологическая перспектива информационной безопасности. В контексте социологического анализа информационная безопасность может пониматься как зависящая от поддержания социального элемента в целях поддержания динамического равновесия системы. По мнению Н. В. Лопатиной, информационные технологии не следует рассматривать как асоциальное явление, поскольку они являются продуктом человеческих усилий, направленных на открытие новых средств, форм и методов для преобразования реальности и удовлетворения общественных потребностей, подобно другим технологиям. Как утверждает Лопатина в своей работе 2006 года, информационные технологии берут начало в социальном опыте.

Информационная безопасность не может существовать вне сферы социального взаимодействия и, как и любое другое социальное явление, требует социологического исследования для понимания реакции социальной системы на информацию.

Информационные технологии как неотъемлемый компонент организационной структуры. В современном мире информационные технологии играют ключевую роль в продвижении общественного прогресса,

[2] Антипов А.А. Информационная безопасность как объект правового регулирования. URL://https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-obekt-pravovogo-regulirovaniya

становясь неотъемлемым компонентом каждой организации. Они облегчают обмен информацией, способствуют сотрудничеству с международными партнерами и объединяют людей в обществе. Опыт показал, что сбои в системах обмена информацией могут привести к дисфункции организации. В результате правительства и предприятия осознают важность защиты информационных ресурсов и их интеграции в стратегическое планирование.

Острая необходимость в информационной безопасности привела к разработке инновационных технических решений и переоценке того, как этот вопрос следует решать с социальной и культурной точки зрения.

Социально-культурные аспекты информационной безопасности. В современных исследованиях информационная безопасность все чаще признается многомерной концепцией, в которой технические соображения играют второстепенную роль по сравнению с социокультурными факторами. Это смещение акцента обусловлено признанием того, что человеческий фактор — индивидуум как создатель и получатель информации — играет решающую роль в процессе обмена информацией. Успех и надежность информационных систем зависят от того, насколько эффективно индивидуальные интересы и психологические черты интегрированы в обмен информацией. В настоящее время информационная безопасность подразумевает комплексную защиту данных, связанных со статусом, перемещением, обработкой и передачей как физических, так и нематериальных активов. Информационная безопасность охватывает не только защиту носителей информации и хранилищ, но также распространяется на защиту жизненно важных интересов, включая интересы отдельных лиц, общества и государства, от любого преднамеренного или непреднамеренного воздействия на распространение информации в любой форме.

К сожалению, в настоящее время наблюдается отсутствие междисциплинарных исследований, которые рассматривают социальный аспект информационной безопасности. Целью данной статьи является рассмотрение вопроса информационной безопасности с социологической точки зрения. По мнению Г. Диллона и Дж. Бэкхауса, понимание принципов, лежащих в основе различных подходов к безопасности, имеет важное значение. В 1979 году Баррелл и Морган предложили структуру, состоящую из четырех социологических парадигм, которая позволяет исследователям понять основы концепций информационной безопасности и их социальный аспект. Морган разработал свой собственный концептуальный и технический подход, изложив два набора теоретических перспектив, основанных на субъективных и

объективных факторах. Объективистская перспектива предполагает, что мир существует независимо от людей, имея особую структуру и функцию. Напротив, субъективная (или номиналистская) перспектива рассматривает реальность как продукт индивидуального восприятия, при этом каждый человек конструирует свою собственную интерпретацию мира и придает значение событиям. Номиналисты утверждают, что объективисты ошибочно воспринимают метафоры буквально, трансформируя абстрактные идеи в конкретные реальности. Объективист, в свою очередь, обвиняют номиналистов в игнорировании этих конструкций, совершая логическую ошибку.

Социологическая перспектива исследований информационной безопасности. В соответствии с точкой зрения Г. Баррелла и Г. Моргана ученые подчеркивают необходимость регулирования человеческих взаимодействий как важнейшего аспекта всеобъемлющей информационной безопасности. Они стремятся понять общество как единую систему, интегрированный организм и организованную сущность. В этом контексте изучаются различные аспекты информационной безопасности, включая разработку методов, основанных на контрольных списках, оценке рисков и анализе. Контрольные списки используются в качестве инструментов для выявления всех возможных областей для мониторинга информации и облегчения изучения различных элементов системы, связанных с безопасностью. Они направлены на создание «идеальной» или «непроницаемой» системы, предоставляя средства для определения и выбора наиболее эффективного подхода для достижения конкретных целей.

Несмотря на широкое использование контрольных списков в практике обеспечения информационной безопасности, они не фокусируются на конкретных проблемных сценариях и вместо этого косвенно затрагивают социальные аспекты этих вопросов. Опора на контрольные списки отдает приоритет процедурному анализу и игнорирует основные причины и потенциальные последствия этих процедур. Часто предполагается, что цели уже установлены. Другим аспектом функционалистского подхода является анализ рисков, который является критически важным инструментом для обеспечения информационной безопасности. Анализ рисков помогает структурировать и организовывать процессы, что приводит к созданию надежных систем защиты для организаций.

Ключевым компонентом анализа рисков является выявление существующих рисков и принятие мер по их снижению. Риски могут возникать из-за социальных, организационных или социально-психологических влияний.

Социальные факторы включают влияние СМИ и культурные нормы. Организационные факторы включают организационную структуру, технологии, эргономические соображения и методы управления. Социально-психологические факторы относятся к влиянию социальных взаимодействий на индивидуальное поведение, особенно в отношении рискованных видов деятельности.

Характер задач и процессов принятия решений, а также наличие потенциальных опасностей также являются важными факторами для рассмотрения. Одним из важнейших аспектов при определении надежности системы является человеческий фактор. Несмотря на сложность автоматизированных систем, они по-прежнему полагаются на вмешательство человека для оптимальной производительности. Эффективное управление информацией и меры безопасности имеют важное значение для снижения рисков и обеспечения устойчивости системы. С точки зрения управления рисками, управление информацией существенно влияет на индивидуальное поведение в чрезвычайных ситуациях, которые могут представлять потенциальные риски информационной безопасности. Исследования в этой области продолжают расширять наше понимание этих сложных взаимодействий.

Однако стало ясно, что управление рисками в текущем контексте требует иного подхода. Сам аналитический процесс должен быть скорректирован для обеспечения безопасности за счет использования синергетических методов и нелинейной динамики, что значительно повысит эффективность предотвращения новых угроз информационной безопасности.

На данном этапе развития существует несколько ограничений методов анализа рисков. Традиционная теория вероятностей неадекватна для точной оценки рисков безопасности, поскольку угрозы по своей сути непредсказуемы и случайны. Кроме того, анализ рисков слишком упрощен, фокусируясь исключительно на таких активах, как информация, оборудование и программное обеспечение, без учета более широких социальных последствий. Вместо изучения групповой динамики анализ рисков выявляет и оценивает только индивидуальные факторы риска. Еще одной областью исследований для функционалистов является изучение политик безопасности. Они предложили различные фреймворки для помощи в концептуализации информационной безопасности и конфиденциальности. Ван ден Ховен, например, концептуализирует конфиденциальность как фундаментальное право человека, которое охватывает защиту неотъемлемой ценности личности с точки зрения

защиты от информационного вреда, предотвращения информационного неравенства, борьбы с информационной несправедливостью и дискриминацией и поощрения автономии[3].

Например, Н. Колокотронис и коллеги предложили комплексную модель, которая охватывает несколько уровней и измерений. Модель включает такие этапы, как анализ и проверка требований организации, проведение оценок рисков и анализов затрат, а также формулирование стратегий безопасности.- Мониторинг результатов. Исследователи подчеркивают необходимость того, чтобы информационной безопасности уделялось особое внимание на самых высоких уровнях организационного управления, и ее не следует рассматривать как просто техническую проблему или набор конкретных задач. Они наблюдают изменение отношения к информационной безопасности среди исследователей и практиков, признавая, что это не просто разработка и внедрение технических решений, а скорее критическая социально-культурная проблема, которая может иметь катастрофические последствия, если ее игнорировать. В своем исследовании информационной безопасности функционалисты обнаружили, что организационные контексты имеют сходство с физической средой, что привело их к созданию научной основы для концепции управления информационной безопасностью. Они рассматривают менеджеров как сформированных своим окружением, а сообщества, организации и системы управления как независимые от индивидуальных когнитивных способностей. Функционалисты утверждают, что этот подход заставляет менеджеров расставлять приоритеты в отношении потребностей и целей организации при разработке стратегии информационной безопасности. Они также утверждают, что менеджеры рассматривают информацию как всеобъемлющее представление реальности и, следовательно, стремятся решать выявленные требования с ее помощью. Функционалисты также утверждали, что если все подсистемы функционируют эффективно, организация будет в значительной степени защищена от рисков. Они представили свой собственный взгляд на информационную безопасность, заявив, что если система защищает свои подсистемы, она также защищает себя. Различные компоненты системы, которые вносят вклад в общую безопасность отдельных субъектов, не обязательно должны быть взаимозависимыми, поэтому общая безопасность может быть достигнута посредством тщательного анализа механизмов каждого компонента. Однако этот подход может упускать из виду глубинные чувства, отношения и восприятие информационной безопасности.

[3] Клара Маатуис. Ответственное поведение в сфере цифровой безопасности: определение и модель оценки.

Интерпретативная парадигма. Как исследователи, следующие интерпретативному подходу, так и функционалисты согласны, что принципы контроля и стабильности являются эффективными и существенными. Однако те, кто придерживаются интерпретативной точки зрения, подходят к проблемам с субъективной точки зрения, сосредотачиваясь на индивидуальном восприятии конкретных социальных контекстов.

Стоит отметить работу И. Коско и Р. Пола, которые использовали социально-организационный подход в своем исследовании информационной безопасности. Они предложили концепцию, состоящую из трех компонентов: доверия, культуры и коммуникации риска при определении целей безопасности[4]. Анализ риска также был предметом активного обсуждения в этом контексте. Например, Л. Уиллкокс и Х. Маргреттс использовали модель для оценки уровня риска для информационных систем. Эта модель подчеркивает важность исторического, процедурного и контентного анализа, подчеркивая значительную роль социальных и качественных факторов в информационной безопасности (Уиллкокс и Маргреттс, 1994).

W.Beck и R.Baskerville оспаривают функционалистский подход к исследованию рисков, утверждая, что неправильно отдавать приоритет техническим решениям для улучшения безопасности информационных систем без учета таких факторов, как понимание целей и мотивов отдельными лицами. Beck подчеркивает, что в зрелом рыночном обществе риски не могут быть четко определены, поскольку они являются не только угрозами, но и возможностями (Beck, 2000, стр. 56). Baskerville утверждал, что оценка рисков может стать более эффективной и ценной, если ее использовать в качестве инструмента для общения между специалистами по безопасности и менеджерами, особенно в контексте управления бизнесом и структур безопасности, разработанных с помощью интерпретационного подхода[5].

А. Шередер и Дёррсен изучают потенциальные негативные последствия использования Интернета, включая экономические, культурные, социальные и индивидуальные аспекты. Экономическое влияние Интернета часто связано с онлайн-покупками и азартными играми, что может привести к долгам и финансовому мошенничеству. Культурное влияние использования Интернета касается индивидуальных ценностей, поведения и идентичности в культурной сфере. В России молодые люди, которые примыкают к субкультурным группам, могут заниматься такими видами деятельности, как нанесение

[4] Коско и Пол, Information Society: Problems and Methods of Their Solution. Power, 7, 2003. P. 90-96.
[5] Baskerville, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. European Journal of Information Systems, 1, 121-130.1991, стр. 121

татуировок, что может привести к проблемам со здоровьем и повышенному риску передачи ВИЧ. Киберпреступность, включая кражу личных данных, фишинг и онлайн-травлю, имеет далеко идущие последствия, которые затрагивают как культурную, так и личную сферы.

Эти действия могут вызывать чувства грусти, тревоги, гнева и раздражительности, а также приводить к социальной изоляции и снижению социальных связей. Они также могут способствовать возникновению проблем с психическим и физическим здоровьем, таких как агрессия, расстройства сна и пищевого поведения, а также повышенная тревожность.

Эти проблемы могут сократить досуговую деятельность и оказать негативное влияние на благополучие человека. Чтобы противостоять этим эффектам, можно реализовать несколько стратегий, включая поиск поддержки у друзей и семьи, игнорирование оскорбительных сообщений, блокировку определенных веб-сайтов и принятие мер по защите конфиденциальности. Российские социологи выделили несколько особенностей информационного общества, таких как компьютерные игры, возросшая мобильность и значительный разрыв между молодыми и старшими поколениями с точки зрения цифрового неравенства.

Цифровое неравенство в России ежегодно увеличивается, и правительство регулирует вопросы, связанные с информацией, для решения этой проблемы. Информационные технологии меняют объем усилий, необходимых для доступа людей к информации, создавая возможности для социальных изменений[6].

D. Backhouse и G. Dillon разработали модель информационной безопасности, которая учитывает внутренние, тонкие поведенческие модели членов организации. Благодаря этому исследованию исследователи смогли смоделировать поведение человека в ситуациях, когда требуется сотрудничество. Взаимодействие между членами организации обсуждалось с точки зрения обеспечения общей информационной безопасности. B. von Solms подчеркнул, что если информационной безопасности не уделяется приоритетное внимание на организационном уровне и не учитываются все соответствующие аспекты и измерения, существует значительный риск серьезных угроз для дальнейшего существования организации. Фон Solms утверждал, что информационная безопасность выходит за рамки чисто технических соображений. Такие факторы, как методы управления,

[6] В.Яницкий, An Integrated Approach for Securing Electronic Transactions over the Web. Benchmarking: An International Journal, 9, P. 166-181

организационная культура и структура, играют решающую роль в поддержании информационной безопасности.

Решения относительно стратегического направления компании предшествуют решениям относительно технических аспектов безопасности, при этом технические меры служат для укрепления и продвижения желаемого поведения людей в организации. По словам Исто Хувилы (2018), большая часть информации теперь генерируется с помощью цифровых устройств, которые заменили многие аналоговые инструменты, которые использовались для сбора, записи и обработки данных. Пожилые люди в России сталкиваются с трудностями при использовании Интернета, смартфонов, банкоматов (АТМ) и других цифровых технологий. Тем не менее, правительство вкладывает значительные ресурсы в обучение этой возрастной группы использованию информационных технологий, поскольку медиа-ландшафт в крупных городских районах значительно продвинулся вперед. Мы считаем, что принятие критического подхода к информационной безопасности позволяет нам рассматривать эту проблему как сложную системную проблему. Этот подход также помогает выявлять и анализировать факторы, влияющие на поведение и взаимодействие людей. Кроме того, он позволяет нам интегрировать анализ технических и социальных аспектов в информационную безопасность. В рамках этой структуры информационная безопасность рассматривается и исследуется с целостной точки зрения, которая включает человеческий фактор. Перспективные области для исследований включают изучение восприятия риска, индивидуальной ответственности за действия, а также возникновение и оценку неформальных норм поведения. Большинство российских организаций отдают предпочтение многоуровневым подходам к интеграции информационных систем с организационными операциями. Выход за рамки строго функционалистской перспективы позволяет более глубоко исследовать взаимодействия между людьми, их поведение, противоречия и последствия, связанные с конкретными действиями. По сути, исследователям необходимо принять комплексный подход, чтобы понять сложности информационной безопасности с точки зрения интерпретации.

Для тех, кто принимает этот подход, может быть полезно опираться на идеи из социальных теорий, таких как феноменология, герменевтика и теория конфликта. Ученые определили сильные и слабые стороны этих фреймворков, что позволяет им разрабатывать более эффективные меры информационной безопасности.

ЗАКЛЮЧЕНИЕ

В этой статье представлен всесторонний обзор информационной безопасности с целью улучшения нашего понимания методов анализа информации. Традиционные подходы к анализу информации часто опираются на устоявшиеся рамки, но они не учитывают контекстные факторы, такие как организационная культура, навыки, отношения и индивидуальные различия. В результате эти подходы могут упускать из виду важные аспекты исследовательского проекта и приводить к неполному пониманию сложности информационной безопасности. Позитивисты склонны рассматривать информационную безопасность как чисто технический или научный вопрос, а не как более широкую организационную проблему, требующую более целостного подхода. Напротив, интерпретационный подход подчеркивает социально-техническую природу информационных систем и фокусируется на целях, связанных с организационным контекстом, обменом информацией, расширением прав и возможностей, креативностью, инновациями и мотивацией сотрудников.

В рамках традиционного позитивистского анализа предполагается, что люди участвуют в коммуникации и формируют отношения. Однако принятие интерпретационной перспективы требует более глубокого погружения в содержание коммуникации и динамику взаимодействия внутри организаций. Позитивистские подходы, как правило, сосредоточены на вопросах, связанных с информационной безопасностью, в то время как те, кто принимает интерпретационный подход, стремятся получить более полное понимание сложных проблем и изучить их различные аспекты. Традиционные методы, такие как контрольные списки и оценки рисков, могут быть более подходящими для решения проблем с четкими решениями.

С другой стороны, интерпретационный анализ оказывается ценным для решения неуловимых проблем или проблем с эмоциональными измерениями, а также проблем в организациях со значительными политическими аспектами. Интерпретативное исследование расширяет сферу анализа, включая такие факторы, как организационный контекст, человеческие взаимодействия, модели коммуникации, поведенческие тенденции, ролевая динамика, эмоциональные тонкости и ориентированное на действия поведение.

Процесс перехода России к информационному обществу находился под влиянием множества факторов. К ним относятся уникальные характеристики современных СМИ, сложность правовой базы, социальные, культурные и психологические аспекты общественного и индивидуального сознания, а также роль правительства в координации усилий различных заинтересованных сторон

по мере того, как страна движется к информационному обществу. С помощью стратегической политики правительство стремится поощрять отдельных лиц и группы к принятию этой новой технологической среды, содействовать росту отраслей, связанных с информацией, и поддерживать демократические ценности, одновременно защищая права личности.

Взаимодействие между экономическими, социальными, культурными и технологическими факторами в развитии информационного общества очевидно в смягчении регулирования СМИ, появлении новых стандартов для журналистов и усилении государственного надзора.

Установлено, что путь к созданию информационного общества в регионах Российской Федерации во многом зависит от успешного развития информационно-коммуникационных технологий, а также существенной государственной поддержки инновационных усилий. Была выявлена корреляция между успешным развитием информационного общества и информационной средой, которая охватывает традиционные структуры, модернизированные взаимодействия и инновационные интегрированные функции. Важно отметить, что каждая парадигма имеет свои сильные и слабые стороны. Однако, применяя теоретический и методологический подход, основанный на различных социологических концепциях, посвященных изучению вопросов информационной безопасности, можно проводить исследования и лучше понимать сложную природу проблем информационной безопасности в современном обществе.

ЛИТЕРАТУРА (REFERENCES)

1. Антипов А.А. Информационная безопасность как объект правового регулирования. URL://https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-obekt-pravovogo-regulirovaniya
2. Антипов А.А. Информационная безопасность как объект правового регулирования. URL://https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-obekt-pravovogo-regulirovaniya
3. Клара Маатуис. Ответственное поведение в сфере цифровой безопасности: определение и модель оценки.
4. Коско и Пол, Information Society: Problems and Methods of Their Solution. Power, 7, 2003. P. 90-96.
5. Baskerville, Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. European Journal of Information Systems, 1, 121-130.1991, стр. 121

6. В.Яницкий, An Integrated Approach for Securing Electronic Transactions over the Web. Benchmarking: An International Journal, 9, P. 166-181
7. Ўзбекистон Республикаси Вазирлар Маҳкамасининг қарори, 05.09.2018 йилдаги 707-сон https://lex.uz/docs/3893085?ONDATE=05.04.2022
8. Ўзбекистон Республикасининг «Ахборот эркинлиги принциплари ва кафолатлари тўғрисида»ги қонуни // Ўзбекистон Республикаси Олий Мажлисининг Ахборотномаси. – 2003. – №1. – 2-м.
9. Аверченков В.И. Системы защиты информации в ведущих зарубежных странах: Учебное пособие. – Брянск, 2007.
10. Алферов А.П., Зубов А.Ю., Кузьмин А.С, Черемушкин А.В. Основы криптографии: Учебное пособие. – М., 2002.
11. Арипов М. , Пудовченко Ю. Е., Арипов М. Основы Интернет. – Т., 2003.
12. Безбогов А.А. Методы и средства защиты компьютерной информации. Учебное пособие. – Тамбов, 2006.
13. Давыдов А.С., Маслова Т.В. Информационные технологии в деятельности органов внутренних дел: Учебное пособие. – Челябинск, 2007.
14. Зайцев А.П., Голубятников И.В., Мещеряков Р.В. Программноаппаратные средства обеспечения информационной безопасности: Учебное пособие. – М., 2006.
15. Информационные технологии управления в органах внутренних дел: Учебник / Под ред. доцента Ю.А. Кравченко. – М., 1998.
16. Мельников В.П. и др. Информационная безопасность и защита информации: Учебое пособие. – М., 2008.
17. Казиев В.М. Введение в правовую информатику. – http://www.intuit.ru.