DOI - 10.32743/UniSoc.2024.108.5.17488

СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ ЦИФРОВОЙ ПРИВАТНОСТИ И ЕЁ РОЛИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

Бурнашев Ринат Фаритович
доц. кафедры «Гуманитарные науки и информационные технологии»,
Самаркандский государственный институт иностранных языков,
Республика Узбекистан, г. Самарканд
E-mail: burnashev1982@gmail.com

Шахрина Шерзоджоновна Шавкатова
студент,
Самаркандский государственный институт иностранных языков,
Республика Узбекистан, г. Самарканд

SOCIO-PHILOSOPHICAL ANALYSIS OF DIGITAL PRIVACY AND ITS ROLE IN ENSURING INFORMATION AND PSYCHOLOGICAL SECURITY

Rinat Burnashev
Associate Professor
of the Department of Humanities and Information Technologies
Samarkand State Institute of Foreign Languages,
Republic of Uzbekistan, Samarkand

Shakhrina Shavkatova
student,
Samarkand State Institute of Foreign Languages,
Republic of Uzbekistan, Samarkand

АННОТАЦИЯ

В научной статье рассматриваются ключевые аспекты цифровой приватности, включая философские, социальные и этические аспекты. В ходе анализа уделяется внимание как позитивным, так и негативным аспектам цифровой приватности, ее роли в защите личности и сохранении психологического благополучия. На основе проведенного анализа делаются выводы о необходимости сбалансированного подхода к управлению цифровой приватностью с учетом интересов как человека, так и общества в целом.

ABSTRACT

The scientific article examines the key aspects of digital privacy, including philosophical, social and ethical aspects. The analysis focuses on both positive and negative aspects of digital privacy, its role in protecting the individual and maintaining psychological well-being. Based on the analysis, conclusions are drawn about the need for a balanced approach to managing digital privacy, taking into account the interests of both the individual and society as a whole.

Ключевые слова: информационное общество, личность, цифровая приватность, философия, этика, информационно-психологическая безопасность.

Keywords: information society, personality, digital privacy, philosophy, ethics, information and psychological security.

Введение

В современном цифровом мире, где информационные технологии проникают во все сферы жизни человека, вопросы цифровой приватности становятся все более актуальными. Цифровая приватность относится к праву человека на контроль и защиту своей личной информации в онлайн-среде. Это включает в себя данные, которые мы делаем доступными через интернет, такие как личная переписка, финансовые транзакции, медицинская и социальная информация, и многое другое. Сохранение цифровой приватности становится все более сложной задачей в условиях постоянного развития цифровых технологий и роста угроз со стороны хакеров и киберпреступников.

Обзор литературы

Изучение существующих теорий и концепций цифровой приватности и информационно-психологической безопасности является ключевым аспектом в современном мире, где цифровые

Библиографическое описание: Бурнашев Р.Ф., Шавкатова Ш.Ш. СОЦИАЛЬНО-ФИЛОСОФСКИЙ АНАЛИЗ ЦИФРОВОЙ ПРИВАТНОСТИ И ЕЁ РОЛИ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ // Universum: общественные науки : электрон. научн. журн. 2024. 5(108). URL: *https://7universum.com/ru/social/archive/item/17488*

технологии играют все более значимую роль в повседневной жизни людей. Рассмотрим несколько основных теорий и концепций:

Концепция защиты данных ориентирована на защиту персональных данных от несанкционированного доступа, использования или раскрытия. Включает в себя различные методы шифрования, аутентификации и контроля доступа [1].

Принципы проектируемой приватности предполагает интеграцию защиты данных и приватности в проектирование системы или приложения на ранних стадиях разработки [2].

Модель угроз предполагает анализ потенциальных угроз безопасности для системы или данных, а также определение уязвимостей, которые могут быть использованы злоумышленниками [3].

Теория оправдания предлагает, что люди принимают решения о своей приватности на основе своего восприятия рисков и выгод [4].

Концепция социальной инженерии фокусируется на манипуляции людьми, чтобы они выполнили действия, которые могут быть вредными для безопасности информации, например, предоставление злоумышленнику доступа к системе [5].

Культурные аспекты приватности и безопасности могут различаться в разных культурах, что влияет на то, как люди воспринимают и реагируют на различные технологии [6].

Изучение этих теорий и концепций позволяет развивать более эффективные стратегии и методы защиты информации и обеспечения приватности в цифровой среде.

Методология исследования

Философский подход помогает нам осознать ценность приватности как фундаментального права личности. Философы размышляют о том, что такое личность, автономия, свобода, и как эти концепции переносятся в цифровую среду. Философский анализ этических аспектов сбора и использования персональных данных ставит вопросы о справедливости, согласии и человеческом достоинстве.

Идентификация ***социально-философских подходов*** к пониманию проблемы цифровой приватности может включать следующие основные направления:

Либертарианский подход к приватности обычно основывается на идее индивидуальной свободы и минимального вмешательства государства. Он подчеркивает важность защиты личной сферы и приватности от власти, будь то частные компании или правительство. Либертарианцы обычно выступают за сильное шифрование и анонимность в сети, а также против любых форм массового наблюдения [7].

Коммунитаризм и общественное доверие. Коммунитаристский подход к приватности подчеркивает важность общественного доверия и социальных норм для поддержания приватности. Он акцентирует взаимосвязь между личной и общественной сферами жизни, а также роль общественных институтов в обеспечении защиты приватности и безопасности граждан [8].

Феминистский подход. Феминистский анализ приватности обычно подчеркивает важность учета гендерных аспектов в вопросах приватности и безопасности. Он исследует, как различные социокультурные факторы, такие как гендерные роли и стереотипы, могут влиять на опыт приватности и уязвимость перед различными формами цифрового надзора и нарушений приватности [9].

Критическая теория и критика технологий. Подход, основанный на критической теории и критике технологий, анализирует социальные и политические аспекты технологических разработок и их влияние на приватность и безопасность. Он обращает внимание на распределение власти и ресурсов в цифровом обществе, а также на вопросы справедливости и равенства в доступе к технологиям [10].

Постколониальный подход. Постколониальный анализ приватности фокусируется на влиянии колониального наследия и глобализации на цифровую приватность. Он исследует, каким образом мировые структуры власти и экономические отношения влияют на приватность и безопасность жителей различных регионов мира [11].

Эти социально-философские подходы предоставляют различные ракурсы и инсайты в понимание проблемы цифровой приватности, помогая увидеть ее в контексте широкого спектра социальных, политических и культурных факторов.

Исследование современных ***технологических*** и ***политических*** инструментов по обеспечению цифровой приватности включает в себя ряд методов и подходов [12]:

Шифрование данных - один из основных технологических инструментов для защиты цифровой приватности. Шифрование позволяет защитить данные от несанкционированного доступа, шифруя информацию таким образом, чтобы она была непонятной для посторонних лиц.

Прокси-серверы и виртуальные частные сети позволяют маскировать IP-адрес пользователя, обеспечивая анонимность и защищенное соединение в интернете.

Браузеры с защитой приватности, такие как Tor и Brave, которые предоставляют инструменты для защиты приватности пользователей, например, блокировка отслеживания и приватный режим просмотра.

Методы анонимизации данных позволяют обрабатывать данные таким образом, чтобы сохранить их полезность для анализа, но при этом не раскрывать личную информацию о пользователях.

Многофакторная аутентификация обеспечивает дополнительный уровень безопасности, требуя не только пароль, но и другие формы идентификации, такие как SMS-коды или биометрические данные.

Законодательство и политические меры. Различные страны принимают законы и нормативные акты для защиты цифровой приватности граждан.

Открытые стандарты и протоколы способствуют созданию более прозрачных и безопасных технологий, позволяя разработчикам и экспертам проводить аудит и проверять их безопасность.

Обучение и осведомленность пользователей. Важно обучать пользователей основам цифровой безопасности и приватности, чтобы они могли принимать осознанные решения и использовать доступные инструменты для защиты своей личной информации.

Исследование этих современных технологических и политических инструментов помогает лучше понять, как обеспечить эффективную защиту цифровой приватности и разработать стратегии для борьбы с угрозами в онлайн-среде.

Результаты

Цифровая приватность в современном мире охватывает широкий спектр аспектов, связанных с защитой личной информации и сохранением приватности в онлайн-среде. Вот основные аспекты цифровой приватности:

Персональные данные. В современном мире большое количество персональных данных пользователей хранится и обрабатывается в цифровой форме. Это включает в себя такие данные, как имя, адрес, номера телефонов, электронные адреса, финансовая информация, медицинские записи и многое другое.

Онлайн-профилирование и отслеживание. Множество онлайн-сервисов и платформ собирают данные о действиях пользователей в интернете, чтобы предлагать персонализированный контент и рекламу. Это может включать в себя записи о поисковых запросах, просмотренных страницах, кликах, лайках и т.д.

Социальные сети и обмен информацией. Пользователи часто делятся личной информацией (фотографии, сообщения, местоположение и другие данные) в социальных сетях.

Электронная почта и переписка. Электронная почта является одним из основных способов коммуникации в цифровом мире. Сообщения, отправленные и полученные по электронной почте, могут содержать конфиденциальную информацию, которую необходимо защищать.

Мобильные устройства и приложения. Смартфоны и планшеты стали неотъемлемой частью повседневной жизни, и они часто содержат огромное количество личной информации. Мобильные приложения также могут запрашивать доступ к различным данным на устройствах, таким как контакты, камера, местоположение и др.

Биометрические данные. С развитием технологий биометрии стали активно использоваться для идентификации и аутентификации, например, отпечатки пальцев, распознавание лица, сканирование сетчатки глаза и т.д. Сбор и хранение биометрических данных также становится важным аспектом цифровой приватности.

Защита паролей и безопасность учетных записей. Управление паролями и безопасность учетных записей играют важную роль в обеспечении цифровой приватности. Слабые пароли или утечка учетных данных могут привести к серьезным нарушениям приватности.

Законодательство и нормативные акты. Различные страны и регионы принимают законы и нормативные акты, направленные на защиту данных граждан.

Эти основные аспекты цифровой приватности подчеркивают необходимость более осознанного подхода к управлению личной информацией и защите приватности в онлайн-среде.

Цифровая приватность имеет значительное влияние на ***информационно-психологическую безопасность***, которая относится к защите индивидуального психологического благополучия и здоровья в онлайн-среде. Вот несколько аспектов, в которых цифровая приватность влияет на информационно-психологическую безопасность:

Страх и тревожность. Нарушения приватности, такие как утечка личной информации или взлом учетных записей, могут вызывать у пользователей страх и тревожность относительно безопасности и конфиденциальности их данных. Это может привести к психологическим проблемам, таким как тревожные расстройства или потеря доверия к цифровым технологиям.

Психологическая безопасность в онлайн-коммуникациях. Цифровая приватность играет ключевую роль в обеспечении безопасности в онлайн-коммуникациях, таких как электронная почта, социальные сети, мессенджеры и видеоконференции. Нарушения приватности могут привести к чувству небезопасности и ограничения свободы выражения мнения.

Конфиденциальность медицинских данных. Защита конфиденциальности медицинских данных имеет особое значение для информационно-психологической безопасности. Нарушение приватности в этой области может вызвать серьезные психологические последствия, такие как стыд, страх или потеря доверия к медицинским учреждениям.

Цифровой сталкинг и кибербуллинг. Нарушения цифровой приватности могут стать предпосылкой для цифрового сталкинга и кибербуллинга, что может иметь серьезные психологические последствия для жертв, включая тревожность, депрессию и даже мысли о суициде.

Психологические аспекты использования социальных сетей. Многие социальные сети и онлайн-платформы собирают и анализируют данные о поведении пользователей для персонализации контента и рекламы. Это может привести к чувству недостатка контроля над личной информацией и к психологическим проблемам, связанным с чувством невидимого наблюдения и манипуляции.

Цифровая приватность и информационно-психологическая безопасность тесно взаимосвязаны, и обеспечение приватности в онлайн-среде является важным аспектом поддержания психологического благополучия и безопасности пользователей.

Обсуждение

Интерпретация результатов социально-философского анализа цифровой приватности и её роли в обеспечении информационно-психологической безопасности позволяет рассмотреть

эту проблему в контексте социальных и философских аспектов, влияющих на психологическое благополучие и безопасность в цифровом мире. Вот несколько ключевых выводов:

Приватность как основополагающий принцип психологического благополучия. Результаты анализа подтверждают, что защита цифровой приватности играет ключевую роль в обеспечении психологического благополучия людей в онлайн-среде. Ощущение контроля над своей личной информацией и приватностью способствует чувству безопасности и комфорта в интернете.

Влияние социальных норм и ценностей на восприятие приватности. Результаты анализа показывают, что социальные нормы и ценности оказывают значительное влияние на то, как люди воспринимают и ценят свою цифровую приватность. Например, в культуре, где приватность ценится выше, люди могут быть более чувствительны к нарушениям приватности и более активно защищать свои данные.

Технологические инновации и риск для психологической безопасности. Анализ подчеркивает, что с развитием технологий возникают новые угрозы для психологической безопасности, связанные с нарушением приватности и контролем над данными. Например, алгоритмы машинного обучения и аналитика данных могут использоваться для манипуляции поведением пользователей, что может негативно сказаться на их психологическом состоянии.

Образование и осведомленность как факторы защиты приватности. Результаты анализа указывают на важность образования и повышения осведомленности о цифровой приватности для обеспечения информационно-психологической безопасности. Чем более осведомлены пользователи о своих правах и мерах защиты данных, тем больше они могут сделать, чтобы защитить свою приватность и психологическое благополучие.

Социальные неравенства и уязвимость. Исследование подчеркивает, что социальные неравенства могут сделать определенные группы населения более уязвимыми перед угрозами нарушения приватности и психологического воздействия в цифровом пространстве. Например, меньшая доступность ресурсов и знаний о защите данных может увеличить риск для психологической безопасности уязвимых групп.

Интерпретация результатов социально-философского анализа цифровой приватности и её роли в обеспечении информационно-психологической безопасности позволяет лучше понять взаимосвязь между защитой приватности, социокультурными факторами и психологическим благополучием в цифровой эпохе. Это помогает выявить ключевые проблемы и разработать соответствующие стратегии для обеспечения безопасности и комфорта пользователей в онлайн-среде.

Выявление ***этических*** и ***философских аспектов*** цифровой приватности и информационной безопасности позволяет рассмотреть эти проблемы с точки зрения ценностей, норм и принципов, лежащих в основе общественной этики и философии:

Принцип автономии и права на приватность. Цифровая приватность напрямую связана с принципом автономии, который подчеркивает право индивида контролировать свою личную информацию и принимать решения о её использовании. Этот аспект поднимает вопросы о том, каким образом технологические инновации и практики сбора данных могут ограничивать или усиливать автономию людей.

Справедливость и равенство в доступе к безопасности данных. Философский аспект справедливости поднимает вопросы о том, кто имеет доступ к средствам обеспечения безопасности данных и кто остается уязвимым перед угрозами. Неравенство в доступе к технологиям и ресурсам может усугубить существующие социальные неравенства и создать этические проблемы.

Этика использования данных и цифрового наблюдения. Использование данных для целей массового наблюдения и манипуляции поднимает вопросы о том, каким образом это вмешивается в частную жизнь и автономию людей. Это вызывает этические дилеммы относительно баланса между безопасностью и защитой приватности, а также между общественными интересами и индивидуальными правами.

Этика обмена данных и бизнес-моделей в интернете. Модели бизнеса, основанные на сборе, анализе и монетизации данных, поднимают вопросы о честности, прозрачности и согласии в отношении использования личной информации пользователей.

Выявление этических и философских аспектов цифровой приватности и информационной безопасности помогает глубже понять основы этических решений и принципов, лежащих в основе разработки политик и практик в этой области. Это помогает развивать более этичные и социально ответственные подходы к управлению данными и обеспечению безопасности в цифровом мире.

Заключение

В ходе данного социально-философского анализа было выявлено, что цифровая приватность не только является основой для защиты личных данных и личной жизни граждан, но также оказывает значительное влияние на психологическое благополучие и социальную стабильность.

Уровень цифровой приватности напрямую связан с уровнем доверия общества к цифровым технологиям и организациям, обрабатывающим персональные данные. Кроме того, цифровая приватность определяет границы между правом на конфиденциальность и интересами общества и государства. Поэтому в развитии политики по защите цифровой приватности необходимо учитывать как индивидуальные права, так и общественные интересы, соблюдая баланс между ними. Развитие и реализация политики по защите цифровой приватности должны основываться на комплексном подходе, учитывающем как технические, так и социальные и этические аспекты, с целью обеспечения информационно-психологической безопасности и устойчивого развития цифрового общества.

Список литературы:

1. Китова Е.Б., Мельгунова А.Г. Отражение ценностной иерархии общества в концепциях data protection «защита данных» и freedom of information «свобода информации» //Вопросы теории и практики журналистики. – 2019. – Т. 8. – №. 2. – С. 330-341.
2. Симонова С.В. Обработка данных пользователей цифровых платформ: актуальные вопросы совершенствования законодательства и практик //Вестник ЯрГУ. Серия Гуманитарные науки. – 2022. – Т. 16. – №. 4. – С. 642-649.
3. Буйневич М.В., Покусов В.В., Израилов К.Е. Модель угроз информационно-технического взаимодействия в интегрированной системе защиты информации //Информатизация и связь. – 2021. – №. 4. – С. 66-73.
4. Агадуллина Е.Р. и др. Теория оправдания системы: новый взгляд на проблему неравенства // Современная зарубежная психология. – 2021. – Т. 10. – №. 1. – С. 132-141.
5. Равочкин Н.Н. Идея как инструмент социальной инженерии: философский анализ // Социодинамика. – 2019. – №. 12. – С. 237-255.
6. Бурнашев Р.Ф., Асророва М.О., Масарова К.Ф. Философские основы концепции безопасности личности в эпоху цифровизации //Universum: общественные науки. – 2023. – №. 11 (102). – С. 33-39.
7. Обухов А.А., Языкова Н.А. Контекстный подход к объяснению дифференцированного восприятия государства в различных социумах //Гуманитарный вектор. – 2019. – Т. 14. – №. 2. – С. 27-32.
8. Молчанов А.В. Коммунитаризм как альтернатива классическим идеологиям //Pro nunc. Современные политические процессы. – 2017. – №. 1 (17). – С. 51-57.
9. Кострицкая Т.А. Приватное и публичное в социально-философской традиции и феминистской теории: сравнительный анализ //Аспирантский вестник Поволжья. – 2019. – №. 3-4. – С. 28-32.
10. Бурнашев Р. Философский анализ концепции информационного общества //Namangan davlat universiteti Ilmiy axborotnomasi. – 2023. – №. 9. – С. 194-202.
11. Якимова Е.В. Эмоции в публичной сфере: новые аналитические подходы //Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 11, Социология: Реферативный журнал. – 2023. – №. 2. – С. 42-61.
12. Володенков С.В. Трансформация современных политических процессов в условиях цифровизации общества: ключевые сценарии //Контуры глобальных трансформаций: политика, экономика, право. – 2020. – Т. 13. – №. 2. – С. 6-24.