УДК: 101:330.101. (575.2) (04)

***[1]Козубаев О.***
*доктор философских наук, профессор*
***Козубаев О.***
*философия илимдеринин доктору, профессор*
***Kozubaev Oskonbai***
*doctor of philosophical sciences, professor*

***[2]Камбарова Н. Н.,*** *соискатель*
***Камбарова Н.Н.,*** *изденүүчү*
***Kambarova N.N.,*** *applicant*

*[1]Национальная Академия наук Кыргызской Республики*
*Кыргыз Республикасынын Улуттук илимдер Академиясы*
*National Academy of Sciences of the Kyrgyz Republic*

*[2]Ошский государственный университет*
*Ош мамлекеттик университети*
*Osh State University*

# СОЦИОКУЛЬТУРНЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
# МААЛЫМАТТЫК КООПСУЗДУКТУН СОЦИОМАДАНИЙ АСПЕКТИЛЕРИ
# SOCIO-CULTURAL ASPECTS INFORMATION SECURITY

**Аннотация.** В данной статье рассматриваются социокультурные аспекты информационной безопасности. Информационные интересы включают в себя общественные информационные потребности и интересы, которые в свою очередь направлены на обеспечение свободного обмена информацией и взаимодействия между различными общественными институтами, организациями и гражданами. Основной целью является обеспечение информационных интересов общества, общественных организаций и интересов личности. Это включает в себя свободу доступа к информации, укрепление реальной демократии, развитие социально-правового общества, поддержание общественного согласия и обеспечение социального контроля.

**Ключевые слова:** информационная безопасность, национальная безопасность, духовная безопасность, информационные технологии, глобализация, общественные организации, гражданин, государство, личность.

**Аннотация**. Аталган макалада маалыматтык коопсуздуктун социомаданий аспектилери изилденет. Коомдун маалыматтык кызыкчылыктарына социалдык маалыматтык керектөөлөр жана кызыкчылыктар кирет, алар өз кезегинде ар кандай мамлекеттик мекемелердин, уюмдардын жана жарандардын ортосунда эркин маалымат алмашууну жана өз ара аракеттенүүнү камсыз кылууга багытталган. Негизги максат - коомдун, коомдук уюмдардын, инсандын маалыматтык кызыкчылыктарын камсыз кылуу болуп саналат. Бул маалымат алуу

эркиндигин, чыныгы демократияны чыңдоону, социалдык-укуктук коомду өнүктүрүүнү, коомдук ынтымакты сактоону жана социалдык көзөмөлдү камсыз кылууну камтыйт.

**Негизги сөздөр**: маалыматтык коопсуздук, улуттук коопсуздук, руханий коопсуздук, маалыматтык технологиялар, ааламдашуу, коомдук уюмдар, жаран, мамлекет, инсан.

**Abstract.** This article of the author discusses the socio-cultural aspects of information security, it also says that the information security of society is to ensure the information interests of society as a whole. These interests include public information needs and interests, which in turn are aimed at ensuring the free exchange of information and interaction between various public institutions, organizations and citizens. The goal here is to ensure the information interests of society, public organizations and the interests of the individual in terms of their information rights. This includes freedom of access to information, the strengthening of real democracy, the development of a social and legal society, the maintenance of social harmony and the provision of social control.

**Key words:** information security, national security, spiritual security, information technology, globalization, public organizations, citizen, state, individual.

Информационная безопасность на практике представляет собой сложное, многогранное и многоуровневое явление. В более общем смысле безопасность можно рассматривать как ощущение защищенности в повседневной жизни, отсутствие внешних угроз, состояние защищенности интересов личности, общества и государства от внутренних и внешних опасностей. Также это может быть способностью объекта, явления или процесса сохраняться при разрушительных воздействиях [1]. С юридической точки зрения, информационная безопасность представляет собой государственную доктрину, определяющую конституционные рамки информационной безопасности государства. Кроме того, существуют социально-психологические аспекты информационной безопасности [2]. Безопасность может проявляться в различных аспектах, включая и экономический аспект. Одним из важных аспектов является национальная безопасность, которая охватывает защиту интересов и ценностей страны в целом. В современной философской дискуссии все больше внимания уделяется духовной безопасности как форме защиты, связанной с внутренним миром человека и его духовными ценностями [3].

Однако не следует забывать и о собственно информационной безопасности, которая становится все более актуальной. В эпоху информационных технологий и глобальной связанности защита информации и данных приобретает особое значение. Вмешательство в информационные системы может иметь серьезные последствия для личной жизни, экономики, а также для функционирования государственных институтов. Итак, безопасность имеет разнообразные проявления: экономические, национальные, духовные и информационные. Понимание и обеспечение всех этих аспектов являются важными задачами современного общества.

Информационная безопасность в самом общем смысле определяется как состояние, включающее свободу от угроз и опасностей, отсутствие страха, беспокойства и тревоги, а также обеспечение сохранности информации и защиту от несанкционированных вторжений извне. В этом контексте понятие безопасности охватывает разнообразные аспекты: оно выступает как характеристика состояния конкретной системы, как психологическое ощущение уверенности, как идея или концепция, а также как набор конкретных мер, направленных на достижение данного состояния [4, 98–103-б.].

С технической точки зрения информационная безопасность означает обеспечение защищенности информационной среды и самих данных. Это включает в себя специальные меры и действия, направленные на предотвращение несанкционированного

проникновения в информационные ресурсы, предотвращение утечки информации, подделки данных, несанкционированного коммерческого использования и незаконной передачи информации третьим лицам без согласия владельцев и правообладателей. Эффективная техническая информационная безопасность включает в себя использование современных методов шифрования, многоуровневых систем аутентификации, систем мониторинга и обнаружения вторжений, установку брандмауэров и антивирусных программ, а также регулярное обновление и патчинг программного обеспечения для устранения уязвимостей. Целью технических мер по обеспечению информационной безопасности является создание надежной и защищенной среды для обработки, хранения и передачи информации, минимизация рисков, связанных с угрозами и атаками на информацию и информационные системы.

Когда речь идет о безопасности, важно учитывать, что она всегда связана с защитой определенного субъекта. В зависимости от того, кто является участником информационных взаимодействий, и чьи информационные интересы и потребности могут быть подвергнуты риску, информационная безопасность делится на информационную безопасность организаций, производственных, коммерческих и финансовых объединений, а также корпораций; и на информационную безопасность общества, государства, отдельных личностей и человека. Каждая из этих сфер требует уникальных подходов и мер по обеспечению безопасности. Организации и предприятия могут ориентироваться на защиту корпоративных данных, коммерческой тайны и финансовых операций. В то время как информационная безопасность общества, государства и личности может включать в себя защиту персональных данных граждан, кибербезопасность государственных систем, а также обеспечение надежных средств коммуникации и доступа к информации для всех членов общества.

Мы сосредоточимся на информационной безопасности общества, государства, личности и человека. В контексте информационной безопасности организаций, производственных, коммерческих, торгово-финансовых объединений и корпораций, акцент смещается на специфическую деятельность их структур и руководителей с целью обеспечения надежной защиты организационной информации. Такая защита гарантирует сохранность данных, эффективное их использование и нормальное функционирование информационных процессов внутри организации. Основная задача здесь — предотвращение утечек информации и негативных последствий от несанкционированных вторжений. Тем не менее, стоит отметить, что обеспечение информационной безопасности организаций и корпораций является неотъемлемым условием для обеспечения информационной безопасности общества и государства. В данном контексте реализация мер, направленных на сохранение данных, эффективное функционирование информационных процессов, а также предотвращение негативных последствий, в основном имеют технический характер, сконцентрированный на практической реализации технологий и процедур.

Информационная безопасность общества заключается в обеспечении информационных интересов общества в целом. Эти интересы включают в себя общественные информационные потребности и интересы, которые в свою очередь направлены на обеспечение свободного обмена информацией и взаимодействия между различными общественными институтами, организациями и гражданами. Целью здесь является обеспечение информационных интересов общества, общественных организаций и интересов личности в части их информационных прав. Это включает в себя свободу доступа к информации, укрепление реальной демократии, развитие социально-правового общества, поддержание общественного согласия и обеспечение социального контроля. Для достижения этой цели важно создание условий, в которых информационные процессы будут прозрачными, недискримина-

ционными и доступными для всех членов общества. Основополагающими аспектами являются укрепление свободы слова и медиа, обеспечение конфиденциальности данных, а также обеспечение гарантий против незаконного монополизма и контроля над информацией, что в свою очередь содействует устойчивому развитию общества.

Информационная безопасность государства заключается в создании условий для эффективного формирования информационной среды и инфраструктуры, которые соответствуют действующему законодательству и Конституции, а также учитывают сложившуюся социальную практику. Эти условия обеспечивают реализацию конституционных прав и свобод общества, общественных организаций и граждан в сфере доступа к открытым информационным ресурсам, свободного информационного взаимодействия, получения необходимой информации и её использования с целью обеспечения эффективного функционирования государства. Информационная безопасность государства также направлена на поддержание незыблемости конституционного строя, государственного устройства и территориальной целостности, государственного суверенитета, а также на достижение социальной и политической стабильности. Она охраняет государственные информационные интересы и потребности, обеспечивая эффективное функционирование государственных структур, при этом ставя перед собой задачи обеспечения законности и правопорядка, поддержания мира и согласия, содействия бесконфликтному взаимодействию с гражданским обществом, равноправному и взаимовыгодному внутригосударственному и международному сотрудничеству. Обеспечение информационной безопасности государства способствует гармоничному и динамичному развитию страны, создает основу для устойчивого функционирования и способствует достижению целей и задач, стоящих перед государством.

Одним из ключевых аспектов обеспечения информационной безопасности государства является защита информации. Защита информации представляет собой комплекс мер, направленных на обеспечение целостности, конфиденциальности и доступности информации, при этом предоставляя доступ к ней общественным организациям и личностям. Защита информации охватывает систематический набор государственных мероприятий, направленных на предотвращение утраты информации, неправомерного проникновения в информационные ресурсы и незаконного использования информации. Это также включает в себя предотвращение использования информации с нарушением авторских прав и прав владельцев и собственников данных.

Ключевые цели защиты информации:

• Обеспечение целостности: гарантирование неприкосновенности информации от изменений или повреждений, чтобы она оставалась точной и достоверной.

• Обеспечение конфиденциальности: защита конфиденциальных данных от несанкционированного доступа, чтобы предотвратить раскрытие информации неавторизованным лицам.

• Обеспечение доступности: обеспечение того, чтобы информация была доступна для тех, кто имеет на то право, и в нужное время.

Для достижения этих целей применяются технические, организационные и правовые меры, такие как шифрование данных, контроль доступа, мониторинг активности, обучение персонала и разработка соответствующего законодательства. Это помогает гарантировать, что информация остается защищенной и используется в соответствии с установленными нормами и правилами. Мероприятия по защите информации включают в себя не только защиту самой информации, но также защиту прав на владение и пользование информацией, защиту от незаконного распространения, разглашения коммерческой, служебной и государственной информации, а также защиту информационных ресурсов и технологий.

В рамках этих мероприятий объектами защиты являются:

- Информация и её целостность.
- Носители информации, такие как физические носители (диски, документы), а также электронные носители (серверы, компьютеры).
- Информационные процессы, включая передачу, обработку и хранение данных.
- Технические средства информации, включая компьютеры, сетевое оборудование и программное обеспечение.
- Системы информационной связи, обеспечивающие передачу данных между участниками.

Средства защиты включают разнообразные меры и действия:

- Меры правового порядка, такие как законы, нормы и указы, регулирующие защиту информации и наказывающие за нарушения.
- Специальные действия и государственные акты, направленные на обеспечение безопасности информации, включая лицензирование информации, сертификацию информационных ресурсов и разработку стандартов использования.
- Государственная аттестация процессов информатизации, оценка соответствия стандартам и проведение информационно-технических экспертиз.

Эти меры и средства направлены на обеспечение надежной защиты информации и информационных ресурсов, а также на соблюдение правовых и нормативных требований в сфере информационной безопасности.

Информационная безопасность личности действительно связана с созданием окружающей среды, в которой человек может жить и функционировать как социальное существо. Она направлена на обеспечение информационного суверенитета личности, сохранение её личных ценностей и индивидуальности, а также на создание условий, при которых человек освобождается от различных форм информационных агрессий и манипуляций сознанием и поведением. Основные аспекты информационной безопасности личности: информационный суверенитет личности: возможность человека контролировать свою информационную среду и решать, какая информация ему доступна, а какая – нет; защита личных ценностей: обеспечение сохранности личных данных, права на конфиденциальность и неприкосновенность личной жизни. свобода выбора и решения: создание условий, при которых человек может принимать собственные решения, свободно выбирать свою модель поведения и воздействие на его сознание минимизировано; противостояние информационным агрессиям: защита от воздействий, направленных на манипулирование сознанием, внушение ложных убеждений и угрозы информационной безопасности.

Эти понятия и меры, такие как информационный суверенитет личности, сохранение личных ценностей и свобода выбора, могут быть предметом философского рассмотрения, так как они касаются основных прав и ценностей человека в современном информационном обществе. Философский анализ помогает понять их этические, социальные и культурные аспекты и разработать подходы к обеспечению информационной безопасности личности [5].

Информационная безопасность личности действительно имеет важное взаимодействие с информационной безопасностью общества и государства. Она является частью общей системы обеспечения безопасности в информационном обществе. Существуют несколько ключевых аспектов, которые следует выделить:

*Взаимосвязь и влияние:* Информационная безопасность личности тесно связана с безопасностью общества и государства. Если информационная безопасность общества и государства нарушена, это может негативно повлиять на безопасность личности. В то же время, если личная информация подвергается угрозам и атакам, это может иметь отрицательное воздействие на общественную и государственную безопасность.

*Сходства и различия:* хотя информационная безопасность личности имеет общие параметры с информационной безопасностью общества и государства, она также имеет уникальные аспекты. Это связано с индивидуальными правами и интересами личности, её специфическими потребностями и уязвимостями.

*Цифровое неравенство:* одним из значимых аспектов информационной безопасности личности является цифровое неравенство. Ограниченный доступ к современным средствам коммуникации может создавать неравенство в возможностях получения информации, участия в цифровых процессах и защиты личных данных. Это может сказаться на социальных группах, у которых доступ ограничен.

*Цивилизационный характер:* информационная безопасность личности отражает характер информационных процессов и ценностей в данной цивилизации. Сложившиеся условия и принятые стандарты влияют на восприятие и обеспечение безопасности личных данных.

*Значение обеспечения общей безопасности:* обеспечение информационной безопасности личности является важной составляющей для обеспечения общей безопасности общества и государства. Без надлежащей защиты личных данных и интересов граждан, трудно обеспечить устойчивость и стабильность информационного пространства в целом.

Итак, в конце нашей статьи следует отметить, что философский анализ этих вопросов помогает осознать глубокие социальные, этические и культурные аспекты информационной безопасности и разработать эффективные стратегии для обеспечения этой безопасности на уровне как личности, так и общества.

**Литература**

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. Артамонова, Я.С. Информационная безопасность и социальный конфликт в современной России: автореф. дис. … канд. социол. наук / Я.С. Артамонова. – Волгоград, 2006. – 25 с.

4. 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.

5. Цифровой барьер [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Цифровой_барьер