**МИНОБРНАУКИ РОССИИ**

Федеральное государственное бюджетное

образовательное учреждение высшего образования

**«Ухтинский государственный технический университет»**

**(УГТУ)**

Кафедра вычислительной техники, информационных систем и технологий

**РЕФЕРАТ**

Дисциплина «Международные и отраслевые стандарты

в области информационных технологий»

Тема «Сертификация и стандартизация»

Шифр 221378 Группа ИСТ-22-оз-М Курс 2

Шарфина Екатерина Сергеевна

Проверил:

доцент кафедры ВТИСиТ И. А. Базарова

Ухта

2024

СОДЕРЖАНИЕ

[Введение 3](#_Toc159410545)

[Сущность сертификации 4](#_Toc159410546)

[Сертификация в области защиты информации 6](#_Toc159410547)

[Международные акты обеспечения информационной безопасности 10](#_Toc159410548)

[Отечественное регулирование в сфере информационной безопасности 13](#_Toc159410549)

[Органы добровольной и обязательной сертефикации в России 17](#_Toc159410550)

[Заключение 19](#_Toc159410551)

[Список использованной литературы 22](#_Toc159410552)

# ВВЕДЕНИЕ

Сертификация является неотъемлемой частью современного производства и торговли. Этот процесс подтверждения соответствия продукции или услуг нормативным требованиям играет важную роль в обеспечении качества и безопасности товаров для потребителей. Сертификационные органы выступают в качестве независимых сторон, удостоверяя соответствие продукции установленным стандартам.

Сертификация дает возможность предприятиям доказать, что их продукция соответствует высоким стандартам качества и безопасности. Это позволяет компаниям укрепить свою репутацию на рынке и повысить доверие потребителей. Однако процесс сертификации также может быть сложным и требовать значительных затрат времени и ресурсов.

В контексте рыночной экономики сертификация становится необходимым инструментом для обеспечения конкурентоспособности продукции на мировом рынке. Она помогает предприятиям доказать свою способность производить товары и услуги, соответствующие международным стандартам.

Государственные интересы также играют важную роль в процессе сертификации. Государство стремится обеспечить безопасность и качество продукции для своих граждан, одновременно поддерживая развитие предпринимательства. Поэтому баланс между обеспечением качества и доступностью сертификации является ключевым в этом процессе.

В данной работе будет рассмотрено понятие сертификации и методы её проведения, а так же нормативно-правовые документы и стандарты в области защиты информации и информационной безопасности. Отечественное организационное, правовое и нормативное обеспечении и регулирование в сфере информационной безопасности. Система менеджмента информационной безопасности.

# Сущность сертификации

Сертификация — это процедура подтверждения соответствия результата производственной деятельности, товара, услуги нормативным требованиям, посредством которой третья сторона документально удостоверяет, что продукция, работа (процесс) или услуга соответствует «заданным требованиям».

Таким образом, Сертификация — основное средство в условиях рыночной экономики, позволяющее гарантировать соответствие продукции требованиям нормативной документации. С позиции государственных интересов, такой инструмент, как Сертификация, должен, с одной стороны, обеспечить улучшение качества продукции и услуг и гарантию безопасности их для потребителя, а с другой — не служить препятствием для развития предпринимательства, процедурно и финансово усложняя процесс получения Сертификата.

Перед началом рассмотрения системы подтверждения соответствия, созданной в настоящее время в нашей стране, и анализом законодательства в этой области необходимо привести используемые в последующем определения терминов и понятий, введенных различными нормативно-правовыми актами Российской Федерации. Сертификация — деятельность третьей стороны, независимой от изготовителя (продавца) и потребителя продукции, по подтверждению соответствия продукции установленным требованиям.

Сертификация направлена на достижение следующих целей:

* содействие потребителям в компетентном выборе продукции (услуги);
* содействие экспорту и повышению конкурентоспособности продукции;
* защита потребителя от недобросовестности изготовителя (продавца, исполнителя);
* контроль безопасности продукции (услуги, работы) для окружающей среды, жизни, здоровья и имущества;
* подтверждение показателей качества продукции (услуги, работы), заявленных изготовителем (исполнителем);
* создание условий для деятельности предприятий, учреждений, организаций и предпринимателей на едином товарном рынке Российской Федерации, а также для участия в международном экономическом, научно-техническом сотрудничестве и международной торговле.

# Сертификация в области защиты информации

Под сертификацией средств защиты информации (СЗИ) по требованиям безопасности информации (далее сертификация) понимается проверка (подтверждение) характеристик СЗИ на соответствие требованиям государственных стандартов или иных нормативных документов по защите информации, выпущенные уполномоченными федеральными органами: ФСТЭК России (Гостехкомиссией России), ФСБ России и Министерство обороны.

Вся система сертификации обеспечивает достижение прежде всего национальной безопасности в сфере информатизации. Не менее важным является формирование и осуществление единой научно - технической и промышленной политики в сфере информатизации. А так же содействие формированию рынка защищенных информационных технологий и средств их обеспечения, регулирование и контроль разработки, а также последующего производства средств защиты информации, помощь потребителям в компетентном выборе средств защиты информации, защита потребителя от недобросовестности исполнителя (продавца, изготовителя), подтверждение показателей качества продукции.

Поскольку обязательная сертификация информационных средств в России не применяется, все виды сертификатов в этой области выдаются в добровольном порядке. Их делят на две укрупненные категории:

* корпоративные, которые подтверждают соответствие политики компании требованиям информационной безопасности;
* персональные, подтверждающие уровень квалификации конкретного специалиста в этой сфере.

Одним из самых авторитетных инструментов в корпоративной сфере является сертификация систем менеджмента информационной безопасности ISO 27001. Она признана во всем мире в качестве эталонной при оценке политики компании в данной предметной области. Кроме этого, в реестре зарегистрированных систем добровольной оценки соответствия, ведение которого осуществляет Росстандарт, значатся еще несколько десятков комплексов критериев, которые применяются компаниями для подтверждения своей ответственной позиции в этом вопросе.

За производство и поддержку сертифицированных СЗИ отвечают Заявители. Согласно нормативным документам Заявители должны:

* обеспечивать соответствие средств защиты информации требованиям нормативных документов;
* принимать меры для обеспечения соответствия и стабильности характеристик каждого выпускаемого экземпляра характеристикам эталонного экземпляра, который непосредственно подвергался сертификационным испытаниям;
* осуществлять подготовку материалов для безопасного внедрения и эксплуатации сертифицированных СЗИ и доводить их до пользователей;
* предоставлять сопроводительные документы установленного образца на каждый экземпляр сертифицированного СЗИ;
* осуществлять маркировку и учет каждого произведенного экземпляра и предоставлять доступ к учетной информации должностным лицам уполномоченных органов;
* осуществлять проверку (сертификацию) доработок и исправлений сертифицированных СЗИ и обеспечивать их доведение до пользователей.

Заявители осуществляют свою работу на основании лицензий, выдаваемых уполномоченными федеральными органами. В ряде случае правообладатели поручают организацию сертификации и производства сертифицированных версий продуктов организациям, имеющим соответствующие лицензии. Как правило, эти организации осуществляют дальнейшую сертификационную поддержку производимых продуктов.

Сертификация в области защиты информации обеспечивает безопасность и конфиденциальность данных как на уровне государства, так и на уровне отдельных компаний. Процесс сертификации СЗИ позволяет убедиться в соответствии средств защиты информации требованиям государственных стандартов и обеспечить надежную защиту от утечек и несанкционированного доступа к информации.

Одним из важных аспектов сертификации является формирование рынка защищенных информационных технологий и содействие компаниям в выборе эффективных средств защиты информации. Корпоративные сертификаты, подтверждающие соответствие политики компании требованиям информационной безопасности, играют важную роль в формировании доверия к бизнесу и защите интересов компаний и их клиентов.

Сертификация систем менеджмента информационной безопасности ISO 27001 является одним из самых авторитетных инструментов в области защиты информации. Этот стандарт признан международным сообществом и помогает компаниям оценить свою политику безопасности и повысить уровень защиты данных.

Заявители, отвечающие за производство и поддержку сертифицированных СЗИ, обеспечивают соответствия средств защиты информации требованиям нормативных документов. Они обязаны обеспечивать стабильность характеристик продукции, предоставлять необходимые документы пользователям и осуществлять маркировку каждого экземпляра сертифицированного СЗИ.

В целом, сертификация в области защиты информации способствует повышению уровня безопасности данных, формированию доверия к информационным технологиям и развитию отрасли. Добровольный характер сертификации позволяет компаниям самостоятельно выбирать подходящие стандарты и стратегии защиты, соответствующие их потребностям и целям.

Сертификация в области защиты информации также способствует повышению конкурентоспособности компаний на рынке, так как сертифицированные продукты и услуги могут быть привлекательнее для потенциальных клиентов, которые ценят безопасность и конфиденциальность своих данных. Кроме того, процесс сертификации помогает компаниям улучшить свои внутренние процессы и стандартизировать подходы к защите информации, что способствует эффективному управлению рисками и обеспечению стабильности в работе организации.

Сертификация в области защиты информации обеспечивает безопасность данных и конфиденциальность информации. Она позволяет убедиться в том, что организация следует определенным стандартам и требованиям по защите информации, что в свою очередь способствует предотвращению утечек данных, хакерским атакам и другим угрозам. Сертификация также помогает повысить доверие клиентов и партнеров к организации, демонстрируя ее готовность и способность обеспечивать безопасность информации.

Одной из основных проблем, которые решает сертификация в области защиты информации, является установление стандартов и процедур для защиты данных. Это позволяет организациям более эффективно управлять рисками, связанными с утечками информации, и обеспечить соответствие законодательным требованиям в области защиты данных. Кроме того, сертификация способствует повышению осведомленности сотрудников о правилах безопасности информации и обучению их соответствующим методам защиты, что также снижает вероятность возникновения инцидентов безопасности.

# Международные акты обеспечения информационной безопасности

Международные правовые и нормативные акты играют большую роль в обеспечении информационной безопасности процессов переработки информации в современном мире. С увеличением объемов передаваемой и обрабатываемой информации становится все более важным разработка и принятие международных стандартов и норм, направленных на защиту данных от утечек, несанкционированного доступа и других угроз.

Международные правовые акты в области информационной безопасности создают базу для сотрудничества между государствами, организациями и компаниями в целях обеспечения защиты информации на международном уровне. Они определяют общие принципы и требования, которым должны соответствовать все участники процессов переработки информации, чтобы обеспечить ее надежную защиту.

Соблюдение международных правовых и нормативных актов по информационной безопасности является необходимым условием для успешного функционирования современных информационных систем и процессов обработки данных. Эти акты способствуют установлению единого стандарта защиты информации на международном уровне и содействуют повышению доверия к электронным коммуникациям и цифровым технологиям.

Цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей.

В международной практике обеспечения ИБ основными направлениями являются:

- нормирование компьютерной безопасности по критериям оценки защищённости надёжных систем и информационных технологий;

- стандартизация процессов создания безопасных информационных систем.

Рассмотрим американский "Закон об информационной безопасности". Его цель - реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Такая программа должна включать:

- периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;

- правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;

- обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;

- периодическую проверку и (пере)оценку эффективности правил и процедур;

- действия при внесении существенных изменений в систему;

- процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь; организовать взаимодействие с правоохранительными органами.

Международные правовые и нормативные акты обеспечивают информационную безопасность в современном мире, где объемы передаваемой и обрабатываемой информации постоянно растут. Разработка и принятие международных стандартов и норм, направленных на защиту данных от различных угроз, становятся все более важными. Эти акты создают базу для сотрудничества между государствами, организациями и компаниями, обеспечивая единые принципы и требования для надежной защиты информации.

Соблюдение международных правовых и нормативных актов по информационной безопасности является необходимым условием для успешного функционирования современных информационных систем и процессов обработки данных. Они способствуют установлению единого стандарта защиты информации на международном уровне и повышают доверие к электронным коммуникациям и цифровым технологиям. Цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей, что важно для обеспечения стабильности и безопасности информационного пространства.

В международной практике обеспечения информационной безопасности акцент делается на нормировании компьютерной безопасности по критериям оценки защищенности систем и стандартизации процессов создания безопасных информационных систем.

# Отечественное регулирование в сфере информационной безопасности

Законодательный уровень является важнейшим для обеспечения информационной безопасности. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

На законодательном уровне различаются две группы мер:

- меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности (меры ограничительной направленности);

- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

Основным законом Российской Федерации является Конституция, принятая 12 декабря 1993 года.

В соответствии со статьей 24 Конституции, органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом.

Статья 41 гарантирует право на знание фактов и обстоятельств, создающих угрозу для жизни и здоровья людей, статья 42 - право на знание достоверной информации о состоянии окружающей среды.

В принципе, право на информацию может реализовываться средствами бумажных технологий, но в современных условиях наиболее практичным и удобным для граждан является создание соответствующими законодательными, исполнительными и судебными органами информационных серверов и поддержание доступности и целостности представленных на них сведений, то есть обеспечение их (серверов) информационной безопасности.

Основополагающим среди российских законов, посвященных вопросам информационной безопасности, следует считать закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года номер 24-ФЗ (принят Государственной Думой 25 января 1995 года). В нем даются основные определения и намечаются направления развития законодательства в данной области.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;

- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Законодательный уровень так же обеспечивает информационную безопасность, поскольку законы и нормативные акты создают основу для регулирования отношений в области защиты информации. Они определяют правила и стандарты, направленные на предотвращение угроз безопасности, защиту личных данных и обеспечение конфиденциальности информации. Российская Федерация активно разрабатывает и внедряет законы, такие как "Об информации, информатизации и защите информации", чтобы обеспечить соблюдение принципов информационной безопасности на всех уровнях общества.

Важно отметить, что законодательство также способствует повышению информационной грамотности общества и развитию средств обеспечения информационной безопасности. Поддержание доступности и целостности информации, а также защита прав граждан на конфиденциальность и сохранение личных данных являются важными задачами законодателей. С учетом быстрого развития технологий и угроз в сфере информационной безопасности, законодательство должно постоянно совершенствоваться и адаптироваться к новым вызовам, чтобы обеспечить эффективную защиту информации в цифровой эпохе.

С точки зрения разработчика получение сертификата на созданный им программный продукт обеспечивает:

- определенное признание и повышение имиджа организации разработчика в регионе и отрасли;

- конкурсные преимущества на получение государственного или любого другого заказа в рамках целевых программ, которые финансируются из бюджетов всех уровней;

- более широкие возможности сотрудничества в совместных работах и проектах с российскими и иностранными организациями.

С точки зрения потребителя или заказчика преимущество при приобретении сертифицированной программной продукции состоит в предоставлении определенной гарантия того, что приобретаемый программный продукт соответствует всем указанным в нем и его приложении требованиям нормативных документов, условиям и характеристикам эксплуатации.

Одним из эффективных способов охраны названия, присвоенного программе ЭВМ, оригинального изображения представления программного продукта является использование товарных знаков. Товарный знак — это символ, позволяющий отличить продукцию одного производителя от другого или услугу одной фирмы от другой. Если этого не сделать, плодами «раскрутки» может воспользоваться другая фирма, выпустив под аналогичной торговой маркой товар худшего качества. Товарный знак может быть бессрочным и в этом состоит его преимущество перед патентами и объектами авторского права.

# Органы добровольной и обязательной сертИфикации В РОССИИ

**Обязательное** подтверждение соответствия проводится только в случаях, установленных соответствующим техническим регламентом, и исключительно на соответствие требованиям технического регламента. Объектом обязательного подтверждения соответствия может быть только продукция, выпускаемая в обращение на территории РФ. Обязательной сертификации подлежат программ для ЭВМ и баз данных, созданные для информатизации особо опасных объектов, включая предприятия оборонного комплекса.

Организациями, оказывающими услуги по обязательной сертификации программных продуктов, являются:

- Федеральная служба по техническому и экспортному контролю (ФСТЭК России), предоставляющая сертификат в области методов и средств защиты информации;

- органы и испытательные лаборатории Россертификации, аккредитованные на оказание услуг по сертификации ПП на соответствие документам Госстандарта.

**Добровольное** подтверждение соответствия осуществляется по инициативе заявителя на условиях договора между заявителем и органом по сертификации. Добровольное подтверждение соответствия может осуществляться для установления соответствия национальным стандартам, стандартам организаций, техническим требованиям к ПП, условиям договоров.

Добровольная сертификация может проводиться юридическим лицом и/или индивидуальным предпринимателем либо несколькими юридическими лицами и/или индивидуальными предпринимателями, зарегистрированными в установленном порядке федеральным органом исполнительной власти по техническому регулированию.

В России в настоящее время зарегистрировано более 200 систем добровольной сертификации, например:

- орган сертификации «Росинфосерт» — система добровольной сертификации средств и систем в сфере информатизации;

- орган сертификации «Инкомтехсерт» — система добровольной сертификации информационно-коммуникационных технологий в Образовании.

# Заключение

Сертификация играет важную роль в обеспечении качества и безопасности продукции, подтверждая их соответствие установленным стандартам. Этот процесс не только способствует повышению репутации компаний на рынке, но и укрепляет доверие потребителей. Однако, сертификация может быть сложным и затратным процессом, требующим значительных ресурсов.

В современной рыночной экономике сертификация становится необходимым инструментом для обеспечения конкурентоспособности продукции на мировом рынке. Подтверждение соответствия международным стандартам помогает компаниям доказать свою способность производить товары и услуги высокого качества. Государственные интересы также играют важную роль в процессе сертификации, стремясь обеспечить безопасность и качество продукции для граждан, соблюдая баланс между качеством и доступностью сертификации.

Изучение понятия сертификации, методов её проведения, нормативно-правовых документов и стандартов в области информационной безопасности является важным шагом для обеспечения защиты информации. Развитие отечественного организационного и правового обеспечения в сфере информационной безопасности, а также систем менеджмента информационной безопасности, обеспечивают эффективную защиту информации в цифровой эпохе.

Сертификация обеспечивает соответствия продукции нормативным требованиям и гарантировании ее качества и безопасности для потребителей. Этот процесс является неотъемлемой частью рыночной экономики, способствуя улучшению качества товаров и услуг, повышению конкурентоспособности национальной продукции и защите интересов потребителей.

Одновременно с этим, важно находить баланс между обеспечением высоких стандартов качества и доступностью процедур сертификации, чтобы не затруднять развитие предпринимательства. Система сертификации должна быть эффективной, прозрачной и содействовать как контролю качества продукции, так и развитию экономики в целом, обеспечивая условия для успешного участия российских компаний на мировом рынке и поддерживая безопасность и доверие потребителей.

Международные правовые и нормативные акты обеспечивают информационную безопасность в современном мире, где объемы передаваемой и обрабатываемой информации постоянно растут. Разработка и принятие международных стандартов и норм, направленных на защиту данных от различных угроз, становятся все более важными. Эти акты создают базу для сотрудничества между государствами, организациями и компаниями, обеспечивая единые принципы и требования для надежной защиты информации. Соблюдение международных правовых и нормативных актов по информационной безопасности является необходимым условием для успешного функционирования современных информационных систем и процессов обработки данных. Они способствуют установлению единого стандарта защиты информации на международном уровне и повышают доверие к электронным коммуникациям и цифровым технологиям. Цель законодательных мер – предупреждение и сдерживание потенциальных нарушителей, что важно для обеспечения стабильности и безопасности информационного пространства.

В заключение, можно отметить, что отечественное регулирование в сфере информационной безопасности обеспечивает надежность и защиту информации. Законодательный уровень устанавливает основные принципы и требования для обеспечения безопасности данных, а также определяет ответственность за нарушения в этой области. Стремление к созданию и поддержанию негативного отношения к нарушениям информационной безопасности, а также содействие в повышении образованности общества в этой сфере являются важными аспектами законодательной деятельности. Российское законодательство, включая закон "Об информации, информатизации и защите информации", устанавливает цели защиты информации и права граждан на конфиденциальность и безопасность данных, что способствует обеспечению информационной безопасности и прав граждан в цифровую эпоху.

Таким образом, в России действует как обязательная, так и добровольная системы сертификации программных продуктов. Обязательное подтверждение соответствия проводится только в случаях, установленных техническими регламентами, и направлено на обеспечение безопасности и соответствия требованиям технического регулирования. Добровольное подтверждение соответствия может осуществляться по инициативе заявителя для установления соответствия стандартам и требованиям, не предусмотренным обязательной сертификацией.

Организации, оказывающие услуги по обязательной сертификации, такие как Федеральная служба по техническому и экспортному контролю (ФСТЭК России) и Россертификация, обеспечивают безопасность информации. Добровольные системы сертификации, такие как «Росинфосерт» и «Инкомтехсерт», способствуют повышению качества информационных технологий в различных сферах, таких как информатизация особых объектов и образование.

Таким образом, развитие систем сертификации программных продуктов в России является важным шагом для обеспечения безопасности информации и повышения качества информационных технологий в стране.

По моему мнению, сертификация средств защиты информации необходима, поскольку она обеспечивает надёжность продукта в глазах потребителей. Можно быть уверенным что продукт сохраняет безопасность данных с ограниченным доступом, а так же целостность информации и способов её обработки.

Эти преимущества широко известны специалистам в данной области. По этой причине сертификат соответствия информационной безопасности сразу же воспринимается как свидетельство грамотной и ответственной позиции компании в вопросах обеспечения защиты данных.

Компания, которая успешно прошла проверку на соответствие требованиям системы и подтвердила выполнение обязательных стандартов, получает сертификат установленного образца. Он оформляется аккредитованным сертификационным органом, который проводил аудит на предприятии. Документ выдается, чтобы его владелец мог предъявить сертификат любому заинтересованному лицу — например, потенциальному партнеру.

# СПИСОК ИСПОЛЬЗОРВАННОЙ ЛИТЕРАТУРЫ

1. Позднеев Б. Стандартизация и сертификация основа гарантий качества в сфере е-Learning // Высшее образование в России. 2008. №11. URL: https://cyberleninka.ru/article/n/standartizatsiya-i-sertifikatsiya-osnova-garantiy-kachestva-v-sfere-e-learning (дата обращения: 21.02.2024).
2. ГОСТ Р ИСО/МЭК 12207-99. Информационная технология. Процессы жизненного цикла программных средств[Электронный ресурс]. — URL: http://vsegost. com/ Catalog/38/38119.shtml
3. Авагян Сурен Константинович Сертификация и стандартизация в сфере информационных технологий // Наука, техника и образование. 2020. №4 (68). URL: https://cyberleninka.ru/article/n/sertifikatsiya-i-standartizatsiya-v-sfere-informatsionnyh-tehnologiy (дата обращения: 21.02.2024).
4. Гвоздева С. М. Сертификация как инструмент повышения качества продукции // Изв. Сарат. ун-та Нов. сер. Сер. Экономика. Управление. Право. 2010. №1. URL: https://cyberleninka.ru/article/n/sertifikatsiya-kak-instrument-povysheniya-kachestva-produktsii (дата обращения: 21.02.2024).
5. Аннабашимова Мерджен Шохрадовна ОСНОВНЫЕ ПРИНЦИПЫ СТАНДАРТИЗАЦИИ // IN SITU. 2023. №1. URL: https://cyberleninka.ru/article/n/osnovnye-printsipy-standartizatsii (дата обращения: 21.02.2024).