*migration processes create both positive effects that help to replenish the labor shortage and stimulate economic growth, and negative consequences associated with the need for social adaptation of migrants and the fight against illegal migration.*

***Keywords:*** *region, economic security of the Tver region, migration processes.*

Об авторе:

КАЛИНИН Сергей Владимирович – студент, ФГБОУ ВО «Тверской государственный технический университет», Тверь. E-mail: serezhenka_kalinin_2003@mail.ru

Научный руководитель – Скворцова Галина Геннадьевна, кандидат экономических наук, доцент кафедры экономики и управления производством, ФГБОУ ВО «Тверской государственный технический университет», Тверь. E-mail: gala-skvortsova@yandex.ru

About the author:

KALININ Sergey Vladimirovich – Student, Tver State Technical University, Tver. E-mail: serezhenka_kalinin_2003@mail.ru

Research manager – Skvortsova Galina Gennadyevna, Candidate of Economic Sciences, Associate Professor of the Department of Economics and Production Management, Tver State Technical University, Tver. E-mail: gala-skvortsova@yandex.ru

*УДК 338.1:004*

# ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИЙ В ЦИФРОВУЮ ЭПОХУ: ПРОБЛЕМЫ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

**Д.С. Лепеханова**



***Аннотация.*** *В статье рассмотрена проблема утечки конфиденциальной информации через сотрудников как важный фактор обеспечения экономической безопасности современных организаций. Обоснована необходимость комплексного подхода к решению проблемы с учетом взаимосвязи таких факторов, как конкуренция, киберугрозы и человеческий капитал.*

***Ключевые слова:*** *экономическая безопасность, организации, конкуренция, киберугрозы, человеческий капитал.*

***Введение***

В современном мире информация как объект обеспечения экономической безопасности организации приобретает все большую ценность и становится важнейшим инструментом для успешного ведения бизнеса. Рост цифровизации экономики привел к значительному расширению использования информационных технологий. Это увеличивает риски, связанные с возможностью утечки, искажения или уничтожения информации. Для обеспечения экономической безопасности организации в эпоху цифровизации особое значение приобретает, наряду с внутренним контролем, аудитом и финансовым мониторингом, информационная безопасность.

Традиционные подходы к защите информации, основанные исключительно на технических решениях, показывают недостаточную эффективность.

Экспертно-аналитический центр InfoWatch в ежегодном аналитическом отчете об утечках информации ограниченного доступа в России из российских коммерческих организаций, государственных организаций, силовых структур и органов власти отмечает, что количество инцидентов, связанных с утечками данных в России, остается стабильным третий год подряд (после резкого увеличения в 2022 г.) [1].

Количество утечек данных в России за 2019–2024 гг. показано на рис. 1.

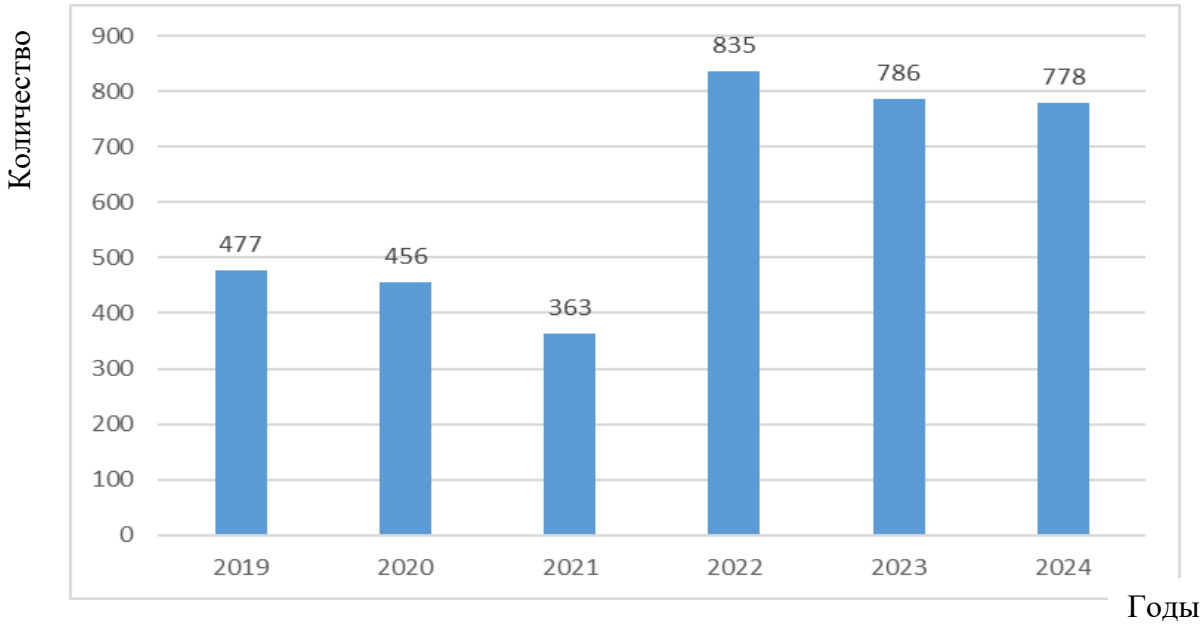


Рис. 1. Число утечек данных в России (2019–2024 гг.) [1]

Исследователи отмечают [2]: «Кибератак стало меньше, утечек по вине персонала – больше». Несмотря на то, что в структуре по типам инцидентов 70 % приходится на утечки вследствие кибератак, на первом

месте у большинства респондентов ряда опросов стоит человеческий фактор – внутренние нарушители. Респонденты отмечают, что каждый третий случай – это гибридная атака, т.е. совместные действия внутренних и внешних нарушителей. Распределение утечек информации по типам инцидентов в России за 2024 г. представлено на рис. 2.

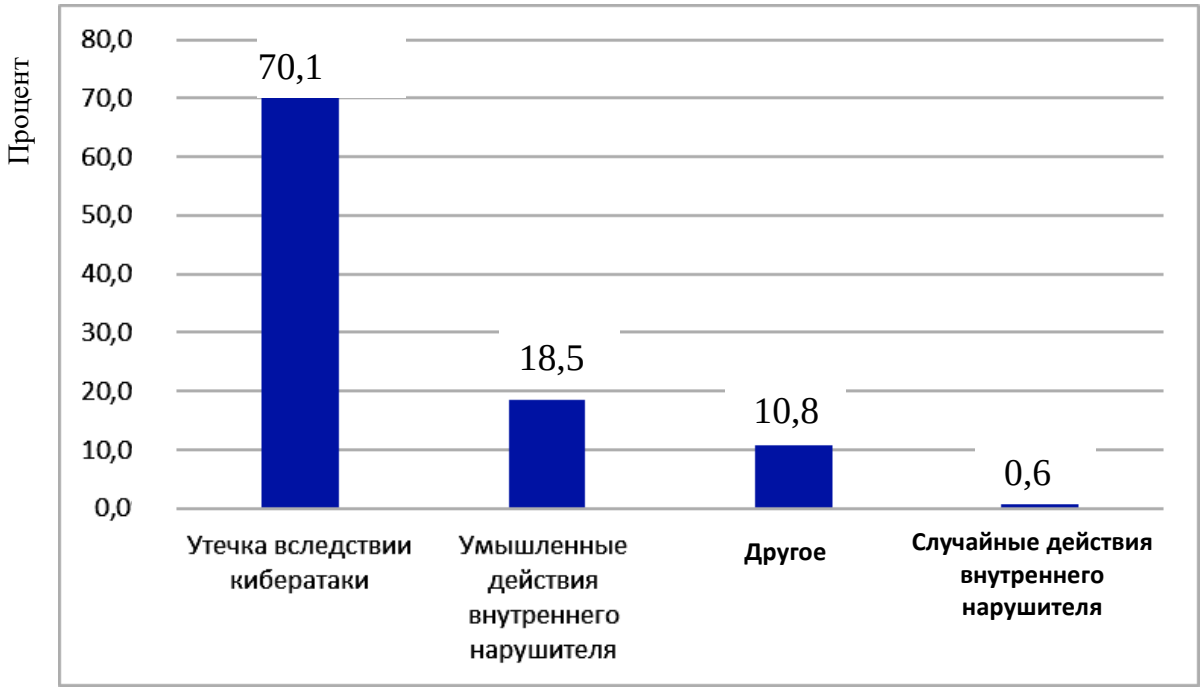


Рис. 2. Распределение утечек информации
по типам инцидентов в России (2024 г.) [1]

Таким образом, бизнес видит основную угрозу информационным активам в действиях персонала (как умышленных, так и случайных).

Цель исследования заключается в формировании комплексного подхода к решению проблемы утечки конфиденциальной информации организации.

***Результаты исследования***

В результате рассмотрения существующих подходов к определению экономической безопасности организации [5, с. 145; 9, с. 369; 10, с. 103] было составлено определение, включающее ключевые положения различных исследователей в данной области. Экономическая безопасность организации представляет собой комплексную характеристику ее состояния, отражающую способность эффективно функционировать и развиваться в условиях рыночной экономики, при которой обеспечиваются устойчивая защита жизненно важных экономических интересов от внутренних и внешних угроз, рациональное использование имеющихся ресурсов и потенциал адаптации к изменяющимся условиям внешней

среды, что позволяет достигать поставленных стратегических целей в долгосрочной перспективе.

Выявление внутренних и внешних угроз – одна из важнейших задач обеспечения экономической безопасности организации.

*Внешние угрозы* возникают вне организации и не связаны с ее производственной деятельностью. В современных условиях информация стала одним из ключевых ресурсов, обеспечивающих конкурентоспособность организации на рынке. В этой связи утечка, искажение или уничтожение информации могут нанести значительный ущерб деятельности любой компании. Рассмотрим *конкуренцию* как внешнюю угрозу.

Термин «конкуренция» вошел в экономическую теорию из разговорного языка (от лат. concurrentia, т.е. «столкновение», «состязание»). В экономике конкуренция определяется как соперничество между участниками рыночного хозяйства за лучшие условия производства, купли и продажи товаров [3, с. 6].

Влияние конкуренции на организации можно рассматривать с разных сторон.

С одной стороны, конкуренция стимулирует организации к инновациям и техническому прогрессу. В условиях конкурентной борьбы компании вынуждены искать новые решения, внедрять современные технологии и улучшать производственные процессы. Эти процессы способствуют рациональному использованию ресурсов и снижению издержек производства, что в конечном счете может привести к снижению цен для потребителей. Кроме того, конкуренция способствует повышению качества продукции и услуг, так как организации стремятся привлечь и удержать клиентов, предлагая лучшие товары и услуги.

С другой стороны, конкуренция может создавать нестабильность в деятельности организации. В условиях жесткой борьбы за рынок компании могут сталкиваться с финансовыми трудностями, что может привести к банкротству. Кроме того, они вынуждены тратить значительные ресурсы на ведение конкурентной борьбы, что иногда отвлекает их от долгосрочных инвестиций в развитие и инновации.

В эпоху цифровизации внешними являются *угрозы, связанные с киберпространством* и позволяющие злоумышленникам получить несанкционированный доступ к информации или повредить системы, инфраструктуру или устройства, подключенные к сети. Они могут нанести серьезный ущерб хозяйствующим субъектам, так как могут привести к утечке конфиденциальных данных, финансовым или репутационным потерям [4, с. 404].

Влияние киберугроз на хозяйствующий субъект можно рассмотреть с точки зрения финансовых, операционных и стратегических последствий.

Финансовые убытки – одна из самых ощутимых проблем, с которыми сталкивается организация после кибератаки. Затраты на восстановление инфраструктуры, защиту данных и обеспечение безопасности могут быть колоссальными. Происходит потеря прибыли из-за временной остановки бизнеса, а убытки от упущенных возможностей возникают из-за потери доверия клиентов. Организации также уплачивают штрафы и выплачивают компенсации из-за несоблюдения законодательства о защите данных.

Операционные последствия кибератак включают снижение продуктивности и нарушение обычной работы компании. Когда атака поражает важные системы, предприятие может временно остановить свою деятельность, что приводит к задержкам в обработке заказов и предоставлении услуг, негативно влияет на клиентов и их доверие.

Кибератаки способны нанести организации существенный урон в долгосрочной перспективе. Невозможность защитить данные снижает доверие инвесторов, которые рассматривают такие атаки как риск для устойчивости бизнеса и могут отказаться от вложений. Это ограничивает приток капитала и ухудшает финансовые показатели. Недостаток доверия, в свою очередь, влияет на конкурентоспособность, так как компании должны демонстрировать не только прибыльность, но и устойчивость к угрозам. Частые атаки могут подорвать репутацию в глазах клиентов и партнеров, привести к потере доверия и возможным юридическим проблемам.

*Внутренние угрозы* связаны с хозяйственной деятельностью организации, ее персоналом. Они обусловлены процессами, возникающими в рамках производственной деятельности и коммерческих операций на всех этапах жизненного цикла продукции, и могут повлиять на результаты.

Практика показывает, что совокупный ущерб экономической безопасности организации от внутренних негативных воздействий во много раз превосходит ущерб от внешних и зачастую приводит к банкротству тех компаний, которые уделяют недостаточное внимание анализу поступающей информации.

Исследования InfoWatch показывают, что, несмотря на преобладание внешних кибератак, главной угрозой для информационной безопасности в бизнесе считается человеческий капитал.

Около 44 % организаций связывают утечки с неумышленными действиями сотрудников, а 37 % – с умышленными. При этом каждый третий случай представляет собой сговор персонала с внешними нарушителями, о чем свидетельствуют сообщения хакеров [2].

Таким образом, внутренние угрозы остаются приоритетными в восприятии бизнеса, опережая даже растущую опасность киберпреступности.

Человеческий капитал представляет собой совокупность профессиональных, личностных и мотивационных характеристик сотрудников, способных решать стоящие перед ними текущие и перспективные задачи [6, с. 63].

Профессиональные характеристики включают в себя квалификацию и опыт сотрудников, специализированные знания и навыки, способность к освоению новых технологий и экспертность в профильных областях. Например, в производственной организации это может быть знание технологических процессов, умение работать с современным оборудованием, понимание стандартов качества.

Личностные качества сотрудников играют важную роль в деятельности хозяйствующих субъектов. Ответственность, дисциплинированность и добросовестность помогают соблюдать сроки, стандарты и прозрачность работы.

Добросовестность сотрудников является фундаментальным фактором, определяющим не только эффективность работы организации, но и ее защищенность от различных угроз, включая киберугрозы.

Ответственность и дисциплинированность сотрудников проявляются в строгом соблюдении корпоративных политик и процедур безопасности. Сотрудник, имеющий высокие этические стандарты, неизменно придерживается регламента обращения с конфиденциальными данными и категорически исключает возможность их разглашения посторонним субъектам. В противоположность этому отсутствие указанных качеств несет в себе потенциальную угрозу компрометации систем доступа и несанкционированного распространения защищенной информации.

К мотивационным аспектам относят профессиональное стремление, экономический интерес, карьерные ориентиры, приверженность корпоративной культуре и нацеленность на профессиональный рост. Персонал, испытывающий финансовые затруднения или не идентифицирующий себя с корпоративными ценностями, может представлять потенциальную угрозу для системы безопасности, проявлять халатность в соблюдении установленных регламентов как осознанно, так и по неосторожности.

Таким образом, в современной бизнес-среде существует серьезная угроза утечки конфиденциальной информации через сотрудников, что напрямую связано с такими факторами, как конкуренция, киберугрозы и человеческий капитал.

Рассмотрим, как эти факторы взаимосвязаны, на примере сотрудников, готовых продать информацию конкурентам. В условиях жесткой конкуренции организации вынуждены постоянно оптимизировать бизнес-процессы и искать новые пути развития. Это создает дополнительную нагрузку на персонал и повышает требования к компетенциям сотруд-

ников. При этом возрастает и ценность конфиденциальной информации для конкурентов.

Человеческий капитал, являясь ключевым ресурсом организации, может как способствовать ее развитию, так и представлять собой потенциальную угрозу. Сотрудники, обладающие доступом к важной информации и не имеющие достаточной мотивации к соблюдению информационной безопасности, становятся уязвимым звеном в системе защиты данных.

Особенно сильно данная проблема обостряется в периоды активной конкурентной борьбы, когда компании внедряют новые технологии, разрабатывают инновационные продукты и стратегии. В таких условиях возрастает как ценность конфиденциальной информации, так и риски ее утечки через сотрудников, которые могут быть привлечены предложениями конкурентов или которые могут действовать из соображений личной выгоды.

Киберугрозы в данном контексте играют двойственную роль. С одной стороны, они создают дополнительные риски утечки информации через взломанные системы. С другой – сами сотрудники могут использовать эти уязвимости для передачи данных третьим лицам. Например, если в компании не установлены должные системы контроля доступа и мониторинга действий персонала, недобросовестный сотрудник может легко выгрузить конфиденциальные данные через незащищенное соединение и продать их конкурентам организации.

Важно понимать, что утечка информации через сотрудников – это не изолированная проблема, а результат взаимодействия множества факторов. Эффективное решение возможно только при комплексном подходе, учитывающем все аспекты взаимосвязи конкуренции, киберугроз и человеческого капитала организации.

В конечном счете проблема утечки информации через сотрудников требует постоянного внимания к следующим ключевым направлениям:

1. Внедрению современных систем защиты информации. Необходимо не только установить современные технические средства контроля доступа и мониторинга, но и регулярно проводить аудит существующих систем, выявлять уязвимости и своевременно их устранять. Важно также организовать непрерывный процесс обучения сотрудников правилам информационной безопасности, включая распознавание фишинговых атак, социальную инженерию и другие методы получения конфиденциальной информации.

2. Разработке и внедрению политики информационной безопасности. В рамках такой политики должен быть четко предусмотрен порядок доступа сотрудников и других лиц к информационным системам. Кроме того, должны быть установлены процедуры реагирования на инциденты безопасности, а также процедуры проведения регулярных проверок. Одним

из наиболее эффективных методов защиты информации, который следует включить в политику безопасности, является принцип «дробления» данных. Суть этого метода заключается в том, что каждый сотрудник получает доступ только к той информации, которая необходима ему для выполнения прямых должностных обязанностей. Такой подход исключает возможность ознакомления с данными, не относящимися к компетенции конкретного работника.

3. Развитию человеческого капитала и корпоративной культуры. Работников необходимо информировать о возможных угрозах и способах их предотвращения, а также о том, как правильно использовать системы и следовать политике безопасности. Сюда относится обучение сотрудников основам безопасности, пониманию основных угроз и способов их предотвращения, а также формирование правильного отношения к вопросам защиты информации. Без создания такой культуры все технические меры защиты могут оказаться бессильными перед человеческими ошибками или недостатком понимания важности проблемы [7].

Пренебрежение любым из указанных аспектов приводит к серьезным последствиям, включая утрату конкурентных преимуществ, финансовые потери и репутационный ущерб. В связи с этим крайне важно воспринимать проблему утечки информации как элемент комплексной системы экономической безопасности организации.

Что касается законодательства Российской Федерации, то в Федеральном законе «Об информации, информационных технологиях и о защите информации» № 149-ФЗ [1] предусмотрены следующие меры защиты информации для организаций: назначение ответственных лиц за безопасность, внедрение процедур контроля доступа и ведение журналов доступа.

В рамках правовых и кадровых мер необходимо заключать с сотрудниками договоры о неразглашении, устанавливать ответственность за нарушения, регламентировать порядок работы с информацией и сообщать об инцидентах в компетентные органы. Все меры должны применяться комплексно и постоянно совершенствоваться в соответствии с возникающими угрозами и изменениями законодательства.

***Вывод***

В современных условиях человеческий капитал становится ключевым звеном в обеспечении экономической безопасности организации, через которое проявляются как конкурентные угрозы, так и киберугрозы. Это связано с тем, что сотрудники имеют прямой доступ к важной информации организации, а в условиях жесткой конкуренции ценность конфиденциальных данных для соперников постоянно возрастает.

Особую опасность представляет то, что даже самые современные системы защиты могут оказаться бессильны перед сотрудником, который хочет причинить вред компании. Он обладает знанием внутренних процессов и способен найти или использовать слабые места в системе безопасности. Сотрудники становятся точкой пересечения конкуренции и киберугроз, что создает серьезные риски для организации.

Эффективная защита от утечки информации требует системного и комплексного подхода, охватывающего три ключевых направления: техническую защиту, организационные меры и работу с персоналом. Система защиты должна включать в себя современные технические средства контроля и мониторинга, регулярные аудиты безопасности, а также постоянное обучение сотрудников распознаванию угроз и правильным действиям в кризисных ситуациях.

Важным элементом является внедрение продуманной политики информационной безопасности с принципом «необходимого минимума доступа», когда каждый сотрудник получает доступ только к той информации, которая требуется ему для исполнения рабочих обязанностей. При этом особую роль играет развитая корпоративная культура безопасности, при которой любой сотрудник осознает важность защиты информации и понимает свою ответственность в этом процессе.

Эффективная система экономической безопасности должна быть динамична и адаптивна к постоянно изменяющимся условиям внешней и внутренней среды организации. Только такой комплексный подход, в котором учитываются все аспекты проблемы, позволит обеспечить надежную защиту конфиденциальной информации и минимизировать риски ее утечки через сотрудников. Это является неотъемлемой частью общей системы экономической безопасности современной организации.

**Библиографический список**

1. Об информации, информационных технологиях и о защите информации: Федер. закон // Собрание законодательств РФ. 2006. № 31. Ст. 16. URL: https://www.szrf.ru/ (дата обращения: 21.03.2025).

2. Аналитический отчет России: утечки информации ограниченного доступа 2023–2024 // InfoWatch. URL: https://www.infowatch.ru (дата обращения: 21.03.2025).

3. Богомолов В.А. Введение в специальность «Экономическая безопасность»: учебное пособие. М.: ЮНИТИ-ДАНА, 2017. 279 с.

4. Биксина Н.А. Конкуренция в бизнесе: полное определение понятия, виды, плюсы и минусы конкуренции // Экономика и управление: проблемы, решения. 2018. Т. 2. № 5. С. 4–7.

5. Касперович С.А., Дербинская Е.А. Эволюция понятия «экономическая безопасность» // Труды БГТУ. 2017. № 1. С. 214–218.

6. Куклина Д. В. Киберугрозы и меры защиты: путь к обеспечению безопасности в цифровой среде // Цифровая экономика глазами студентов: материалы IV Международной научной конференции (14 мая 2024 г., Казань). Казань: ИП Сагиев А.Р., 2024. С. 402–405.

7. Нестерова К.И., Нестерова Ю.Д. Персонал организации как фактор угроз ее информационной безопасности // Современное состояние экономических систем: управление, развитие, безопасность: сборник научных трудов V Международной научно-практической конференции, 9–10 декабря 2024 г., Тверь / под общ. ред. И.В. Вякиной, Г.Г. Скворцовой. Тверь: ТвГТУ, 2025. С. 112–116.

8. Скороходова О.Р. Кадровый потенциал: понятие, сущность, основные характеристики // Экономика и управление в XXI веке: тенденции развития. 2015. № 24. С. 67–71.

9. Экономическая и национальная безопасность: учебник / Е.А. Олейников [и др.]. М.: Экзамен, 2005. 768 с.

10. Экономическая безопасность России: общий курс / В.К. Сенчагов [и др.]; под ред. В.К. Сенчагова. М.: Дело; Акад. народ. хоз-ва при Правительстве Рос. Федерации, 2005. 895 с.

## ECONOMIC SECURITY OF ORGANIZATIONS IN THE DIGITAL AGE: PROBLEMS OF CONFIDENTIAL INFORMATION LEAKAGE

**D.S. Lepehanova**

***Abstract.*** *The article examines the problems of confidential information leakage through employees as an important factor in ensuring the economic security of modern organizations. The necessity of an integrated approach to solving the problem is substantiated, taking into account the interrelationship of such factors as competition, cyber threats and human capital.*

***Keywords:*** *economic security, organizations, competition, cyber threats, human capital.*

Об авторе:

ЛЕПЕХАНОВА Дарья Сергеевна – студентка, ФГБОУ ВО «Тверской государственный технический университет», Тверь. E-mail: darya.lepehanova@mail.ru

Научный руководитель – Скворцова Галина Геннадьевна, кандидат экономических наук, доцент кафедры экономики и управления производством, ФГБОУ ВО «Тверской государственный технический университет», Тверь. E-mail: gala-skvortsova@yandex.ru

About the author:
LEPEHANOVA Darya Sergeevna – Student, Tver State Technical University, Tver. E-mail: darya.lepehanova@mail.ru
Research manager – Skvortsova Galina Gennadyevna, Candidate of Economic Sciences, Associate Professor of the Department of Economics and Production Management, Tver State Technical University, Tver. E-mail: gala-skvortsova@yandex.ru

*УДК 331.108*

# ПРОБЛЕМЫ КАДРОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

**Ю.Д. Нестерова**



***Аннотация.*** *В статье рассмотрена актуальная проблема сохранения информационной безопасности хозяйствующих субъектов. Отмечено, что главные угрозы информационной безопасности связаны с персоналом организации и устранить их могут только грамотные ИТ-специалисты.*

***Ключевые слова:*** *информационная безопасность, персонал организации, кадровое обеспечение*.

Информация – один из самых ценных ресурсов, которые могут использовать компании для достижения своих целей и повышения конкурентоспособности на рынке. В условиях развития информационного общества и постоянного роста объемов обрабатываемых данных вопрос информационной безопасности становится не просто актуальным, а критически важным для любого хозяйствующего субъекта.

Под информационной безопасностью подразумевается комплекс мер, направленных на защиту информации от различных угроз, таких как несанкционированный доступ, утечка, искажение, а также полное уничтожение данных.

Информационная безопасность охватывает множество аспектов, связанных с защитой информации, которая находится в распоряжении организации. При этом ключевыми элементами информационной безопасности являются конфиденциальность, целостность и доступность сведений. Конфиденциальность – это защита данных от несанкционированного доступа, целостность – сохранение точности и полноты