

**ПРОФИЛАКТИКА ПРАВОНАРУШЕНИЙ В СФЕРЕ
ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.**

Sadullayeva Sevinch Zarif qizi

O'ZBEKISTON RESPUBLIKASI IIV AKADEMIYASI KURSANTI

Kalit so'zlar: *axborot texnologiyalari, huquqbuzarliklar, profilaktika, axborot xavfsizligi, qonunchilik, ta'lim va tarbiya.*

Annotatsiya: *Maqola "Axborot texnologiyalari sohasidagi huquqbuzarliklarning profilaktikasi" masalasiga bag'ishlangan bo'lib, unda axborot xavfsizligi va huquqbuzarliklarning oldini olish bo'yicha muhim masalalar ko'rib chiqiladi. Ushbu maqolada axborot texnologiyalarining tez rivojlanishi va shu bilan birga, ushbu sohada yuzaga keladigan huquqbuzarliklarning tahlili hamda ularga qarshi kurashishning samarali usullari taqdim etiladi. Axborot huquqbuzarliklarini oldini olishda davlat va jamoat tashkilotlarining roli, qonunchilikdagi o'zgarishlar, ta'lim va tarbiyaning ahamiyati haqida so'z boradi. Maqola axborot texnologiyalari sohasida huquqbuzarliklarni oldini olish uchun zaruriy chora-tadbirlar va kompleks yondashuvlarni taklif qiladi.*

Ключевые слова: *информационные технологии, правонарушения, профилактика, информационная безопасность, законодательство, образование и воспитание.*

Аннотация: *Статья посвящена профилактике правонарушений в сфере информационных технологий, в которой рассматриваются ключевые вопросы информационной безопасности и методов предотвращения правонарушений в данной области. В статье проводится анализ быстрого развития информационных технологий, а также возникающих правонарушений и эффективных методов борьбы с ними. Рассматриваются роль государства и общественных организаций в профилактике правонарушений, изменения в законодательстве, а также важность образования и воспитания. Статья предлагает необходимые меры и комплексный подход для профилактики правонарушений в сфере информационных технологий.*

Keywords: *information technology, offenses, prevention, information security, legislation, education and awareness.*

Annotation: *This article focuses on the prevention of offenses in the field of information technology, addressing key issues related to information security and methods for preventing crimes in this area. The paper analyzes the rapid development of information technologies and the crimes emerging as a result, along with effective measures to combat them. The role of government and public organizations in crime prevention, changes in legislation, and the importance of education and awareness are discussed. The article proposes necessary measures and a comprehensive approach to prevent offenses in the field of information technology.*

ВВЕДЕНИЕ

Сфера информационных технологий в последние десятилетия стремительно развивается, оказывая значительное влияние на все аспекты жизни общества. В то же время, быстрый рост технологий сопровождается увеличением числа правонарушений, связанных с использованием информационных систем. Киберпреступность, утечка персональных данных, несанкционированный доступ к информации и другие формы нарушений становятся все более актуальными угрозами для безопасности как индивидуумов, так и организаций. Профилактика правонарушений в области информационных технологий представляет собой комплекс мер, направленных на предупреждение преступлений и минимизацию рисков, связанных с нарушением информационной безопасности. Эффективная профилактика требует не только применения современных технических решений, но и активного участия государственных органов, образовательных учреждений, а также самого общества. Важно обеспечить грамотное законодательство, которое будет отвечать на вызовы времени, а также создать систему обучения и осведомленности, которая позволит предотвращать преступления до их совершения. В данной статье рассматриваются основные угрозы в сфере информационных технологий, а также предлагаются возможные пути решения проблемы профилактики правонарушений, включая развитие законодательства, улучшение информационной безопасности и повышение уровня образования и информированности граждан.

Основная часть

Сфера информационных технологий стремительно развивается, и с этим ростом увеличивается количество правонарушений, связанных с нарушением информационной безопасности. Киберпреступность, кражи данных, несанкционированный доступ к конфиденциальной информации и интернет-мошенничество становятся актуальными угрозами как для физических лиц, так и для организаций. Проблемы безопасности в этой области требуют комплексного подхода и разработки эффективных механизмов профилактики правонарушений. Одной из основных угроз в сфере информационных технологий является киберпреступность. Это включает в себя несанкционированный доступ к компьютерным системам, хакерские атаки, распространение вирусов и других вредоносных программ. В условиях глобализации и анонимности Интернета преступники могут легко скрыться за технологиями и совершать различные правонарушения, такие как кража личных данных, финансовые мошенничества или взломы корпоративных сетей. Другая угроза — это утечка конфиденциальной информации. Несанкционированный доступ к базам данных или внутренним системам организации может привести к утрате важной информации или ее распространению. В современном мире, где данные стали одним из самых ценных активов, защита информации является приоритетной задачей как для частных компаний, так и для государственных структур. Кибербуллинг и защита репутации — это еще одна проблема, которая активно обсуждается в контексте информационной безопасности. Использование технологий для совершения

психологического насилия, угроз или распространения ложной информации в интернете наносит значительный вред как отдельным лицам, так и обществу в целом. Для профилактики правонарушений в области информационных технологий требуется целый ряд мер. В первую очередь, необходимо укрепление законодательной базы, которая должна быть гибкой и своевременно реагировать на новые угрозы, возникающие в этой сфере. Законы должны учитывать особенности киберпреступности, защиты персональных данных и интернет-мошенничества. Важно развивать международное сотрудничество, поскольку многие преступления носят транснациональный характер и требуют согласованных действий на глобальном уровне. Одним из важнейших аспектов профилактики является повышение уровня информационной безопасности. Каждая организация должна принимать меры для защиты своих информационных систем, используя современные технологии, такие как шифрование данных, антивирусное ПО, системы защиты от вторжений. Также важно, чтобы сотрудники организаций были обучены правильному обращению с конфиденциальной информацией и использованию безопасных методов работы в сети. Образование и повышение осведомленности пользователей является не менее важной частью профилактики правонарушений. Важно обучать людей основам цифровой безопасности, предотвращению угроз, таких как фишинг, вирусы, интернет-мошенничество и другие. Программы обучения должны быть направлены на повышение общей культуры безопасности и осведомленности о возможных рисках в Интернете. Технологии также играют ключевую роль в профилактике правонарушений в сфере информационных технологий. Развитие искусственного интеллекта и машинного обучения позволяет создавать системы для мониторинга и анализа сетевой активности, которые могут оперативно обнаруживать угрозы и предотвращать их. Эти технологии также позволяют повысить уровень безопасности данных и снизить риски утечек и взломов. Роль государства и общества в профилактике правонарушений в информационных технологиях неопределима. Государственные органы должны не только разрабатывать эффективное законодательство, но и создавать условия для активного сотрудничества с частным сектором, образовательными учреждениями и международными организациями. Образовательные учреждения, в свою очередь, играют важную роль в формировании у граждан культуры безопасности в сети и распространении знаний о киберугрозах. В будущем ключевыми направлениями профилактики правонарушений в сфере информационных технологий будут автоматизация процессов безопасности, использование новых технологий для борьбы с киберугрозами, а также усиление международного сотрудничества в этой области. Важнейшую роль в этом процессе будет играть повышение уровня цифровой грамотности населения и обучение людей безопасному поведению в Интернете.

Заключение

Профилактика правонарушений в сфере информационных технологий является важнейшей составляющей обеспечения безопасности в современном мире. В

условиях глобализации и активного развития цифровых технологий, киберугрозы становятся все более разнообразными и сложными. Киберпреступность, утечка персональных данных, интернет-мошенничество и другие угрозы требуют комплексного подхода и скоординированных усилий на всех уровнях — от разработки законодательства до повышения осведомленности пользователей. Эффективная профилактика правонарушений невозможна без активного участия государства, образовательных учреждений и частных организаций. Государственные органы должны разрабатывать и внедрять законодательные инициативы, направленные на борьбу с киберпреступностью, защиту личных данных и создание условий для международного сотрудничества. Образовательные учреждения играют ключевую роль в формировании цифровой культуры и безопасности среди граждан. Частные компании и организации должны инвестировать в технологии информационной безопасности, обучать своих сотрудников и принимать меры по защите данных. Развитие технологий, таких как искусственный интеллект, машинное обучение и системы мониторинга, предоставляет новые возможности для обнаружения и предотвращения угроз в реальном времени. Однако важнейшим элементом профилактики остается повышение цифровой грамотности и осведомленности пользователей о возможных рисках и способах защиты от киберугроз. В будущем, с учетом дальнейшего развития информационных технологий, вопросы безопасности и защиты информации будут только набирать актуальность. Поэтому важно продолжать совершенствовать механизмы профилактики правонарушений в сфере информационных технологий, обеспечивая более высокую степень защиты и безопасности для всех участников цифровой среды.

FOYDALANILGAN ADABIYOTLAR:

1. Digital Forensics and Cyber Crime / R. S. O'Connor. — New York: Springer, 2020.

Ushbu manba kiberjinoatlarni aniqlash, ularni tekshirish va oldini olish bo'yicha ilmiy yondashuvlarni keltiradi.

2. Основы компьютерной криминологии / Н. В. Баглей. — М.: Наука, 2017. Компьютер jinoyatchiligi va uning oldini olishning asosiy tamoyillari.

3. Руководство по безопасности информационных технологий / И. А. Щербинин. — М.: ИТК, 2021.

Axborot texnologiyalarida xavfsizlikni ta'minlash uchun zarur bo'lgan qadamlar va texnikaviy chora-tadbirlar haqida tavsiyalar.