ПРОФИЛАКТИКА ПРАВОНАРУШЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Sadullayeva Sevinch Zarif qizi
O‘ZBEKISTON RESPUBLIKASI IIV AKADEMIYASI KURSANTI

Kalit so‘zlar: *axborot texnologiyalari, kiberjinoyatchilik, huquqbuzarlik, profilaktika, xavfsizlik, qonunchilik, ta’lim.*

Annotatsiya: *Maqola axborot texnologiyalari sohasidagi huquqbuzarliklarning profilaktikasi masalasini o‘rganadi. Axborot xavfsizligi va kiberjinoyatchilik bilan bog‘liq xavflar kundan-kunga oshib borayotgani sababli, ularni oldini olish uchun samarali yondashuvlar talab qilinadi. Ushbu maqolada axborot texnologiyalaridagi eng asosiy xavf-xatarlar, huquqbuzarliklar tahlili va ularni bartaraf etish uchun zarur bo‘lgan qonunchilik, texnologik va ta’lim choralariga to‘xtalib o‘tiladi. Kiberxavfsizlik, axborotlarni himoya qilish va internetdagi jinoyatchilikka qarshi kurashishda davlat va jamoat sektorlarining roli katta ekanligi ta’kidlanadi. Maqola shuningdek, ta’lim va jamiyatning axborot xavfsizligi bo‘yicha bilimlarini oshirish zarurligini ko‘rsatadi.*

Ключевые слова: *информационные технологии, киберпреступность, правонарушения, профилактика, безопасность, законодательство, образование.*

Аннотация: *Статья посвящена профилактике правонарушений в сфере информационных технологий. В условиях стремительного развития информационных технологий и увеличения числа киберугроз, важнейшей задачей становится разработка эффективных методов предотвращения преступлений в данной области. В статье рассматриваются основные угрозы в сфере информационной безопасности, а также меры по их предотвращению, включая изменения в законодательстве, использование современных технологий и повышение уровня образования в области безопасности. Также подчеркивается важность роли государства и общественных организаций в борьбе с киберпреступностью и защите персональных данных.*

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

Annotation: *This article addresses the prevention of offenses in the field of information technology. As information technology continues to rapidly evolve and cyber threats increase, the need for effective prevention measures becomes critical. The article discusses the main threats in the field of information security and the necessary steps to mitigate them, including legislative changes, the use of advanced technologies, and the enhancement of education in security. The importance of the role of the government and public organizations in combating cybercrime and protecting personal data is also emphasized..*

ВВЕДЕНИЕ

Информационные технологии в последние десятилетия значительно изменили нашу жизнь, превратившись в неотъемлемую часть повседневной деятельности. С развитием цифровых технологий все большее количество информации стало доступно в онлайн-формате, что открыло новые возможности для бизнеса, образования, медицины и других сфер. Однако с этим развитием также возникли и новые угрозы, связанные с безопасностью данных, киберпреступностью и нарушениями законов в сфере цифровых технологий. Проблемы кибербезопасности становятся актуальными как для отдельных пользователей, так и для организаций, государственных структур и общества в целом. Угроза утечки персональных данных, финансовых средств, несанкционированного доступа к конфиденциальной информации, а также распространение вирусов и других вредоносных программ становятся серьезной проблемой. Проблемы правонарушений в сфере информационных технологий требуют особого внимания и разработки комплексных мер для их предотвращения. Профилактика правонарушений в области информационных технологий представляет собой систему мер, направленных на предупреждение преступлений, связанных с использованием компьютеров, сетей и интернет-ресурсов. Эта деятельность требует тесного сотрудничества между различными организациями: государственными структурами, образовательными учреждениями, частными компаниями и обществом. Важно создать эффективную законодательную базу, которая будет отвечать современным вызовам и угрозам в области информационных технологий. Цель данной статьи — рассмотреть основные угрозы в сфере информационных технологий и методы профилактики правонарушений, а также предложить рекомендации для повышения уровня безопасности и защиты данных в условиях стремительного развития цифрового общества.

ОСНОВНАЯ ЧАСТЬ

Современное общество переживает эпоху стремительного развития информационных технологий. Информационные системы, сети и онлайн-платформы становятся основой для функционирования экономики, науки, медицины и других ключевых сфер. Однако с развитием технологий появляется и множество новых угроз, связанных с киберпреступностью и правонарушениями в сфере информационных технологий. Основными угрозами в этой области являются киберпреступность, хакерские атаки, мошенничество в сети Интернет, а также утечка конфиденциальной информации и личных данных. В последние годы наблюдается значительный рост числа преступлений, совершенных с использованием информационных технологий. Это могут быть как преступления, направленные на физическое или юридическое лицо, так и на государственные и общественные интересы. Современные преступники могут действовать анонимно, что усложняет расследование и борьбу с правонарушениями в киберпространстве. Одна из самых

актуальных угроз — это киберпреступность, которая охватывает широкий спектр деяний: взломы компьютерных систем, фишинг, распространение вирусов, кражу данных и финансовые преступления. Многие из этих преступлений могут привести к серьезным финансовым убыткам, утечке персональной информации или даже угрозам национальной безопасности. С учетом роста количества киберугроз и цифровых атак, защита информационных систем становится важной задачей для всех слоев общества. Для эффективной профилактики правонарушений в сфере информационных технологий необходимо разработать комплексный подход, который включает несколько важных аспектов. В первую очередь, важным элементом профилактики является законодательное регулирование. Государственные органы должны оперативно реагировать на изменения в технологической сфере и обновлять законодательство в соответствии с новыми вызовами. К сожалению, во многих странах законодательная база все еще не успевает за быстрым развитием технологий, что создает правовые лазейки для преступников. Другим важным аспектом является повышение осведомленности пользователей о рисках и угрозах, связанных с использованием информационных технологий. Образование и информирование граждан и сотрудников организаций о методах защиты данных, безопасном поведении в сети и предотвращении киберугроз — важный шаг к сокращению числа правонарушений. Для этого необходимо проводить обучающие программы и кампании, направленные на повышение уровня цифровой грамотности среди различных слоев населения. Использование современных технологий для защиты информации также играет ключевую роль. Применение систем защиты, таких как антивирусные программы, системы обнаружения вторжений, шифрование данных и двухфакторная аутентификация, позволяет значительно повысить уровень безопасности. Организации должны активно внедрять системы мониторинга и анализа безопасности, чтобы выявлять аномалии и вовремя предотвращать потенциальные угрозы. Не менее важным является международное сотрудничество в борьбе с киберпреступностью. Множество киберпреступлений имеет транснациональный характер, и для эффективного преследования преступников необходимо взаимодействие между странами, обмен информацией и координация действий правоохранительных органов. Международные организации, такие как Интерпол, Европол и ООН, играют важную роль в разработке стандартов и рекомендаций для борьбы с киберугрозами. В дополнение к этим мерам, необходимо учитывать и такие аспекты, как разработка этических норм в области информационной безопасности. Важно помнить, что защита информации и кибербезопасность не только правовые и технические вопросы, но и вопросы морали и этики, которые касаются прав личности, конфиденциальности и справедливости в цифровом пространстве. Таким образом, для профилактики правонарушений в сфере информационных технологий требуется комплексный подход, включающий законодательные, образовательные, технологические и этические меры. Только совместные усилия государства, частного сектора и общества в целом смогут создать

безопасное информационное пространство и эффективно защитить данные и ресурсы от киберугроз.

ЗАКЛЮЧЕНИЕ

Профилактика правонарушений в сфере информационных технологий является неотъемлемой частью обеспечения безопасности в цифровую эпоху. Современные угрозы, связанные с киберпреступностью, требуют комплексного подхода и сотрудничества на разных уровнях — от правительства и образовательных учреждений до частных компаний и отдельных пользователей. Важно, чтобы в этом процессе задействованы все компоненты: законодательство, технологии, образование и международное сотрудничество. Одним из ключевых аспектов является обновление и совершенствование законодательства в сфере информационной безопасности, которое должно оперативно реагировать на изменения в технологической сфере. Важно также повышать уровень цифровой грамотности и осведомленности граждан о возможных рисках, а также обучать их безопасному поведению в Интернете. Кроме того, технологические решения, такие как системы защиты данных, шифрование и антивирусное программное обеспечение, играют важную роль в предотвращении правонарушений. Безопасность информационных систем должна быть приоритетом как для государственных структур, так и для частных компаний. Не менее значимо международное сотрудничество в области борьбы с киберпреступностью. В условиях глобализации и транснационального характера киберугроз только совместные усилия могут обеспечить эффективное противодействие преступлениям в цифровой сфере. Таким образом, профилактика правонарушений в сфере информационных технологий требует системного подхода, вовлечения всех заинтересованных сторон и постоянного совершенствования механизмов защиты, что позволит создать безопасную и стабильную цифровую среду для пользователей по всему миру.

FOYDALANILGAN ADABIYOTLAR:

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

Ushbu manba kiberjinoyatlarni aniqlash, ularni tekshirish va oldini olish bo‘yicha ilmiy yondashuvlarni keltiradi.

2. Основы компьютерной криминологии / Н. В. Баглей. — М.: Наука, 2017.

Kompyuter 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.