

ПЕРСПЕКТИВЫ СНИЖЕНИЯ КРИМИНОГЕННОГО ПОТЕНЦИАЛА В ЦИФРОВОМ ОБЩЕСТВЕ

Prospects for reducing the criminogenic potential in a digital society

О. Л. Альтшулер-Феррейра, преподаватель кафедры иностранных языков
Уральский юридический институт МВД России
(Екатеринбург, ул. Корепина, 66)

Аннотация

В статье рассматриваются перспективы снижения криминогенного потенциала в цифровом обществе. Автор анализирует основные тенденции в данной области и оценивает перспективы и намечает основные направления противодействия преступности в цифровом обществе

Ключевые слова: криминогенный потенциал, цифровое общество, киберпреступность, правовое сознание.

Summary

The article examines the prospects for reducing the criminogenic potential in a digital society. The author analyzes the main trends in this area and assesses the prospects and outlines the main directions for combating crime in a digital society

Keywords: criminogenic potential, digital society, cybercrime, legal consciousness.

Цифровое общество характеризуется интенсивным развитием информационных технологий, сетевых коммуникаций и глобализацией виртуального пространства [1]. С одной стороны, этот процесс способствует ускорению социально-экономического развития общества, улучшению качества жизни населения и повышению эффективности государственного управления. Однако с другой стороны, внедрение цифровых технологий создает новые риски и угрозы безопасности личности, общества и государства. Одним из наиболее значимых негативных последствий является рост преступности в цифровой среде — киберпреступность.

Цель данной работы заключается в выявлении перспективных направлений снижения криминогенного потенциала цифрового общества путем анализа существующих проблем и разработки мер противодействия криминальному поведению в условиях современной информационной среды.

Методология исследования

Для достижения поставленной цели были использованы следующие методы научного познания: теоретический анализ научной литературы, статистическое моделирование, контент-анализ материалов, метод экспертных оценок. Исследовательская работа выполнена на основе изучения отечественной и зарубежной литературы по вопросам кибернетической преступности, обеспечения информационной безопасности и профилактики правонарушений в цифровом пространстве.

Анализ состояния проблемы

Современное состояние криминогенной ситуации в цифровом обществе определяется несколькими ключевыми факторами:

— Расширение возможностей анонимизации действий пользователей в сети Интернет, затрудняющее выявление преступников и расследование преступлений.

— Высокая скорость распространения вредоносного программного обеспечения (ПО), способствующего совершению различных видов мошенничества, хищений денежных средств и кражи конфиденциальной информации [2].

— Нехватка квалифицированных специалистов в области защиты информации и компьютерной криминалистики, необходимых для эффективной борьбы с киберпреступлениями.

— Недостаточная правовая регламентация отношений, возникающих в результате деятельности субъектов информационного взаимодействия.

Кроме того, значительная доля правонарушений совершается лицами молодого возраста, имеющими высокий уровень владения современными технологиями и часто испытывающими дефицит этического воспитания и правовой культуры. Основные направления предупреждения преступности в цифровом обществе:

— Снижение уровня криминогенности цифрового общества возможно через реализацию комплекса взаимосвязанных мероприятий, направленных на повышение защищённости персональных данных, создание условий для эффективного расследования компьютерных преступлений и формирование правового сознания участников социальных сетей и иных онлайн-платформ.

— Повышение уровня технической защиты от кибератак

Одним из приоритетных направлений выступает обеспечение надежной системы предотвращения несанкционированного доступа к информационным ресурсам и базам данных организаций всех форм собственности. Важно использовать современные технологии шифрования, антивирусные программы и средства обнаружения вторжений. Следует регулярно проводить мониторинг уязвимостей и оперативно устранять обнаруженные недостатки.

— Совершенствование законодательства

Необходимо развивать нормативную базу, регулирующую отношения в сфере оборота информации, права и обязанности владельцев ресурсов, меры ответственности за нарушения правил пользования сетью Интернет и правила обращения с персональными данными [3]. Требуется обеспечить согласованность национальных законодательств стран СНГ и международное сотрудничество в борьбе с транснациональной организованной киберпреступностью.

— Формирование устойчивого правового сознания среди молодежи.

Библиографический список

1. *Крайнова Н. А.* "Международная цифровая безопасность": миф или реальность? // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 42-46.
2. *Никуленко А. В.* О некоторых вопросах кибербезопасности в современном мире: взгляд дилетанта // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 37-41.
3. *Бегишев И. .Р.* Безопасность критической инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27-32.