УДК 343.85

КОМПЛЕКС ПРОФИЛАКТИЧЕСКИХ МЕРОПРИЯТИЙ, НАПРАВЛЕННЫХ НА БОРЬБУ С ПРЕСТУПЛЕНИЯМИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ ДЛЯ СТАБИЛЬНОГО РЕГИОНАЛЬНОГО РАЗВИТИЯ

Талашко Н.Г.

Студент 3 курса заочной формы обучения,

Направление подготовки 40.04.01 «Юриспруденция»

ЧОУ ВО ЮУ (ИУБиП)

Научный руководитель: **Руденко В.В.**

к.э.н., доцент кафедры государственно-правовых дисциплин

ЧОУ ВО ЮУ (ИУБиП)

Аннотация: В статье автор определяет комплекс профилактических мероприятий, направленных на борьбу с преступлениями в сфере высоких технологий для стабильного регионального развития.

Ключевые слова: компьютерная преступность, стабильное региональное развитие, частная жизнь, интернет, преступление.

A SET OF PREVENTIVE MEASURES AIMED AT COMBATING CRIMES IN THE FIELD OF HIGH TECHNOLOGIES FOR STABLE REGIONAL DEVELOPMENT

Talashko N.G.

Rudenko V.V.

Abstract: In the article, the author defines a set of preventive measures aimed at combating crimes in the field of high technologies for stable regional development.

Keywords: computer crime, stable regional development, privacy, internet, crime.

Сегодня в результате быстрого развития компьютерных технологий и активного расширения их применения в различных сферах жизни человечество вошло в новую эру информатизации, когда компьютер является необходимым инструментом в самых различных областях деятельности человека. Мы можем, например, элементарно общаться или совершать многомиллионные денежные операции с людьми с другой стороны планеты

и делать это быстро и недорого. Постоянное увеличение количества персональных компьютеров, свободный доступ к Интернету и динамично развивающийся рынок новых коммуникационных устройств изменили как способы проведения досуга, так и методы ведения бизнеса. Однако любая медаль имеет обратную сторону. Доступность глобальных цифровых технологий открыла новые возможности и преступному сообществу. Ежедневно обладающие компьютерными знаниями и навыками преступники незаконно получают огромные денежные средства. Хуже того, глобальные компьютерные сети также используются с целью разжигания национальной розни, способствуют усилению экстремизма и сепаратизма, достаточно часто применяются для координации и осуществления террористических актов. К глубокому сожалению, во многих случаях правоохранительные органы отстают от преступников, испытывая недостаток как технических средств, так и, что особенно важно, квалифицированного персонала для отражения новой и быстрорастущей угрозы киберпреступности с использованием компьютерной техники, информационных технологий и глобальных сетей). До недавнего времени в мире не придавали большого значения исследованиям феномена киберпреступности и последствий её расширения. Во многих случаях работники правоохранительных органов ощущали недостаток инструментария, необходимого для того чтобы заняться этой проблемой [1, С.405].

Важным элементом системы мер борьбы с компьютерной преступностью являются меры превентивного характера, или меры предупреждения. Большинство зарубежных специалистов указывают на то, что предупредить компьютерное преступление намного легче и проще, чем раскрыть и расследовать его.

Обычно выделяют три основные группы мер предупреждения компьютерных преступлений: правовые; организационно-технические и криминалистические, составляющие [2, С.404] в совокупности целостную систему борьбы с этим социально опасным явлением.

Специалисты называют пять основных направлений правового регулирования Интернет-отношений: защита личных данных и частной жизни в Сети; регулирование электронной коммерции и иных сделок и обеспечение их безопасности; защита интеллектуальной собственности; борьба против противоправного содержания информации и противоправного поведения в Сети; правовое регулирование электронных сообщений.

Что касается международно-правовой защиты интеллектуальной собственности, а также авторских прав на материалы, распространяемые по сети Интернет, то должны быть выработаны международные правовые нормы, устанавливающие ответственность за компьютерные преступления.

В Интернете пользователь не только получает возможность доступа к различным информационным ресурсам, но и создает канал для доступа к своему компьютеру. Ответственности за помещаемую в Интернет информацию фактически не несет ни автор, ни провайдер. Никто не несет ответственности и за попытки несанкционированного доступа к сетевым информационным ресурсам. Все вопросы защиты собственной информации относятся к компетенции пользователя. Необходима разработка международных правовых положений, устанавливающих ответственность за несанкционированный доступ к ресурсам Интернета. В соответствии с требованиями Резолюции 428 Консультативной Ассамблеи Совета Европы (раздел С) приоритет отдаётся уважению и защите частной жизни в ущерб праву на свободу информации.

Стратегия межрегионального сотрудничества в сфере противодействия компьютерной преступности и приоритетные направления ее реализации, в том числе: межрегиональные соглашения, организация межрегиональной оперативно-розыскной деятельности, обоснование необходимости разработки и принятия соответствующей комплексной межрегиональной программы.

Министерство внутренних дел Российской Федерации планирует создавать подразделения для борьбы с преступностью в области высоких

технологий, в том числе с теми, которые происходят через интернет. Так, до конца года должен быть подготовлен ведомственный приказ о внесении изменений в штатное расписание, а вместе с тем должны быть разработаны соответствующие приказы в территориальных ОВД [3, С.23].

Поэтому для стабильного развития всех регионов Российской Федерации (не считая городов федерального значения, где уже развиты меры защиты против преступлений в сфере высоких технологий) необходимо усовершенствовать систему оперативно-розыскных мероприятий, направленных на выявление лиц, которые будут проявлять нездоровый интерес к данной сфере, а именно те, которые обладают высокими навыками и познаниями в данной деятельности, дабы избежать проявления активности с их стороны на совершение преступлений в сфере высоких технологий. Самым распространенным видов преступлений в сфере высоких технологий являются преступления, которые посягают на общественные отношения, связанные нормальным функционированием банковской системы и прикрепленных к ней банков и кредитных организаций. И сейчас в регионах совершается все больше и больше таких преступлений, где в самым распространенным последствием является кража денег у граждан Российской Федерации с их дебиторских карт и сберегательных счетов, ячеек для хранения и иных способах хранения денежных средств и ценных бумаг.

Поэтому чтобы избежать такой неприятной ситуации необходимо совершать простые меры по охране своего имущества от преступного посягательства. Даже самые осторожные могут стать жертвами мошенников. Эти люди – тонкие психологи, и умеют найти подход даже к хладнокровным и бдительным. Однако есть способы существенно снизить риск финансовых махинаций. Общие правила известны всем: держать карту подальше от чужих глаз и не передавать ее другим лицам во временное пользование; во время расчета в торговых точках не выпускать карту из поля зрения, не позволять кассиру уходить с пластиком или проводить операции под

прилавком; не сообщать ПИН-код карты посторонним, в том числе сотрудникам банка; не хранить ПИН-код вместе с картой.

Поэтому для того, чтобы регион стабильно развивался и не был местом совершения преступлений в сфере высоких технологий необходимо не только принятие новых законов, которые будут направлены на ужесточение ответственности за таким видом преступления, а также координация действия правоохранительных органов, но необходимо гражданам соблюдать все необходимые меры безопасности в целях сохранения своего имущества от преступных посягательств.

Библиографический список

1. Ахмедова А.А., Махотенко М.А. Правовое регулирование использования цифровых технологий в судебной деятельности Российской Федерации // Интеллектуальные ресурсы – региональному развитию. – 2020. – № 2. – С. 404-408. – URL: https://elibrary.ru/download/elibrary_43033263_49278542.pdf (дата обращения 11.01.2020).
2. Махотенко М.А. Некоторые аспекты цифровой трансформации муниципалитетов // Интеллектуальные ресурсы – региональному развитию. – 2020. – № 2. – С. 400-404. – URL: https://elibrary.ru/download/elibrary_43033262_27169930.pdf (дата обращения 11.01.2020).
3. Фролов Д.Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом// Законодательство и экономика. – 2015. – №5. – С.23.