УДК 343.34:004

ПРАВОВЫЕ ОСНОВЫ ПРЕДУПРЕЖДЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

Шаромова А.И.

Студент 3 курса заочной формы обучения,

Направление подготовки 40.04.01 «Юриспруденция»

ЧОУ ВО ЮУ (ИУБиП)

Научный руководитель: **Сазанова Е.А.**

к.ю.н., доцент кафедры уголовно-правовых дисциплин

ЧОУ ВО ЮУ (ИУБиП)

Аннотация: В статье автор анализирует базовые направления повышения эффективности контроля над компьютерной преступностью в России, а также предлагает создание целостной системы обучения, подготовки и переподготовки специалистов по борьбе с компьютерными правонарушениями.

Ключевые слова: преступление, высокие технологии, объект преступления, компьютерная информация, вредоносные программы, информационные технологии.

LEGAL FRAMEWORK FOR CRIME PREVENTION IN THE FIELD OF HIGH TECHNOLOGY

Sharomova A.I.

Sazanova E.A.

Abstract: in the article, the author analyzes the basic directions for increasing the effectiveness of control over computer crime in Russia, and also proposes the creation of a holistic system for training, training and retraining specialists in combating computer offenses.

Keywords: crime, high technologies, crime object, computer information, malware, information technologies.

Борьба с компьютерной преступностью в России осуществляется в условиях действия комплекса факторов, снижающих ее эффективность. По мнению многих ученных к наиболее значимым следует отнести следующие факторы:

- отсутствие отлаженной системы правового и организационно-технического обеспечения законных интересов граждан, государства и общества в области информационной безопасности;

- ограниченные возможности бюджетного финансирования работ по созданию правовой, организационной и технической базы информационной безопасности;

- недостаточное осознание органами государственной власти на федеральном и, особенно, региональном уровне возможных политических, экономических, моральных и юридических последствий компьютерных преступлений;

- слабость координации действий по борьбе с компьютерными преступлениями правоохранительных органов, суда и прокуратуры и неподготовленность их кадрового состава к эффективному предупреждению, выявлению и расследованию таких деяний;

- несовершенство системы единого учета правонарушений, совершаемых с использованием средств информатизации;

- серьезное отставание отечественной индустрии средств и технологий информатизации и информационной безопасности от мирового уровня.

К базовым направлениям повышения эффективности контроля над компьютерной преступностью в России следует отнести:

- формирование целостной системы непрерывного отслеживания обстановки в сфере обеспечения информационной безопасности различных систем в стране и упреждающего принятия решений по выявлению и пресечению компьютерных преступлений; [5]

- организацию взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой;

- организацию эффективного взаимодействия правоохранительной системы России с правоохранительными органами зарубежных стран, осуществляющими борьбу с компьютерными преступлениями;

- координацию действий с общественными и частными организационными структурами (фондами, ассоциациями, фирмами, службами безопасности банковских и коммерческих структур), на своем

уровне осуществляющими практические мероприятия по обеспечению информационной безопасности.

Создаваемая система должна быть обеспечена высококвалифицированными кадрами. Создание целостной системы обучения, подготовки и переподготовки специалистов по борьбе с компьютерными правонарушениями является одной из основных задач.

В целях борьбы с компьютерной преступностью российским законодательством (глава 28 УК РФ) предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ). Содержание этих статей достаточно подробно рассматривалось в главе 4 данного учебного пособия.

Исходя из анализа главы 28 УК РФ, в соответствии со ст. 272 УК РФ, преступлением является неправомерный доступ к охраняемой законом компьютерной информации.

Признано, что для выработки всесторонней стратегии по профилактике и борьбе с компьютерной преступностью необходим единый согласованный план действий, включающий:

- неправительственные мероприятия, под которыми подразумевается программа инициатив по внедрению принципов ответственности в экономике и промышленности, стандартов профессиональной квалификации, технических и процедурных норм, а также этических установок и кодексов поведения;

- правительственные меры, то есть действия правительства на национальном уровне, направленные на совершенствование национального уголовного законодательства, а там, где это необходимо, и промышленного производства средств противодействия компьютерным преступлениям;

- межправительственные меры и международное сотрудничество, направленные на унификацию законодательных актов, развитие

международных стандартов и координацию действий органов уголовной юстиции. Прогресс в науке и технике идет в направлении новых информационных технологий. [4]

Чем больше компьютерные технологии вовлекаются в коммерческий оборот, тем больше возникает потребность в их защите от противоправных действий. Возникли понятия компьютерной преступности (киберпреступности), Интернет-преступности. Предметом преступной деятельности стала информация. Стремительно растет число преступлений в сфере интеллектуальной собственности и компьютерной информации. Перед правоохранительными органами России стала неотложная задача: на высоком профессиональном уровне раскрывать преступления в сфере высоких технологий.

Как показывает практика, оперативно-розыскная деятельность (ОРД) по раскрытию преступлений в сфере компьютерной информации должна осуществляться с учетом особой специфики этих преступлений.

Залог успешного осуществления оперативно-розыскных мероприятий состоит, прежде всего, в том, что стратегию и тактику выявления и раскрытия противоправных деяний необходимо строить на основе хороших знаний специфики состава преступления. [2,С.664] Другими словами, сотрудники правоохранительных органов должны обладать хорошими знаниями в области компьютерных технологий, кибернетики, психологии, психолингвистики. Понятно, что в настоящее время такой подход реализовать довольно трудно ввиду слабой подготовки сотрудников МВД в области современных информационных технологий.

Учитывая неотложность решения задачи по раскрытию и пресечению преступлений в рассматриваемой предметной области, оперативно-розыскная деятельность должна базироваться на следующих принципах:

- стратегия и тактика ОРД в области компьютерной информации должны строиться на основе самого широкого использования современных достижений в области информационных технологий;

- на этапе разработки стратегии и тактики ОРД в области компьютерной информации гласно и негласно должны привлекаться высококвалифицированные специалисты по информационным технологиям;

- необходимо существенно пересмотреть качественный состав субъектов при установлении конфиденциального сотрудничества (при осуществлении агентурной работы);

- арсенал оперативной техники необходимо комплектовать современными техническими приборами и устройствами (в т.ч. компьютерными программами), разработанными и успешно применяемыми в информационно-технологической сфере народнохозяйственного комплекса; [1, С.660]

- личный состав специализированных оперативных подразделений должен проходить соответствующую подготовку (переподготовку) по применению современных технологий и программных средств.

Без использования самых современных технических и программных средств эффективность оперативно-розыскной деятельности в сфере компьютерной информации резко снизится. [3, С.40]

Библиографический список

1. Бабкова, Н.С. Особенности совершения преступлений в сфере компьютерной информации / Н.С. Бабкова // Интеллектуальные ресурсы – региональному развитию. – 2021. – № 1. – С. 660-664. – EDN ZMSEZG.
2. Бабкова, Н.С. Проблемы раскрытия преступлений в сфере компьютерной информации / Н. С. Бабкова // Интеллектуальные ресурсы – региональному развитию. – 2021. – № 1. – С. 664-667. – EDN MMNVYK.
3. Иванов В.В. Законодательные меры по борьбе с компьютерной преступностью. // Проблемы преступности в капиталистических странах. – 2018. – №10. – С. 40.
4. Шахрай С.С. «Система преступлений в сфере компьютерной информации: сравнительно-правовой, социолого-криминологический и уголовно-правовой аспекты»: дис. ... кандидата юридических наук. – Москва, 2016, – С. 149.
5. Шехов В.В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): автореф. дис. … канд. юрид. наук: 12.00.08 – уголовное право и криминология; уголовно-исполнительное право / В. В. Шехов. – Н. Новгород, 2015. – 28 с.