УДК 343.3.7+004.056.5

ПРЕСТУПЛЕНИЯ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ: ПРОБЛЕМЫ ПОДГОТОВКИ КАДРОВ

Дмитриева А.Р., аспирант 1года обучения
ЧОУ ВО ЮУ (ИУБиП), e-mail: a.dm3008@yandex.ru

Аннотация: В данной статье проанализированы современные образовательные программы подготовки специалистов в сфере обеспечения кибербезопасности и противодействия киберпреступности, а также проанализированы проблемы расследования преступлений в сфере компьютерной информации, были определены знания и компетенции, которыми должен обладать специалист в сфере противодействия киберпреступности и предложены пути решения выявленных проблем.
Ключевые слова: высокие технологии, информационные технологии, кибербезопасность, киберпреступления, повышение квалификации, профессиональная переподготовка кадров, цифровые компетенции.

CRIMES IN THE SPHERE OF HIGH TECHNOLOGIES: PROBLEMS OF PERSONNEL TRAINING

Dmitrieva A.R.

Abstract: This article analyzes modern educational programs for training specialists in the field of cybersecurity and countering cybercrime, as well as analyzes the problems of investigating crimes in the field of computer information, identifies the knowledge and competencies that a specialist in the field of countering cybercrime should have, and suggests ways to solve the identified problems.
Keyword: high technology, information technology, cybersecurity, cybercrime, training, professional retraining, digital competence.

Интернет является инструментом коммуникации и взаимодействия между людьми. Человек XXI века способен покупать товары, общаться со своими близкими и зарабатывать, не выходя из дома. Неудивительно, что вместе с глобализацией всего мира и цифровизацией экономики развитых стран, появилось такое понятие как «компьютерная преступность» – преступность в сфере высоких технологий. За последнее десятилетие компьютерная преступность стала привлекать внимание, как правоохранительных органов, так и государственных структур, что свидетельствует о быстром ее росте в сфере высоких технологий.

Наибольшую угрозу компьютерная преступность представляет для сферы бизнеса. С одной стороны это показатель развития страны с точки зрения реновации и цифровизации экономики, а с другой – двигатель,

направленный на совершенствование технологий в области – защиты информации считываемой и обрабатываемой вычислительной машиной [1].

Впервые о преступлениях в виртуальном мире стали говорить в Америке в начале 60-х гг, а затем уже в Европе, когда появились первые правонарушения с использованием ЭВМ. Понятие компьютерной преступности появилось в эпоху «компьютерно-телефонного фанатизма» и выражалось в недобросовестном использовании компьютеров и телефонов для заказа различных товаров и услуг через сети различных торговых фирм без оплаты.

Правовая база противодействия организованной преступности, не смотря на существенные изменения законодательства как на международном, так и на национальном уровне не соответствует современным реалиям, так как существенно отстает от развития высоких информационных технологий, используемых преступным сообществом. В этой связи следует отметить, что настала необходимость выработки эффективных мер борьбы с ней.

Киберугрозы постоянно меняются, становятся менее заметны для пользователя в момент их активной работы, тем самым становятся более опасными и поэтому требуют высокого уровня технической подготовки. Для этого в вопросе противодействия киберпреступности правоохранительным органам необходимо обладать различным набором кадров, в том числе и техническими специалистами, которые смогут оказывать содействие в предупреждении и раскрытии киберпреступлений. Соглашение между Интерполом и «Лабораторией Касперского» является серьезным шагом к глобальному объединению усилий в борьбе с киберпреступностью и дает уверенности в том, что будут разработаны самые современные средства обеспечения безопасности.

В связи с вышесказанным есть вопрос о фактическом количестве и качестве преступлений в сфере компьютерной информации и высоких технологий, совершаемых в Российской Федерации, об их официальной регистрации и скрытом характере деяний в указанной сфере. Отдельно –

вопрос об уровне профессиональной подготовленности сотрудников правоохранительных органов, специализирующихся на выявлении, раскрытии и расследовании названных преступлений.

Ранее подготовка исследования киберпреступности и подготовка специалистов в сфере информационной безопасности проводились только в закрытых и отдельных военных вузах. Стремительное развитие информационных технологий и повышение актуальности проблем ИБ определили понимание руководства государства о необходимости организации более масштабной и открытой системы подготовки специалистов.

Сейчас не во всех вузах России запущены образовательные программы подготовки кадров, такие как 10.05.01 «Компьютерная безопасность», 10.03.01 «Информационная безопасность» и т.п. Студенты изучают языки программирования, основы компьютерной безопасности, криптографические методы защиты информации, администрирование сетей, технические средства и методы защиты информации, алгоритмы кодирования и сжатия информации, анализ уязвимостей программного обеспечения. Выпускники могут разрабатывать и применять методы, средства защиты, контролировать процессы создания программного обеспечения, анализировать защиту компьютерных систем от вирусов. Специалисты работают в органах власти и местного самоуправления, на промышленных предприятиях, в финансовых учреждениях, банках и других учреждениях.

Необходимыми условиями для борьбы с компьютерными преступлениями являются: знания теоретических основ уголовного права и процесса, умение с помощью различных средств и приемов толковать уголовно-правовые нормы, применение норм уголовного законодательства в судебно-следственной практике, владение основными методами, способами и средствами получения, хранения, переработки информации, навыки работы с компьютером как средством управления информацией; применение нормативных правовых актов; реализация норм материального и

процессуального права в профессиональной деятельности; юридически правильная квалификация фактов и обстоятельств.

Для того, чтобы обеспечить специалистов необходимым набором компетенций, в основу профессионального цикла образовательной программы должны лечь дисциплины, изучающие механизм совершения киберпреступлений, типы и классификацию киберпреступлений, криминологические, технические и психологические аспекты совершения таких преступлений. В настоящее время остро стоит две проблемы: проблема теории квалификации киберпреступлений и технические особенности совершения и расследования киберпреступлений. У современных специалистов не хватает технических компетенций для успешной борьбы с киберпреступностью, поэтому считаем необходимым включить в профессиональный цикл образовательной программы такие дисциплины как:

– вычислительные системы, сети и телекоммуникации;

– основы программирования;

– платежные системы;

– информационная безопасность;

– компьютерное мошенничество, проблемы квалификации мошенничества с использованием банковских пластиковых карт;

– криптография и защита информации;

– проблемы квалификации использования высоких технологий при совершении преступлений террористической направленности.

Таким образом, проанализировав выше сказанное можно сделать вывод о необходимости создания новой образовательной программы, которая будет содержать в себе необходимый набор компетенций для подготовки кадров для борьбы с преступностью в сфере компьютерной информации. Наиболее оптимальным вариантом будет являться создание профиля образовательной программы для магистратуры, так как такая образовательная программа будет одновременно служить следующей ступенью высшего образования после бакалавриата, повышением квалификации для выпускников

специалитета, а также программой переподготовки для действующих сотрудников правоохранительных органов.

Библиографический список

1. Понфанов Р.О. Основные атаки в сетях. [Электронный ресурс] – URL: http://www.intuit.ru. 2016.
2. Постановление Пленума Верховного Суда РФ от 22.12.2015 № 58 «О практике назначения судами Российской Федерации уголовного наказания» // Бюллетень Верховного Суда РФ. – 2016. – № 2.
3. Храмов В.В. Оценка качества подготовки специалистов в условиях современного образовательного процесса // Интеллектуальные ресурсы – региональному развитию. – 2014. – № 1. – С. 125-130.
4. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (УК РФ).
5. Комментарий к Уголовному кодексу Российской Федерации (постатейный) /под ред. А.В. Бриллиантова). – М.: Проспект, 2010.
6. Лихачев. В. Кадровое обеспечение информационной безопасности // Кадровик. Кадровый менеджмент. – 2007. – №12.
7. Храмов В.В. Генерация моделей объектов интеллектуального пространства. Теория и использование для управления сложными системами // Управление в социальных, экономических и технических системах: Труды межреспубликанской научной конференции. – 2000. – С. 67-68. – URL:https://elibrary.ru/item.asp?id=32737843 (Дата обращения 05.02.2021)