Талагаева Екатерина Владимировна
студентка
Институт права
ФГБОУ ВО «Самарский государственный
экономический университет»
г. Самара, Самарская область
Губайдуллина Эльмира Хамитовна
преподаватель
ФГБОУ ВО «Самарский государственный
экономический университет»
г. Самара, Самарская область

ПРЕСТУПЛЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Аннотация: *в данной статье рассматриваются проблемные вопросы безопасности компьютерной информации, конкретизируются основные меры профилактики, с помощью которых можно предотвратить информационные правонарушения.*

Ключевые слова: *компьютерная преступность, киберпространство, безопасность компьютерной информации, информация.*

На сегодняшний день не осталось сфер жизни, где не используется глобальная сеть «Интернет», она нашла свое применение и в политике, науке, культуре, бизнесе и образовании. Сеть «Интернет» представляет собой огромное пространство, на котором происходит интеллектуальное творчество, поиск необходимых материалов, обмен информацией, и самое главное, это общение в социальных сетях. Информация копируется, передается очень просто, существующая анонимность этих действий представляет собой серьезную угрозу соблюдения прав.

Преступление в сети «Интернет» причиняют как неимущественный, так и имущественный вред, тем самым посягая на гарантии Конституции Российской Федерации. Однако Уголовный закон не содержит нормы права, которые бы предусматривали наказание за данное деяние.

Чтобы борьба с преступностью в информационной сфере была более эффективной, мировое сообщество объединяет свои усилия и идет по пути максимального сближения своих национальных законодательств [1].

Так, борьба с компьютерными преступлениями в современном мире приобретает большую актуальность, которую можно приравнивать к проблеме терроризма.

Термин «компьютерная преступность» впервые появился в американской, а потом и в другой печати зарубежья, где – то в начале 1960 г., тогда были выявлены самые первые случаи преступлений, совершенных с использованием ЭВМ. Первые компьютерные преступления начались с нарушения, впервые зарегистрированного Stanford Research Institute (США) в 1958 году [2]. Но это было лишь сигналом о начале преступлений в информационной сфере. Первый случай хищения с использованием компьютера был зарегистрирован в 1966 году, когда был ограблен Minnesota bank [3].

В 1996 году российский законодатель, исходя из новых экономических, социальных и политических отношений, которые сложились в обществе и в соответствии с потребностью в усилении борьбы с преступностью, принял Уголовный кодекс. Так, глава 28 «Преступление в сфере компьютерной информации» содержит большое количество терминов и понятий, ранее не использованные в уголовно – правовой терминологии, а некоторые и в законодательстве, регулировавшем информационные правоотношения. Главным термином в информационных правоотношениях – понятие «информация». В Российском законодательстве существует Федеральный закон «Об информации, информатизации и защите информации»: «Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления» [4]. Любая информация имеет свою стоимостную оценку – цену, причем для каждого индивидуальную. Для кого – то информация о чем – либо или о ком – либо может иметь бесценный характер. Так, понятие компьютерная информация имеет несколько определений, но наиболее точное это информация, зафиксированная на

машинном носителе и передаваемая по телекоммуникационным каналам в форме доступной восприятию ЭВМ [5].

Как известно, существует определенная классификация информационных и компьютерных преступлений. Согласно классификации В.В. Крылова, то противопроавные действия с компьютерной информацией включает в себя:

– неправомерный доступ к информации с использованием компьютерной техники;

– распространение вредоносных программ для ЭВМ.

Противоправные действия в области телекоммуникаций включают действия:

– незаконная прослушка телефонных разговоров;

– перехват информации с различных технических каналов.

Противоправные действия с использованием информационного оборудования:

– нарушение правил при эксплуатации ЭВМ;

– поддельное изготовление кредитных карт.

Противоправные действия любой другой информации включают:

– нарушения конфиденциальности тайной переписки, государственной тайны, банковской тайны;

– операции с дефектной информацией (ложная реклама, фальсификация избирательных документов и т. д.) [6].

Очень актуальной для России является проблема правового регулирования отношений в сфере информатизации всего обществ, но и обеспечение, прежде всего информационной безопасности. Именно поэтому, на сегодняшний день приняты и действуют нормативно – правовые акты, которые полностью регламентируют указанные отношения между людьми, а именно Федеральный закон «О правовой охране топологий интегральных микросхем». Данный закон закрепляет обязательственные правила работы со всеми базами данных, программными продуктами файлами. Эти законы являются основными нормативными актами

для работников организаций, связанных по своему роду деятельности с компьютерной информацией и электронными технологиями.

За нарушение норм, которые закреплены в вышеупомянутом законе, наступает уголовная ответственность. К уголовно наказуемым отнесены: нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ), неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание и использование, распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).

В Росси с каждым годом увеличивается число преступлений, которые совершаются с использованием информационных технологий и расследовать их достаточно трудно [7]. Согласно гл. 28 УК РФ за совершение, какого – либо вида преступления в сфере компьютерной информации предусмотрены такие виды наказания как: ограничение свободы, арест, штраф, обязательные работы, исправительные работы, лишение права занимать определенные должности [8]. Опыт борьбы с преступлениями растет и свидетельствует о том, что самым эффективным способом в борьбе с информационной преступностью является общесоциальное предупреждение, а если точнее, то комплекс мер экономического, социального, политического, правого и культурного характера, основным направлением которого является повышение социальной справедливости, уровня жизни всего населения страны.

Существует три группы мер предупреждения преступлений в сфере компьютерной информации:

Правовые (включают нормотворческую деятельность по созданию законодательства, регулирующего отношения в обществе, связанного с обеспечением информационной безопасности).

Организационные (разработка программы защиты, изучение обстановки на объекте, деятельность по проведению указанной программы в жизнь, организация конфиденциального делопроизводства) [9].

Информационная преступность на сегодняшний момент является наиболее сложным явлением. В связи с новыми социальными преобразованиями, которые происходят в обществе, правоохранительные органы в своей деятельности

должны большое внимание уделять криминологическим исследованиям, результат которых должен привести к формированию новых путей решений борьбы с преступностью в киберпространстве, обеспечить правоприменительную практику научно обусловленными рекомендациями.

Список литературы

1. Флетчер Дж. Основные концепции современного уголовного права / Дж. Флетчер, А.В. Наумов. – М., 1998. – С. 352.

2. Combatigation McGraw – Mill., 1922. – С. 23–24.

3. Серго А.Г. Интернет и право. – М., 2003. – С. 217.

4. Уголовный кодекс РФ. – Ст. 272. – Глава 28.

5. Комментарий к Уголовному кодексу РФ / Под общ. ред. Ю.И. Скуратова, В.М. Лебедева. – М., 1999. – С. 696.

6. Крыло В.В. Расследование преступлений в сфере информации. – М., 1998. – С. 165.

7. Красненкова Е.В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами.: Дис. ... канд. юрид. наук: 12.00.08. – М., 2006. – С. 118.

8. Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны.: Дис. … канд. юрид. наук: 12.00.08. – Казань., 2008. – С. 27.

9. Курушин В.Д. Указ. соч. / В.Д. Курушин, Л. Минаев. – С. 171.