УГОЛОВНО-ПРАВОВАЯ ОХРАНА СФЕРЫ ВЫСОКИХ ТЕХНОЛОГИЙ КАК НЕОБХОДИМОЕ УСЛОВИЕ СТАБИЛЬНОГО РЕГИОНАЛЬНОГО РАЗВИТИЯ

Кулишова Диана Васильевна

студент ЧОУ ВО «Южный Университет (ИУБиП)», РФ, г. Ростов-на-Дону

Актуальность темы обусловлена тем, что в современных условиях сфера высоких технологии становятся главной составляющей и неотъемлемой частью современного общества.

Несмотря на то, что первый персональный компьютер появился относительно недавно, дальнейшее стремительное развитие компьютерных и других информационных технологий стало следствием различных проблем, в том числе и в области уголовно-правовогорегулирования отношений в сфере компьютерной информации.

Эффективное противодействие компьютерным преступлениям, защита прав и законных интересов граждан, а также обеспечение информационной безопасности государства и юридических лиц возможно только при постоянно изменяющемся комплексе всех мер защиты, включая и формирование правовой базы.

Информатизация современного общества привела к формированию новых видов преступлений, при совершении которых используются вычислительные системы, новейшие средства телекоммуникации и связи, средства негласного получения информации и т.п.

За последние 10-15 лет резко увеличилось количество преступлений с использованием вычислительной техники или иной электронной аппаратуры, хищения наличных и безналичных денежных средств.

Для совершения преступлений все чаще используются устройства, в основе которых лежат высокоточные технологии их изготовления и функционирования, иными словами, это преступления, в которых используются высокие технологии.

Преступления в сфере компьютерной информации - общественно опасные деяния, посягающие на отношения, обеспечивающие безопасность информационного процесса в части сбора, обработки, накопления, хранения, поиска и распространения информации с использованием ЭВМ, их систем и сетей, ответственность за которые предусмотрена ст. 272-274 главы 28 УК РФ.

Действующим УК РФ предусмотрена ответственность за три вида преступлений в сфере компьютерной информации: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации компьютерной техники (ст. 274 УК РФ).

Меры предупреждения над компьютерной преступностью подразделяются на правовые, организационно-тактические и программно-технические.

К правовым мерам относятся разработка норм, устанавливающих ответственность за совершение компьютерных преступлений, защита авторских прав программистов, а также вопросы контроля за разработчиками компьютерных систем и применение международных договоров об их ограничениях.

К организационно-тактическим мерам относятся охрана вычислительных центров,

Кулишова Д.В. УГОЛОВНО-ПРАВОВАЯ ОХРАНА СФЕРЫ ВЫСОКИХ ТЕХНОЛОГИЙ КАК НЕОБХОДИМОЕ УСЛОВИЕ СТАБИЛЬНОГО РЕГИОНАЛЬНОГО РАЗВИТИЯ // Молодежный научный форум: электр. сб. ст. по мат. CLXXIII междунар. студ. науч.-практ. конф. № 22(173). URL: https://nauchforum.ru/archive/MNF_interdisciplinarity/22(173).pdf *(дата обращения: 03.09.2025)*

тщательность подбора персонала, исключение случаев ведения особо важных работ только одним человеком и т.п.

К программно-техническим мерам можно отнести защиту от несанкционированного доступа к системе, профилактику от компьютерных вирусов, резервирование особо важных компьютерных подсистем, применение конструктивных мер защит от хищений, саботажа диверсий, взрывов, установку резервных систем электропитания, оснащение помещения кодовыми замками, установку сигнализации и другие меры.

Основной целью государственной политики по выявлению и пресечению компьютерных преступлений является создание эффективной национальной системы борьбы с правонарушениями в сфере компьютерной информации.

Недавно ФБР приняло на вооружение новую технологию мониторинга Интернета вместо устаревшей системы Carnivore.

Возможности «новорожденного» значительно шире – они позволяют отслеживать сетевую активность подозреваемых в совершении преступлений, одновременно вести базу данных о вполне законопослушных гражданах, а также фиксировать интернет-трафик, включая IP-адреса, просмотры отдельных страниц и электронную почту.

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 в совокупности целостную систему борьбы с этим социально опасным явлением.

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 форм хранения денежных средств и ценных бумаг.

Поэтому, анализируя все возникающие проблемы уголовно-правовой охраны сферы высоких технологий как необходимого условия стабильного регионального развития можно прийти к выводу, что для формирования сферы развития защиты таких «инновационных объектов» от преступных посягательств необходимо разработать специальные приемы, методы, межрегиональные программы для борьбы с таким видом преступлений в целях обеспечения стабильного развития регионов Российской Федерации.

Список литературы:

1. Гражданский кодекс Российской Федерации от 30 ноября 1994 года № 51 - ФЗ (ред. от 16.12.2019) [Электронный ресурс] // КонсультантПлюс. – Режим доступа: http://www.consultant.ru (Дата обращения 10.02.2021).

2. Гончаров Д.Ю. Проблемы квалификации хищений, совершаемых с помощью компьютеров // Право. 2019. № 64.

3. Кушниренко С.П., Панфилова Е.И. Уголовно-процессуальные способы изъятия компьютерной информации по делам об экономических преступлениях: Учеб. пособие. 2-е

изд., исп. и доп. - СПб., 2017. — 88 с.

4. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: Учеб. - практ. пособие. М. «Палеотип», 2012 - 148 с.

5. Максимов В.Ю. Незаконное обращение с вредоносными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания. Краснодар: Ставропольский государственный университет, 2016. – 169 с.

6. 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: Б. и., 2015. – 28 с.

7. Широкова А.В. «Проблемы квалификации преступлений в сфере высоких технологий»: Дис. ... кандидата юридических наук: Москва, 2018, 220 с.