ПРОБЛЕМЫ РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ И ПУТИ ИХ РЕШЕНИЯ

Духова Анастасия Александровна

студент, Саратовская государственная юридическая академия, РФ, г. Саратов

Кананыхина Алина Александровна

студент, Саратовская государственная юридическая академия, РФ, г. Саратов

Гарига Ольга Анатольевна

научный руководитель, канд. юрид. наук, доцент, Саратовская государственная юридическая академия, РФ, г. Саратов

Развитие информационных технологий не только принесло огромную пользу обществу, но также и открыло новые способы для совершения преступлений в компьютерной сфере, основной формой выражения которых является – кибермошенничество. Возможность дистанционного совершения таких преступлений обеспечивает их низкую раскрываемость и высокую латентность, в связи с чем мошенники все чаще стали использовать ресурсы компьютерных систем для совершения хищения информации.

С каждым годом количество преступлений в сфере информационных технологий только растет, это подтверждают данные статистики. По данным МВД за 2022 год количество киберпреступлений увеличилось на 20,8%. По аналитическим данным, в 2023 году прогнозируется еще больше преступлений в информационной сфере.

В атаках на организации злоумышленникам удалось украсть конфиденциальную информацию в 47% случаев, в атаках на частных лиц – в 64%. Как отмечают МВД России каждое четвертое преступление совершается, непосредственно, высокими технологиями [1, с. 3].

В связи с чем органы правопорядка ведут активную борьбу с кибермошенничеством, методика расследования таких преступлений совершенствуются, однако уровень раскрываемости таких преступлений остается достаточно низким. В нормативном регулировании также остается множество пробелов, которые не позволяют в полной мере противостоять мошенникам.

При разработке методики расследования кибермошенничества используется сочетание методов расследования простого мошенничества и специфичных методов расследования преступлений с сфере компьютерной информации. Основным структурным элементом методики является криминалистическая характеристика данного преступления. Однако с этим возникают проблемы, поскольку кибермошенничество является довольно прогрессивным и структурно сложным видом преступления, а быстро адаптировать методику расследования и раскрытия преступления к новым реалиям не всегда возможно.

При расследовании преступлений в сфере информационных технологий также возникает вопрос к какому виду следов отнести компьютерную информацию. Виртуальный характер не позволяет отнести их ни к идеальным, ни к материальным видам следов. В связи с эти законодателю необходимо внести новый вид следов - «виртуальные следы», к которым следует относить следы киберпреступлений. Это, в свою очередь, облегчило бы документальное оформление деятельности следователя [2, с. 113].

При разработке методики расследования киберпреступлений предполагается, что

следователь и другие участники производства по делу обладают специальными знаниями в сфере IT технологий, понимают специфику компьютерных преступлений и разбираются в самих информационных технологиях. Однако на практике это не всегда так [3, с.66]. На сегодняшний день, в России отмечается наличие дефицита специалистов в правоохранительных органах, которые имеют профессиональные навыки и знания в расследование киберпреступлений. В настоящее время, не во всех образовательных учреждениях имеются программы обучения предоставляющие знания в сфере компьютерных технологий, которые являются необходимыми при расследовании киберпреступлений. Для решения данной проблемы следует организовать специальные лаборатории, направленные на практическое ознакомление и решение поставленных задач [4, с. 16]. В организованную деятельность предлагается включить, помимо научно-педагогического состава, также экспертов, имеющих знания и опыт в предупреждение и расследование киберпреступлений. Предлагаемая программа, позволит обучающимся не только ознакомиться с современными методами и приемами работы киберкриминалистов, но и стать профессионалами в данной сфере, что способствует повышению кадров в узконаправленной специальности.

Информационные технологии, используемые при совершении кибермошенничества, предполагают, что при их применении злоумышленник руководствуются особой логикой, основанной на строгой дисциплине к мыслительному процессу. Следователь должен уметь противостоять таким действиям, оставаться дисциплинированным и сосредоточенным при решении трудных задач, а также быть готовым к изучению нового, т.к. данная сфера очень динамично и стремительно развивается.

Ещё одной не менее важной проблемой является то, что в государстве отсутствует новая система для криминалистического учета и идентификации данных, которые возможно использовать для предупреждений и расследований в киберпространстве. При криминалистической регистрации следует использовать идентификаторы электронных устройств пользователей, благодаря которым смогут оставаться при посещении ими любого интернет-ресурса, а именно модель использованного устройства, установленная версия операционной системы и браузера, ip-адрес и другие параметры соединения, рекламные идентификаторы и иные. В данной совокупности идентификационные элементы способствуют установить и выделить уникальное устройство из прочих. Например, на базе отдела специальных разработок Технопарка Санкт-Петербурга в начале 2020 года компанией «Интернет-Розыск» был создан прототип такой разработки, предназначенной для предупреждения, пресечения и расследования правонарушений, совершаемых посредством современных информационно-телекоммуникационных технологий. Агрегация в рамках проекта стартапов правоохранительной направленности с готовыми решениями позволит сократить временные и финансовые затраты, которые могли бы понести правоохранительные органы при разработке решений с нуля [5, с. 1].

Таким образом, киберпреступления являются насущной проблемой современного мира. С развитием информационных технологий методы и способы совершения преступлений в IT сфере совершенствуется и усложняются. В связи с чем методика расследования и раскрытия киберпреступлений требует постоянного совершенствования, т. к. преступления в сфере компьютерной информации являются быстроразвивающимися и сложными видами преступлений, к расследованию которых необходимо подходить ответственно и комплексно.

Список литературы:

1. Прокопьев Д. За цифрой большая работа // Щит и Меч. - 2023. - 2.02. - Ст. 4

2. Маилян А. В «Актуальные вопросы расследования и раскрытия кибермошенничества «фишинг» // Философия права. 2022. №2 (101). URL: https://cyberleninka.ru/article/n/aktualnye-voprosy-rassledovaniya-i-raskrytiya-kibermoshennichestva-fishing (дата обращения: 16.04.2023).

3. Билан, А. Н. Методика расследования кибермошенничества / А. Н. Билан. — Текст : непосредственный // Молодой ученый. — 2022. — № 32 (427). — С. 65-68. — URL: https://moluch.ru/archive/427/94355/ (дата обращения: 16.04.2023).

4. Бедеров И.С. Проблемы и тенденции в расследовании преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Противодействие киберпреступлениям и преступлениям в сфере высоких технологий. - М.: Московская академия СК России, 2021. - С. 15-17.

5. Открытие отдела специальных разработок // Интернет-розыск URL: https://интернет-розыск.рф/ (дата обращения: 16.04.2023).