EYIB
EDUCATIONAL YIELD
INSIGHTS & BREAKTHROUGHS
TA'LIMGA OID TUSHUNCHALAR VA YUTUQLAR
ISSN:3060-4648
Vol.5 №2
https://eyib.uz

ОПЕРАТИВНО РОЗЫСКНАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ.

Абдухакимов Парвиз

Академия МВД Республики Узбекистан курсант 338-группы

Annotatsiya

Преступления в сфере информационных технологий представляют особую проблему для правоохранительных органов по всему миру. В статье рассматриваются оперативно-розыскные особенности подобных преступлений и сложности, с которыми сталкиваются следователи при борьбе с киберпреступностью. Рассматривая природу этих правонарушений, статья стремится пролить свет на ключевые стратегии и инструменты, необходимые для эффективного расследования и предотвращения в цифровую эпоху.

Kalit so‘zlar: киберпреступность, информационные технологии, эксплуатационные характеристики, методы расследования, цифровая криминалистика

Авторизоваться

В современном взаимосвязанном мире стремительное развитие информационных технологий произвело революцию в различных аспектах общественной жизни. Однако наряду с этими достижениями наблюдается рост киберпреступности, что является серьезной проблемой для правоохранительных органов по всему миру. Преступления в сфере информационных технологий охватывают широкий спектр правонарушений, включая взлом, утечку данных, кражу личных данных и мошенничество в Интернете. Расследование подобных преступлений требует глубокого понимания оперативных и следственных особенностей, присущих цифровому ландшафту.

Оперативные характеристики киберпреступлений

Киберпреступления обладают уникальными операциональными характеристиками, которые отличают их от традиционных преступлений. Одной из таких особенностей является анонимность и географическая гибкость, которыми преступники пользуются в цифровой сфере. Преступники могут действовать из любой точки мира, что затрудняет их отслеживание и поимку правоохранительными органами. Кроме того, скорость совершения киберпреступлений и объем данных представляют собой существенные препятствия для следователей.

Стремительный характер киберпреступлений отличает их от традиционных преступлений и создает особые проблемы для

правоохранительных органов. Преступная деятельность в цифровой сфере имеет уникальные особенности, которые усложняют расследование и профилактику.

Анонимность и географическая гибкость:

Одной из ключевых характеристик киберпреступности является анонимность и географическая гибкость, которыми пользуются преступники. Преступники могут действовать из удаленных точек по всему миру, используя такие инструменты, как VPN и сетевую анонимность, чтобы скрыть свою личность и избежать обнаружения. Такая анонимность затрудняет правоохранительным органам выявление источников кибератак и установление виновных. Кроме того, безграничный характер Интернета позволяет киберпреступникам преследовать жертв в разных юрисдикциях из одного места, что усложняет судебные разбирательства и процессы экстрадиции.

Скорость и емкость передачи данных:

Еще одной важной характеристикой деятельности является быстрый рост киберпреступности. В цифровой сфере злоумышленники могут запускать атаки за считанные секунды, используя уязвимости и нанося значительный ущерб еще до того, как будут приняты меры безопасности. Огромный объем данных, связанных с киберпреступностью, еще больше усложняет задачу следователям. Во время кибератак генерируются большие объемы данных, включая журналы, сетевой трафик и системную информацию, для эффективного анализа и обработки которых требуются специализированные инструменты и опыт.

Сложность и техническая изощренность:

Киберпреступления часто связаны со сложными приемами и передовыми технологиями, для понимания и расследования которых требуется высокий уровень технических знаний. Киберпреступники используют широкий спектр инструментов и стратегий для осуществления своей незаконной деятельности: от сложных вредоносных программ и методов шифрования до тактик социальной инженерии и ботнетов. Расследование таких преступлений требует от следователей быть в курсе последних тенденций в области кибербезопасности, методологий цифровой криминалистики и новых угроз, чтобы эффективно реагировать на кибератаки и предотвращать их последствия.

Гибкость и тактика развития:

Еще одной характеристикой киберпреступности является гибкость и постоянное развитие тактики, используемой киберпреступниками. По мере совершенствования мер кибербезопасности и устранения уязвимостей преступники разрабатывают новые методы обхода защиты и эксплуатации новых технологий. Эта игра в кошки-мышки между киберпреступниками и экспертами по безопасности требует проактивного и динамичного подхода к кибербезопасности, постоянного мониторинга, обмена данными об угрозах и сотрудничества между заинтересованными сторонами, чтобы оставаться впереди развивающихся угроз.

Методы расследования в цифровой криминалистике

Цифровая криминалистика играет решающую роль в расследовании киберпреступлений. Он включает сбор, хранение, анализ и представление цифровых доказательств таким образом, чтобы они были допустимы в суде.

Следователи используют специализированные инструменты и методы для извлечения важной информации из цифровых устройств, сетей и онлайн-платформ. К этим методам относятся, среди прочего, создание образа диска, сетевая криминалистика, анализ памяти и анализ метаданных.

Проблемы расследования киберпреступлений

Расследование киберпреступлений создает множество проблем для правоохранительных органов. Одним из основных препятствий является транснациональный характер многих киберпреступлений, что требует международного сотрудничества и координации действий правоохранительных органов. Кроме того, постоянно меняющиеся тактики, используемые киберпреступниками, требуют от следователей быть в курсе последних технологических разработок и угроз безопасности.

Эффективные стратегии скрининга и профилактики

Для эффективной борьбы с киберпреступностью правоохранительные органы должны использовать комплексный подход, сочетающий в себе стратегии упреждающего предотвращения с надежными методами расследования. Это включает в себя инвестирование в программы обучения следователей, создание специализированных подразделений по борьбе с киберпреступностью, развитие партнерских отношений с частным сектором и повышение осведомленности общественности о передовых методах обеспечения кибербезопасности.

Заключение

Киберпреступность является серьезной проблемой для правоохранительных органов по всему миру. Понимая стремительный характер киберпреступности и применяя передовые методы расследования, следователи могут повысить свои возможности по эффективной борьбе с цифровыми угрозами. Правоохранительные органы должны адаптироваться к меняющейся ситуации в сфере киберпреступности и сотрудничать на глобальном уровне для защиты отдельных лиц, предприятий и критически важной инфраструктуры от цифровых злоумышленников. В заключение следует отметить, что оперативные характеристики киберпреступности подчеркивают сложность и динамичность цифровых угроз, требующих многогранного и совместного подхода для эффективной борьбы с киберпреступной деятельностью. Правоохранительные органы, специалисты по кибербезопасности, политики и частный сектор должны работать сообща для повышения устойчивости, укрепления обороны и смягчения последствий киберпреступности во взаимосвязанном и зависящем от технологий мире.

Использованная литература:

1. O‘zbekiston Respublikasining 2017-yil 16-oktyabrdagi O‘RQ-448-son “O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida”gi Qonuni // Qonun hujjatlari ma’lumotlari milliy bazasi, 17.10.2017 y., 03/17/448/0126-son; 30.01.2018 y., 03/18/463/0634-son; 08.01.2020 y., 03/20/601/0025-son; Qonunchilik ma’lumotlari milliy bazasi, 24.11.2021 y., 03/21/730/1089-son, 03/22/763/0306-son; 29.10.2022 y., 03/22/798/0972-son.

2. O‘zbekiston Respublikasining 2019-yil 15-yanvardagi O‘RQ-516-son “Iqtisodiy jinoyatlarga va ommaviy qirg‘in qurolini tarqatishni moliyalashtirishga qarshi kurashish mexanizmlari takomillashtirilishi munosabati bilan O‘zbekiston Respublikasining ayrim qonun hujjatlariga o‘zgartish va qo‘shimchalar kiritish to‘g‘risida” qonuni // Qonun hujjatlari ma’lumotlari milliy bazasi, 16.01.2019 y., 03/19/516/2484-son; 08.01.2020 y., 03/20/601/0025-son; 26.02.2021 y., 03/21/677/0155-son; Qonunchilik ma’lumotlari milliy bazasi, 24.11.2021 y., 03/21/730/1089-son

3. Smit, J. (2020). Kiberjinoyat va raqamli tergov. Nyu-York: Springer.

4. Keysi, E. (2018). Raqamli dalillar va kompyuter jinoyati. Kembrij: Akademik matbuot.

5. Gudman, M. (2019). Kiber huquq va kiber axloqni tekshirish. London: Routledge.