УДК 34:51:659

Кульчунова К.Т.

*ЫГУ им. К.Тыныстанова*

# ПРОБЛЕМЫ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА. КРИМИНОЛОГИЧЕСКИЕ ОСОБЕННОСТИ КОМПЬЮТЕРНОГО ПРЕСТУПЛЕНИЯ

*Обеспечение безопасности при работе с компьютерной системой – задача многогранная. В ней можно выделить два основных направления: безопасность персонала и информационную безопасность. Оба аспекта составляют предмет жарких дискуссий ведущих специалистов отрасли на многочисленных совещаниях, семинарах и конференциях.*

Личность преступника служит объектом криминологического исследования, и многие типологические данные о ней являются элементом криминологической характеристики преступлений.

Обнаруживаемые на месте совершения преступления вещественные улики проливают свет как на сведения о некоторых социально психологических свойствах и качествах личности, так и на сведения о ее преступном опыте, профессии, поле, возрасте и т.п.

С научной точки зрения, существует четкая классификация криминалистически значимой информации, которая подразделяется по следующим основаниям:

1. По источнику получения.
2. По физической природе.
3. По форме представления.
4. По характеру структуры.
5. По структурным элементам события преступления.
6. По направлению движения и назначению, по профессиональному значению.

Криминалистически значимые данные о личности преступника в настоящее время базируются на трех специфических группах преступников.

**Первая группа** включает в себя данные о личности неизвестного преступника по оставленным им следам как на месте преступления, в памяти свидетелей, так и по другим источникам с целью установления направления и приемов его розыска и задержания.

**Вторая группа** преступников включает в себя информацию, полученную с помощью изучения личности задержанного подозреваемого или обвиняемого с целью оценки личности субъекта.

К числу особенностей, указывающих на совершение компьютерного преступления рассматриваемой категории, можно отнести следующие:

1. Отсутствие целеустремленной продуманной подготовки к преступлению.
2. Оригинальность способа совершения преступления.
3. Использование в качестве орудий преступления бытовых технических средств и предметов.
4. Непринятие мер к сокрытию преступления.
5. Совершение озорных действий на месте происшествия.

Близко к рассматриваемой группе преступников можно отнести еще одну, включающую в себя лиц, страдающих новым видом психических заболеваний, информационными болезнями или ***компьютерными фобиями***.

С позиции данной науки, человек рассматривается как универсальная саморегулирующая информационная система с установленным балансом биологической информации. Нарушение последнего под взаимодействием внешних или внутренних дестабилизирующих факторов, как врожденного, так и приобретенного в процессе жизни индивида характера (т.е. инстинктов и рефлексов), приводит к различному роду информационных болезней, среди которых наиболее распространены информационные

нервозы. Иными словами, человек нуждается в равной степени как в физической, так и в информационной энергии (духовной или эмоциональной). Когда ее мало – наступает информационный голод, когда ее много – человек страдает от информационной нагрузки (различного рода стрессов и эмоциональных срывов), приводящих в стечении определенных обстоятельств к ***аффективному*** состоянию. Нарушение одного из этих компонентов информационного процесса приводит к потерям информации субъектом (нарушение памяти человека), преждевременной физической и умственной усталости, в конечном итоге перерастает в ***информационную болезнь***.

По мнению Полевого Н.С., компьютерные преступления, совершаемые преступниками рассматриваемой группы, в основном связаны с преступными действиями, направленными на физическое уничтожение либо повреждение средств компьютерной техники без наличия преступного умысла, с частичной или полной потерей контроля над своими действиями.

**Третью** и последнюю группу составляют профессиональные «компьютерные» преступники с ярко выраженными корыстными целями, так называемые «***асы***». Они характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на сокрытие, и обладающие в связи с этим устойчивыми преступными навыками. В отличие от первой переходной группы «любителей» и второй специфической группы «больных», преступников третьей группы отличает такая особенность, как многократность и сокрытие, навыки, профессионализм. Преступники этой группы обычно являются членами хорошо организованных, мобильных и технически оснащенных высококлассным оборудованием и специальной техникой (нередко оперативно-технического характера) преступных групп и сообществ.

**Наиболее типичными целями являются:**

1. Подделка счетов и платежных ведомостей.
2. Приписка сверхурочных часов работы.
3. Фальсификация платежных документов.
4. Хищение наличных и безналичных денежных средств.
5. Вторичное получение уже произведенных выплат.
6. Перечисление денежных средств на фиктивные счета.
7. Отмывание денег.
8. Легализация преступных доходов.
9. Совершение покупок с фиктивной оплатой.
10. Незаконные валютные операции.
11. Незаконное получение кредитов.
12. Манипуляция с недвижимостью.
13. Получение незаконных льгот и услуг.
14. Продажа конфиденциальной информации.
15. Хищение материальных ценностей, товаров и т. д.

Возраст правонарушителей колеблется от 15 до 45 лет: на момент совершения преступления возраст 33% преступников не превышал 20 лет; 13% - старше 40 лет и 54% - в возрасте от 20 до 40 лет.

Большинство лиц данной категории составляют мужчины - 83%, но доля женщин быстро увеличивается из-за профессиональной ориентации некоторых специальностей и профессий (секретарь, делопроизводитель, бухгалтер, контроллер, кассир и т.д.). Размер ущерба от преступлений, совершенных мужчинами, в четыре раза больше, чем от преступлений, совершенных женщинами.

По уровню образования диапазон также широк – от высококвалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя. 52% - имели специальную подготовку в области автоматизированной обработки информации. 97% - являлись служащими

государственных учреждений и организаций, использующих компьютерную технологию в своих производственных процессах, а 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

Большинство преступников – 77% при совершении преступлений имели средний уровень интеллектуального развития, 21% - выше среднего и только 2% - ниже среднего, при этом 40% преступников имели специальное образование, 40% - высшее и 20% - среднее.

Так, 38% преступников действовали без участников, тогда как 62% - в составе преступных групп.

**Психологические особенности компьютерных преступников**

Для криминологии, социологии и психологии более приемлем генетический подход, позволяющий изучить поведение человека в развитии, как в пространстве, так и во времени. Умные личности, назовем их обобщенно «***хакерами***», в кругу компьютерщиков, крутых взломщиков и вандалов называются «***крекерами***», «***факерами***», а не просто мошенниками в сфере финансовых махинаций, субъективные интересы которых противоречат общественным интересам.

В этой области мало серьезных научных исследований. Все они при совершении преступления добиваются получения доступа к информации, а затем совершают определенные действия.

**Философия искусственного интеллекта**

Хакеры появились задолго до изобретения компьютеров. Первым открытием хакеров было удивительное свойство палки, позволяющее использовать ее одновременно как орудие охоты, обороны и для многих других целей.

До конца 60-х гг. хакеров можно было сопоставить с античными Мастерами. «***Хак***» ассоциировался с высшим профессионализмом и вытекающей из него культурой поведения. Тесная связь культурного и интеллектуального уровней давно отмечалась психологами.

Итак, «хакер» - это искусство взлома всевозможных систем, доведение данного процесса до высот технического изящества. Хакер вооружается различными методиками, исходя из которых он строит собственную стратегию взлома той или иной программы.

Термин «компьютерная преступность» возник в США в начале 70-х годов. В настоящее время под компьютерными преступлениями подразумеваются: неправомерный доступ к компьютерной информации (статья 289 УК КР); создание, использование и распространение вредоносных программ для ЭВМ (статья 290 УК КР); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (статья 291 УК КР); хищение, подделка, уничтожение компьютерной информации и др. Характерной чертой преступлений в сфере компьютерной информации является то, что компьютер может выступать и как предмет преступных посягательств, и как инструмент преступления. Если разделять два последних понятия, то термин компьютерное преступление как юридическая категория имеет двойной смысл. Действительно, если компьютер – только объект посягательства, то квалификация преступления может квалифицироваться существенными нормами уголовного права. Если же только инструмент, то достаточен только такой признак, как «применение технических средств». Впрочем, возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет преступления. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то данное деяние квалифицируется как уголовное преступление. Также если с данным деяниям связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность предусмотрена уголовным кодексом КР.

Уровень разработанности правовых способов регулирования компьютерной

преступности растет с научно-техническим прогрессом в обществе. При этом, среди наиболее эффективных способов, направленных на предупреждение преступлений в сфере компьютерной информации, выделяют технические, организационные и правовые.

К **техническим мерам** можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, принятие специальных конструкционных мер защиты от хищений, саботажа, диверсий, чрезвычайных ситуаций, терроризма, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и т.п.

К **организационным мерам** относится охрана вычислительного центра, тщательный подбор персонала, исключения случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра построенной организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение административной, дисциплинарной и уголовной ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К **правовым мерам** следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы государственного контроля над разработчиками компьютерных программ и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран и др.

На сегодняшний день сформулировано три базовых правовых принципа информационной безопасности, которая должна обеспечивать:

- Целостность данных – защиту от сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных;
- Конфиденциальность – (законность) информации;
- Доступность информации для всех авторизованных зарегистрированных пользователей:
- Защита компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка).

Таким образом, проблема компьютерной преступности составляет важную часть кыргызского уголовного права. Важность проблемы (темы), ее роль на современном этапе глобальной информатизации общества, актуальность темы определяют поставленные цели и задачи настоящего исследования.

**Литература:**


1. Батурин Ю.М. Проблемы компьютерного права. -М.: Юрид. лит. 1991.
2. Пантелеев И.Ф., Селиванов Н.А. Криминалистика. Учебник. -М., 1993.
3. Полевой Н.С. Правовая информатика и кибернетика. -М.: Юрид. лит. 1993.
4. Савельева И.В. Правовая охрана программного обеспечения ЭВМ. -М., МГУ, 1990.
5. Фигурнов В.Э. IBM PC для пользователя. -М.: Фин. и - Стат, 1996.