ПРОБЛЕМЫ ТЕХНИЧЕСКОГО ОБЕСПЕЧЕНИЯ КОМПЛЕКСНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПРАВОВЫЕ, КРИМИНОЛОГИЧЕСКИЕ И КРИМИНАЛИСТИЧЕСКИЕ ПРОБЛЕМЫ ПРЕСТУПНОСТИ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

П.Н. Алпеев, АлтГУ, юридический факультет, 4 к.
Научный руководитель – ***В.В. Поляков,*** к.ю.н., доцент.

Научно-техническая революция XX в. полностью изменила представления человечества об окружающем мире. Процесс внедрения высоких технологий в повседневную жизнь сказывался на качественном изменении отношений в обществе, информация приобретала все большую значимость. Негативным последствием информатизации общества стало появление так называемой компьютерной преступности. Сложность решения вопроса заключается в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк – от преступлений традиционного типа до чисто компьютерных преступлений.

Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров дало возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контроле доступа к информации, ее сохранности и целостности. Проблема защиты информации и информационных систем сейчас является одной из самых актуальных во всем мире.

К разряду компьютерных следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а средством совершения преступлений служит компьютер [1].

Компьютерная информация, особенно в виде баз данных, содержащих различного рода сведения конфиденциального характера, обладает, с одной стороны, высокой стоимостью, а с другой - ее использование лицами, не уполномоченными для этого. В последнее десятилетие картотеки и базы данных многих государственных и иных структур преобразованы в электронную форму. В

силу встречающейся недобросовестности их держателей, а также иных причин, значительное число таких баз данных стало достоянием различных структур, которые занимаются их продажей. Это влечет за собой неконтролируемое использование такой информации. Речь ведется о базах данных ГИБДД, телефонных служб, таможенных органов и т.д. [2]. В последние годы в мире уделяется повышенное внимание проблемам борьбы с распространением детской порнографии в сети Интернет.

Сточки зрения криминологии можно выделить следующие проблемы:

1. устойчивый рост преступности;
2. рост количества преступлений, совершаемых организованными преступными группировками и сообществами, кибертерроризм;
3. качественное изменение в связи со стремительным ростом научно-технического прогресса, применения новейших технологий;
4. высокий уровень латентности;
5. транснациональный характер.

Как следует из интервью Алексея Мошкова, начальника Бюро специальных технических мероприятий, генерал-майора полиции, на протяжении последних 5 лет количественные показатели IT-преступности колебались от 8 тысяч до 17,5 тысяч. За последние 3 года количество обращений граждан непосредственно в Управление «К» МВД России резко увеличилось. Латентность данного вида преступлений остается довольно высокой и по некоторым данным достигает 90 – 95 % [3].

Что касается кибертерроризма, то киберпреступники приняли на вооружение и активно используют тактику «точечных ударов», целенаправленно атакуя определенные компании с целью хищения конфиденциальных данных и финансовой информации.

Страны, где больше всего жертв киберпреступлений среди пользователей: Россия – 85%, Китаи – 77%, Южная Африка – 73%, США – 63%, Канада – 68%, Бразилия – 60%, Мексика – 71%, Объединенное Королевство – 58%, Франция – 45%, Германия – 53%, Италия – 56%, Швеция – 56%, Польша – 60%, Нидерланды – 50%, Австралия – 60%, Индия – 65%, Япония – 19%, Сингапур – 61%, Новая Зеландия – 69%, Турция – 63%, Дания – 50%, Саудовская

Аравия – 62%, ОАЭ – 71%, Колумбия – 64%. Во всех случаях учитывались те, кто оказывался жертвой хотя бы раз в жизни [4].

Несмотря на то, что в последние годы в криминалистической литературе уделяется повышенное внимание методике расследования компьютерных преступлений, в этой области еще остается ряд нерешенных вопросов. Дискуссионными вопросами являются формулировки базовых понятия в области компьютерных преступлений [5].

Следует отметить, что разработка теоретических основ расследования преступлений в сфере компьютерной информации сложна и имеет много аспектов на стыке права, теории информатики, производства и эксплуатации аппаратных средств компьютерных систем, сетей и иного сопряженного оборудования. Однако до сих пор в криминалистике не существует разработанной комплексной методики расследования компьютерных преступлений, отвечающей практическим нуждам их расследования.

В процессе формирования криминалистической методики расследования преступлений в сфере компьютерной информации возникают ряд проблемных вопросов и сложностей, связанных в основном следующими факторами:

1. высокая латентность, достигающая по разным оценкам порядка 90%;
2. сложность сбора доказательств и процесса доказывания в суде ввиду отсутствия достаточной следственной практики;
3. широкий спектр криминалистически значимых признаков этих преступлений;
4. несовпадение места совершения противоправных действий и места наступления общественно опасных последствий [6];
5. механизм совершения скрыт от правоохранительных органов;
6. общественным мнением данный вид преступлений не рассматривается как серьезная угроза;
7. отсутствие четкой программы борьбы с компьютерными преступлениями;
8. сложность раскрытия компьютерных преступлений;
9. отсутствие достаточной следственной практики по расследованию компьютерных преступлений.

Специфика среды, а также способов совершения преступлений в сфере компьютерной информации, привели к тому, что сложившаяся система частных криминалистических теорий оказалась не способной удовлетворить потребности практики борьбы с преступлениями в новой сфере человеческой деятельности. В связи с этим, в последнее время весьма остро встал вопрос о разработке самостоятельной частной криминалистической теории расследования преступлений в сфере компьютерной информации.

В качестве основных проблем, препятствующих успешному решению вопросов выявления и расследования компьютерных преступлений, можно отметить:

1. возможность оперативного сокрытия преступником следов своей преступной деятельности по некоторым видам компьютерных преступлений [7];
2. сложность классификации деструктивных событий, происходящих в компьютерной системе;
3. проблемы организационного характера;
4. проблемы организационно-технического характера;
5. отсутствие единого подхода к описанию имевших место событий;
6. отсутствие действенной методики проведения первоначального этапа расследования по данному виду преступлений; проблемы международных (трансграничных) компьютерных преступлений [8].

В вопросах обеспечения информационной безопасности до сих пор существует широкий спектр проблем, требующих решения. Необходима работа, целью которой является формирование эффективного механизма реализации государственной политики в области обеспечения информационной безопасности в целом и борьбы с преступлениями в сфере компьютерной информации в частности.

Список литературы

1. Батурин Ю.М. Проблемы компьютерного права. – Москва: Юрид лит., 1991. – С. 35.
2. Викторов А.Ю. Секретные материалы оптом и в розницу // Независимая газета. 2008. № 65. С. 7.

3. Чудненко Ю.В. Обзор: ИТ в органах государственной власти 2013 (Алексей Мошков: «Ни одно преступление в сфере ИТ не останется безнаказанным») // CNews: Аналитика. 2014. №187. С. 12.
4. Осипенко К.Ю. Жертвы и последствия киберпреступлений NORTON REPORT 2013 // Information Security/ Информационная безопасность. 2013. №5. С. 25.
5. Поляков В.В. Об использовании новых понятий при доказывании преступлений в сфере компьютерной информации // Российская юридическая наука: состояние, проблемы, перспективы: матер. Всеросс. науч.-практ. конф., посвященной 45-летию юридического образования на Алтае, 19-20 сентября 2008. – Барнаул: Изд-во АлтГУ, 2008. С 427 - 431.
6. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: дис. канд. юрид. наук: 12.00.09. Омск, 2008. 247 с.
7. Поляков В.В. Программное обеспечение, используемое для совершения компьютерных преступлений // Ломоносовские чтения на Алтае–2013: матер. Междунар. молодежной школы-семинара (Барнаул, 5-8 ноября 2013 г.). – Барнаул: Изд-во Алт. ун-та, 2013. Ч. 2 . С. 15-17.
8. Мамедов Н.А. Криминалистические проблемы расследования преступлений в сфере компьютерной информации // Юрист. 2008. №9. С. 32.

АУТЕНТИФИКАЦИЯ КАК СРЕДСТВО ОБЕСПЕЧЕНИИЯ БЕЗОПАСНОСТИ СЕРВЕРОВ НА ОСНОВЕ ClearOS

А.А. Егораев, АлтГТУ, факультет информационных технологий, 4к.
Научный руководитель – ***Е.В. Шарлаев***, к.т.н., доцент.

В условиях современной реальности уже трудно представить какую-нибудь крупную компанию без сосредоточенного информационного управляющего ресурса – сервера, так как с каждым днем человек все более и более стремиться автоматизировать весь процесс своей работы. В офисах появляются множество компьютеров, нормальное функционирование которых без сервера представить сложно – растут вычислительные мощности, объемы