2. Залманзон Л.А. Преобразования Фурье, Уолша, Хаара и их применение в управлении, связи и других областях. / Л.А. Залманзон. – М.: Наука, 1989. – 496 с.
3. Егоров А.В., Поляков В.В., Лаптев А.Ю., Игнатов А.В., Метод обработки сигналов в детекторах обнаружения устройств несанкционированного съема информации // Доклады V Пленума СибРОУМО по образованию в области информационной безопасности и XIII конференции: Томск – Новосибирск, 5–9 июня 2012г. – Томск: В – Спектр, 2012. – с.102-102.
4. Егоров А.В., Парфенова А.В., Применение методов многомерного анализа для интерпретации результатов вихретокового контроля пористых металлических предметов //Известия АлтГУ. – 2011. – №1
5. Поляков В.В., Егоров А.В., Вихретоковой контроль удельной электрической проводимости и магнитной проницаемости изделий из магнитомягких материалов //Дефектоскопия. -1992. – №12

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В СЕТИ ИНТЕРНЕТ КАК СРЕДСТВО ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ПРЕДУПРЕЖДЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

А.С. Мананников, АлтГУ, юридический факультет, 4 к.
Научные руководители – ***В.А. Мазуров,*** к.ю.н., доцент,
В.В. Поляков, к.ю.н., доцент.

XXI век - век информационных технологий, которые динамично развиваются и способствуют улучшению жизнедеятельности общества.

Несмотря на многочисленные преимущества современных компьютерных технологий, они создали новые условия, которые содействуют совершению преступлений на национальном и международном уровнях. [1] Доходы преступников, связанные с незаконным использованием новейших технологий, занимают третье место в мире после доходов от торговли наркотиками и оружием.

В настоящее время усматривается неуклонный рост числа компьютерных преступлений. По данным статистики, за первое

полугодие 2012 года в России было зафиксировано 5696 киберпреступлений, что почти на 11 % больше, чем в аналогичном периоде 2011 года. [2] Стоит отметить, что на сегодняшний день тенденция роста сохраняется.

При этом очевидно, что данная статистика отражает лишь зарегистрированные преступления, но с учетом высокого уровня латентности рассматриваемой категории преступлений, их может быть в разы больше.

По оценкам экспертов, латентность компьютерных преступлений в США достигает 80%, в Великобритании – 85%, в ФРГ – 75%, в России – более 90%. [3]

Отмечается, усиление организованности криминальных структур, использующих возможности Интернета для осуществления преступной деятельности. Такие структуры все чаще применяют методы конспирации, совершенствуют способы сокрытия следов преступлений, пытаются получить доступ к информационным системам правоохранительных органов, спецслужб, органов государственной власти. [4] Тем самым подрывается информационная безопасность государства.

Учитывая неуклонный рост компьютерных преступлений и возможные тяжкие последствия от их совершения, необходимо искать новые пути развития, способные обеспечить более эффективную борьбу с рассматриваемыми общественно-опасными деяниями и лицами, их совершающими.

В этой связи, считаем, что наиболее действенным и первостепенным средством правового обеспечения информационной безопасности и предупреждения компьютерных преступлений является оперативно-розыскная деятельность (далее – ОРД).

Объективная необходимость ОРД изначально предопределена самим существованием преступности, что с неизбежностью подтверждается многовековым историческим и современным опытом развития правоохранительной системы. Ее роль и социальная значимость обусловливается широкими потенциальными возможностями использования результатов в решении различных задач, в том числе и задач уголовного судопроизводства. [5]

В настоящее время Интернет необходимо позиционировать не только как систему телекоммуникаций, допускающую снятие информации с технических каналов связи, но и как место осу-

ществление ОРД. Борьба с преступностью в сети Интернет уже невозможна без применения оперативно-розыскных сил, средств и методов.

Эффективное осуществление оперативно-розыскных мероприятий (далее - ОРМ), в сетевом пространстве невозможно без корректировки методов ОРД. Необходимость модернизации ОРД в данном случае, вызвана уникальностью сетевого пространства, которая заключается в том, что преступления в сети, могут совершаться различными нетипичными способами, в том числе:

1. удаленно (совершение действий, при которых воздействие осуществляется на информационный объект, находящийся на значительном расстоянии или не имеющий физической привязки к конкретному месту); [6]
2. динамически (выполнение действий с помощью мобильных устройств, при перемещении их оператора в физическом пространстве);
3. трансгранично (преступное действие выполняется в одном государстве, общественно-опасные последствия наступают в другом, при этом физического пересечения преступником границ государства не происходит).

При осуществлении определенных ОРМ в сети Интернет (опрос, оперативное внедрение, оперативный эксперимент и др.) для оперативного сотрудника важным является понимание субкультуры хакерского сообщества, включающей взгляды его участников, их привычки, стереотипы поведения, нормы общения. Получение необходимых знаний возможно в процессе наблюдения за местами сетевого общения хакеров, где происходит взаимное согласование мнений, вырабатываются суждения о моральных ценностях, осуществляется обмен криминальным опытом и сведениями о потенциальных жертвах, обсуждаются способы противодействия правоохранительным органам. [7]

На наш взгляд, наблюдение за местами сетевого общения хакеров может осуществляться самим оперативным работником или же путем привлечения к данной деятельности конфидентов. В случае если наблюдение дает положительные результаты, то необходимо незамедлительно брать под контроль выявленные хакерские сайты и форумы для дальнейшего получения ценной оперативной информации (интернет адреса посетителей; характер и сте-

пень их активности; сведения о совершенных или готовящихся преступлениях).

Помимо этого, для обеспечения информационной безопасности и предупреждения преступлений в сфере высоких технологий оперативным сотрудникам надлежит в рамках реализации главы IV ФЗ об ОРД [8] привлекать граждан к содействию ОРД. При этом стоит отметить, что особенности сетевого пространства предполагают специфичные формы привлечения граждан к содействию ОРД. Используя сеть Интернет, граждане могут содействовать ОРД путем заполнения на специализированных сайтах форм сообщений о совершенных или готовящихся преступлениях, о потенциальных преступниках, их связях и т.п. (аналог телефона доверия).

Вместе с тем, считаем, что повысить эффективность ОРД в рассматриваемом направлении может проведение опроса в электронной форме.

Из тактических соображений предпочтение стоит отдавать легендированной форме опроса, при которой оперативный сотрудник скрывает свои истинные цели и профессиональную принадлежность. При осуществлении указанных ОРМ возможно выявление лиц, готовых оказывать содействие оперативно-розыскным органам (далее – ОРО) на конфиденциальной основе. При наличии признаков достаточной осведомленности таких лиц важным становится укрепление доверительных отношений с ними и выход на непосредственное общение. Привлечение граждан к содействию ОРО позволяет не только получать достоверную информацию о состоянии оперативной обстановки на контролируемых сетевых объектах, но и изучать способы совершения и сокрытия следов сетевых компьютерных преступлений, ранее не встречавшихся в оперативно-розыскной практике. [9]

Вместе с тем, в ОРД в области расследования компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и группового преступного поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного по-

ведения определенных криминогенных контингентов. Именно прошлое (судимость, правонарушения, антиобщественные поступки, большие успехи в области программирования), настоящее (поддержание криминальных связей, склонность к антиобщественным занятиям) дают основания для прогностических выводов о вероятном противоправном поведении в будущем. Принимаются во внимание социальные оценки, даваемые лицу, представляющему оперативный интерес, роль для него мнения представителей криминогенной и преступной среды. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм ОРД (поиске, профилактике, разработке). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные информационные технологии и программные средства.

Резюмируя, стоит отметить, что на наш взгляд реализация предложенных рекомендаций и мер поспособствует развитию информационной безопасности и в должной мере будет осуществлена как общая, так и частная превенция компьютерных преступлений.

Список литературы

1. Поляков, В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114 - 116.
2. 30 сентября – День Интернета в России [Электронный ресурс] // Официальный сайт Министерства внутренних дел Российской Федерации. – Режим доступа: http://mvd.ru/news/item/146788/. – Загл. с экрана.
3. Мазуров В.А. Преступность в сфере высоких технологий: Понятие, общая характеристика, тенденции // Вестник Томского государственного университета. 2007. № 300-1. С. 153.
4. Поляков, В.В. Анализ высокотехнологичных способов неправомерного удаленного доступа к компьютерной информации / В.В. Поляков, С.М. Слободян // Известия Томского политехнического университета. – 2007. – Т. 310, № 1. – С. 212 – 216.

5. Маркушин А.Г. Оперативно-розыскная деятельность. Москва: Изд-во Юрайт, 2013. С. 13-14.
6. Поляков, В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.09 / В.В. Поляков. – Омск, 2008. – 28 с.
7. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. Москва: Изд-во ИНФРА-М, 2014. С. 328.
8. Федеральный закон от 12.08.1995 N 144-ФЗ (ред. от 21.12.2013) Об оперативно-розыскной деятельности // Собрание законодательства РФ. 14.08.1995. N 33. ст. 3349.
9. Горянинов К.К., Овчинский В.С., Синилов Г.К. Теория оперативно-розыскной деятельности. Москва: Изд-во ИНФРА-М, 2014. С. 335.

ГЕНЕРАЦИЯ ПАКЕТОВ С ПРОИЗВОЛЬНЫМ СОДЕРЖИМЫМ

К.Ю. Манзюк, АлтГУ, физико-технический факультет, 3 к.
Научный руководитель – ***А.В. Мансуров,*** к.т.н., доцент.

Задача генерации кадров/пакетов сетевого обмена с произвольным содержимым является достаточно актуальной как для вопросов исследования механизмов безопасности сетевого обмена и безопасности сетевых сервисов, так и для практического изучения принципов безопасной работы сетевых сервисов в условиях учебной лаборатории ФТФ. Данное исследование предполагает изучение принципов формирования сетевых кадров/пакетов с произвольной нагрузкой и последующую разработку приложения, специализированного на учебном лабораторном применении при выполнении лабораторных работ в учебной лаборатории безопасности информационных сетей.

Существующие программные средства генерации пакетов с произвольным содержимым являются либо излишне сложными, либо, наоборот, слишком простыми и непригодными для простого решения возникающих задач. Немаловажный аспект — это простой интерфейс, возможность модификации заголовков протоко-