5. См.: Хомич, В.М. Преступность, связанная с наркотиками (результаты комплексного анализа) / В.М. Хомич, А.В. Солтанович, О.В. Русецкий / Науч.-практ. центр проблем укрепления законности и правопорядка Генер. прокуратуры Респ. Беларусь. – Минск: БГКФК, 2010.

6. Количество заключенных по странам мира [Электронныйресурс]. – Режим доступа: https:// prisonstudies. org / highest - to – lowest / prison_population_rate? field_region_ taxonomy_tid=All.- Дата доступа: 20.09.2018.

УДК 343.98:347.77/78:004

ОРГАНИЗАЦИЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ВЫСОКИХ ТЕХНОЛОГИЙ

В.В. Хилькевич
ВГУ имени П.М. Машерова

Быстрое развитие высоких технологий, как во всем мире, так и в Республике Беларусь, внедрение технических возможностей разрабатываемых информационно-телекоммуникационных систем во все сферы деятельности современного общества и нынешнее состояние систем защиты и «взлома» информации создало в последние годы объективные предпосылки возникновения нового вида преступлений – преступлений в сфере телекоммуникационной и компьютерной информации. Распространение преступлений в сфере высоких технологий неизбежно приводит сотрудников правоохранительных органов к необходимости детального изучения технических возможностей существующих компьютерных систем, их применения и использования в борьбе с преступлениями в данной сфере деятельности.

Глобализация общественных процессов развития привела и к последующей глобализации коммуникационных систем. Следствием технического и информационного прогресса является глобальная мировая сеть Интернет. Однако необходимо признать, что Интернет находится в настоящее время в какой-то мере вне законодательного регулирования и контроля государственных органов, что порождает различные правонарушения и преступления под действием факторов, которые существенно влияют на криминогенную обстановку, сложившуюся вокруг Интернета [1, с. 3].

1. Возможность мошенничества при заключении сделок через Интернет, возможность хищения из виртуальных магазинов, а также создания виртуальных финансовых пирамид.

2. Возможность совершения сделок и операций, скрытых от налоговых органов.

3. Возможность нарушения авторских и патентных прав, а также использования различных информационных баз правоохранительных и контролирующих органов.

4. Возможность совершения преступлений в сфере компьютерной информации.

Наиболее часто используются следующие способы подготовки, совершения и сокрытия преступления в сфере компьютерной информации: хищение (изъятие) машинных носителей информации, в т.ч. путем их подмены; копирование конфиденциальной компьютерной информации; создание вредоносных программ для ЭВМ; распространение вредоносных программ; распространение машинных носителей, содержащих вредоносные программы для ЭВМ; внесение изменений в существующие программы; фальсификация входных и/или выходных электронных документов; изготовление дубликатов документов и их носителей; использование недостатков программ для ЭВМ; дезактивация либо обход защиты компьютерной информации и СВТ от несанкционированного доступа (путем подбора пароля, кода доступа и др.); перехват компьютерной информации из канала электросвязи; блокирование, модификация, копирование, уничтожение, повреждение компьютерной информации с использованием специально приспособленных, разработанных, запрограммированных технических средств негласного получения информации.

При выявлении и расследовании преступлений в сфере компьютерной информации подлежат установлению: факт совершения преступления; непосредственная причина нарушения безопасности компьютерной информации и орудий ее обработки; предмет преступного посягательства; категория компьютерной информации (общего пользования или конфиденциальная); место и время совершения преступления; способ совершения преступления; совершено ли преступление дистанционно извне помещения (по каналам электросвязи и локальной сети ЭВМ); личность подозреваемого и основные ее характеристики (обладает ли специальными познаниями, в какой области и каков их уровень); не совершено ли преступление группой лиц, каковы роль и характер каждого участника преступления; мотив преступления; кто является потерпевшим (физическое или юридическое лицо); кому было известно о намерениях преступников, кто участвовал в сокрытии преступления и его следов; причины и условия, способствовавшие совершению и сокрытию преступления, что усугубило их проявление – не обусловлено ли это нарушениями нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам [2, с. 14].

Раскрывать преступления в сфере компьютерной информации, сложно, так как нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место (например, сбой в работе ЭВМ и программного обеспечения, средств электросвязи).

Перечень неотложных следственных действий и оперативных мероприятий, очередность их проведения будут определяться конкретной следственной ситуацией, в которой начинается расследование. Следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного работника.

Поводами и основаниями для возбуждения уголовных дел чаще всего служат: заявления граждан (конкретных потерпевших); сообщения руководителей предприятий, учреждений, организаций и должностных лиц (базирующиеся, как правило, на материалах контрольно - ревизионных проверок и сообщениях служб безопасности); сведения, полученные в результате проведения оперативно-розыскных мероприятий; непосредственное обнаружение признаков преступления.

Как правило, возбуждению уголовного дела предшествует предварительная проверка материалов, поступивших в правоохранительные органы. В связи с этим, следователь может заблаговременно ознакомиться с собранными по делу материалами, совместно с оперативным сотрудником выбрать в тактическом отношении наиболее оптимальный момент для возбуждения дела, а также определить характер и последовательность первоначальных следственных действий, организационных и иных мероприятий. Успех расследования преступления в сфере компьютерной информации во многом обеспечивают: быстрота и решительность действий следователя и оперативного сотрудника в самые первые часы производства по делу; организованное взаимодействие с различными подразделениями правоохранительных органов; наличие специалиста в области компьютерной обработки информации.

В ходе предварительной проверки материалов при решении вопроса о возбуждении уголовного дела следователь должен прежде всего получить четкое и полное представление о предмете посягательства, месте его нахождения и условиях охраны [3, с. 485].

Чтобы детально разобраться в особенностях деятельности потерпевшего, следователю и оперативному сотруднику необходимо ознакомиться с соответствующей справочной литературой, изучить ведомственные нормативные акты, важное значение имеют консультации со специалистами. Для преступлений в сфере компьютерной информации типичны три ситуации первоначального этапа расследования:

1. Сведения о причинах возникновения общественно опасных деяний, способе их совершения и личности преступника отсутствуют.

2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

Таким образом, можно сделать вывод, что внедрение современных информационных технологий и развитие телекоммуникаций создают определенные благоприятные возможности для лиц, вынашивающих противозаконные намерения, которые могут использовать вычислительные сети как средство для реализации своих замыслов.

Интернет все более активно используется преступными группировками для незаконного проникновения в корпоративные и личные базы данных. Результатом развития Интернет является возникновение не только нелегального рынка, где сбывается информация, но и пособий по приготовлению к совершению преступлений, рекомендации относительно того, как уйти от уголовного преследования и т.п.

Учитывая всеобъемлющий характер Интернет и его востребованность, можно говорить о реальной возможности задействовать Интернет в противодействии преступности.

Но, к большому сожалению, у нас в стране существуют проблемы с расследованиями преступлений, совершенных в сети Internet.

Во-первых – это нехватка специалистов в правоохранительных органах, имеющих достаточную квалификацию, во-вторых – высокая латентность данного рода преступлений.

И хочется надеяться на то, что работники правоохранительных органов будут чаще и теснее сотрудничать со специалистами данной сферы. Повышение уровня знаний в нашем современном обществе является непосредственной необходимостью. И все идет к тому, что в ближайшем будущем процент компьютерных преступлений по отношению ко всем преступлениям достигнет достаточно высокой планки.

Список источников

1. Вехов В.Б. Особенности организации и тактика осмотра места происшествия при расследовании преступлений в сфере компьютерной информации // Российский следователь. – 2004. – № 7. – С. 2 – 5.

2. Илюшин Д.А. Особенности тактики производства обыска при расследовании преступлений в сфере предоставления услуг "Интернет" / Д.А. Илюшин // Законность. – 1999. – № 3. – С. 12 – 15.

3. Криминалистика. Учебник. 2-е изд., перераб. и доп. / под ред. В.А. Образцова. – М.: Юрист, 2002. – 735 с.

УДК 341.211

РОЛЬ И ЗНАЧЕНИЕ ГОСУДАРСТВЕННОГО СУВЕРЕНИТЕТА В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ

А.В. Шавцова
Белорусский государственный университет

В конце XX – начале XXI в. в области изучения проблем суверенитета появились новые аспекты, возникшие в контексте обсуждения вопросов глобализации и нового мирового порядка. Все активнее стала обсуждаться тема изменения, «размывания» понятия суверенитета.

Общеизвестно, что суверенитет – неотъемлемое качество государства как субъекта международного права и международных отношений. Благодаря суверенитету государства равны друг другу в правовом отношении, независимо от размеров территории, численности населения, экономического и культурного развития, военной мощи. Это принцип суверенного равенства.

В международном праве суверенитет государства определяется как «полнота законодательной, исполнительной и судебной власти государства на его территории, исключающая всякую иностранную власть на его территории, а также неподчинение государства властям иностранных госу-