Данная работа будет полезна для всех сотрудников, работающих в сфере обеспечения информационной безопасности. Плюс системы рекомендаций – это возможность потенциального заказчика оценить примерную стоимость и возможные конфигурации защиты непосредственно перед работой либо заказом. Данная система рекомендаций будет расширена на другие технические каналы утечки информации.

Список литературы.

1. Торокин А.А. Инженерно-техническая защита информации. – М.: Изд-во Гелиос АРВ, 2005. – 960 с.
2. Халяпин Б.Д. Защита информации. Вас подслушивают? Защищайтесь! – М.: Изд-во Москва «БОЯРД», 2004. – 432 с.
3. Железняк В.К., Макаров Ю.К., Хорев А.А. Некоторые методические подходы к оценке эффективности защиты речевой информации // Специальная техника. – М.: 2000. - №4.
4. Хорев А.А., Макаров Ю.К. К оценке эффективности защиты акустической (речевой) информации // Специальная техника. – М.: 2000. - №5.

СИТУАЦИИ РАССЛЕДОВАНИЯ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

С.В. Казанцев, АлтГУ, юридический факультет, 5 к.
В.В. Поляков, к.ю.н., доцент.

На первоначальном этапе расследования компьютерных преступлений следователь действует в условиях недостаточной исходной информации по делу. Имеющиеся признаки преступления, как правило, могут быть истолкованы неоднозначно [1]. В таких условиях находит свое применение положение, высказанное В.Е. Корноуховым, согласно которому «для решения той или иной задачи должны разрабатываться и отражаться в методике несколько комплексов следственных действий и оперативно-розыскных мероприятий, которые были бы адаптивны к разным условиям расследования преступлений [2]. В криминалистике эффективно практикуется ситуационный подход в расследовании сложных преступлений [3]. Полагаем, что следственная ситуация - это та

обстановка, которая создается при расследовании преступления и объективно отражает «внутреннее состояние, ход и условия расследования на основе совокупности фактических и иных данных» [4]. Базовым компонентом следственных ситуаций является типичная следственная ситуация, которая требует своих тактико-технических приемов разрешения. Она характеризуется устойчивым комплексом признаков, включающих в себя «общие черты хода и состояния расследования к определенному его моменту» [5], отражающих общие черты криминалистической характеристики данного вида преступлений и наиболее вероятную обстановку их расследования.

На основе совокупности криминалистически значимых данных, характерных для соответствующих ситуаций, можно выдвигать следственные типовые версии [6]:

1. заявление о неправомерном удаленном доступе к компьютерной информации подтверждается, преступление действительно имеет место;
2. заявитель ошибается или заблуждается, неправомерного удаленного доступа к компьютерной информации не произошло;
3. имеет место ложное заявление о неправомерном удаленном доступе к компьютерной информации.
4. Более значимым в практическом плане представляется подразделение следственных ситуаций на следующие группы:
5. конфликтные ситуации, при которых «субъект преступления обладает информацией, но умышленно искажает или скрывает ее» [7];
6. бесконфликтные ситуации, при которых субъект преступления объективно передает следователю искомую информацию, не стремится ее искажать или утаивать;
7. слабоконфликтные ситуации, которые возникают в ситуациях допроса, когда допрашиваемый «обладает искомой информацией, желает ее передать, но в силу субъективных или объективных факторов воспринял, запомнил и, соответственно, передает ее с искажениями» [8].

Особое роль для построения эффективной методики предварительного расследования имеет выделение следственных эта-

пов, объединяющих проверочные и следственные действия в соответствии с имеющей место следственной ситуацией. Можно выделять этап предварительной проверки полученных сведений о преступлении, а также первоначального, неотложного, дальнейшего и заключительного этапов расследования.

С позиций ситуационного подхода первоначальный этап расследования преступлений в сфере компьютерной информации может быть охарактеризован тремя типичными следственными ситуациями, классифицируемыми по субъекту выявления преступления [9].

1. Собственник компьютерной информации обнаружил факт преступления и самостоятельно выявил преступника.
2. Собственник компьютерной информации обнаружил факт преступления, но преступник остается не выявленным.
3. Преступление выявлено правоохранительными органами.

В случае неправомерного удаленного доступа к компьютерной информации эта классификация представляется неполной и должна быть дополнена, по нашему мнению, еще одной типичной следственной ситуацией.

4. Преступление выявлено иным лицом, в качестве которого обычно выступает организация – провайдер, обслуживающая собственника конфиденциальной информации.

Типичная доследственная ситуация на предварительном этапе в случае совершения преступления способом относительно простого удаленного доступа к компьютерной информации характеризуется тем, что потерпевшие (физические или юридические лица) сами обнаруживали преступление.

Изучение приведенных и других ситуаций, возникающих по делам о неправомерном удаленном доступе к компьютерной информации на предварительном следствии является основанием для выбора и использования нужной группы криминалистических рекомендаций [10]. Знание этих рекомендаций способно в значительной степени способствовать эффективному сбору доказательств по преступлениям, связанным с неправомерным доступом к компьютерной информации, совершенным дистанционным образом.

Список литературы

1. Гавло В.К., Поляков В.В. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации // Известия Алтайского государственного университета. 2006. №2. С. 44-48.
2. Корноухов В.Е. Адаптация типовой методики к условиям расследования конкретного преступления // Уголовно-процессуальные и криминалистические чтения на Алтае: матер. Межрегион. науч.-практ. конф.; под ред. В.К. Гавло. - Барнаул: Изд-во Алт. ун-та, 2003. Вып. 7-8. С. 172-178.
3. Гавло В.К., Поляков В.В. Ситуационный подход в криминалистике по делам о компьютерных преступлениях // Научно-методические и нормативные материалы и документы IV Пленума СибРОУМО по образованию в области информационной безопасности: матер. Пленума и документы конференции: сб. статей: Томск – Барнаул – Белокуриха, 8-13 июня 2010 г. Томск: «В-Спектр», 2010. С. 186 - 187.
4. Гавло В.К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск: Изд-во Томского ун-та, 1985. – 333 с.
5. Драпкин Л.Я. Проблемы общей теории раскрытия преступлений и криминалистическая тактика // Криминалистические проблемы следственной тактики: межвуз. сб. науч. трудов. - Свердловск: Изд-во УрГУ, 1981. С. 34.
6. Поляков В.В. Особенности расследования неправомерного удаленного доступа к компьютерной информации: автореф. дис. канд. юрид. наук: 12.00.09. Омск, 2008. 28 с.
7. Баев О.Я. Конфликтные ситуации на предварительном следствии (основы предупреждения и разрешения). - Воронеж: Изд-во ВГУ, 1984. 132 с.
8. Комиссаров В.И., Лакаева О.А. Тактика допроса потерпевших от преступлений, совершаемых организованными группами лиц. – М.: Изд-во «Юрлитинформ», 2004. 160 с.
9. Курс криминалистики: в 3 т. Т. III. Криминалистическая методика: Методика расследования преступлений в сфере экономики, взяточничества и компьютерных преступлений / под ред. О.Н. Коршуновой, А.А. Степанова. – СПб. Изд-во «Юридический центр Пресс», 2004. – 573 с.

10. Поляков В.В. Следственные ситуации по делам о неправомерном удаленном доступе к компьютерной информации // Доклады Томского государственного университета. 2010. N1(21). С. 46 - 50.

КИБЕРТЕРРОРИЗМ: МЕРЫ ПРОТИВОДЕЙСТВИЯ В АСПЕКТЕ МЕЖДУНАРОДНОГО СОТРУДНИЧЕСТВА РОССИИ И СТРАН ЗАРУБЕЖЬЯ

М.Н. Кутявина, Т.И. Рыбина, АлтГУ,
юридический факультет, 4 к.
Научный руководитель – ***В.А. Мазуров,*** к.ю.н., доцент.

Сегодня интернет широко используется не только обычными гражданами, но различными террористическими и экстремистскими организациями и играет большую роль в их деятельности, которая не ограничивается лишь пропагандистской и разъяснительной работой, публикацией материалов определенной направленности и др.

Посредством интернет-ресурсов осуществляется привлечение к подобной деятельности «волонтеров», вербовка новых членов, сбор финансовых средств, планирование и координация совместных действий.

Не вызывает сомнения, что компьютерные преступления во всем мире имеют устойчивую тенденцию к росту, поскольку растет и аудитория пользователей высокими технологиями и Интернет-ресурсами. Ключевым положением борьбы с кибертерроризмом является интеграция правовых систем различных стран (например, сближение уголовного законодательства стран Евросоюза). На первый план, по сравнению с национальным законодательством, выходят инструменты межгосударственного (международного) регулирования, поскольку данная проблема не носит, как правило, каких-либо географических или политических границ.

При этом речь идет не столько о включении международных актов в национальное законодательство путем их ратификации, сколько о добровольном и рациональном учете рекомендаций международных (межправительственных) организаций (ЕС, ООН,