Правовое регулирование

в сети «Интернет»

Материалы выступлений на заседании рабочей группы №1
российско-германского семинара в рамках недели Германии
в Санкт-Петербурге 1 марта 2012 года,
Васильевский Остров, 1-я линия, д. 26

Санкт-Петербург

2012

УДК 004.738.52

ББК 76.0

Правовое регулирование в сети «Интернет»: Материалы выступлений (на русском и немецком языках) на заседании рабочей группы №1 российско-германского семинара в рамках недели Германии в Санкт-Петербурге 1 марта 2012 года, Васильевский Остров, 1-я линия, д. 26 / Сост. и перевод А.А. Кабанов, А.А-к Казымова; Под общ. ред. А.А. Кабанова. – СПб., б.и., 2012 – 53 с.

Кабанов А.А.
Россия, Санкт-Петербург,
Санкт-Петербургский университет управления и экономики

ОРГАНИЗАЦИОННЫЕ МЕТОДЫ ПРОФИЛАКТИКИ НЕКОТОРЫХ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

В случае если кошелёк оставлен на скамейке в парке, пропажа кошелька не называется его кражей. Интеллектуальная собственность, оставленная без присмотра, также может пропасть, или быть повреждённой. При этом собственник или пользователь, будучи сам виноват в её копировании или повреждении, порой считает, что в отношении него совершено преступление. Профилактика компьютерных преступлений – дело рук собственников и пользователей информации, представляющей так называемую интеллектуальную собственность.

Вопросы профилактики компьютерных преступлений достаточно активно обсуждаются Интернет-сообществом[1]. Однако ряд статей устарел[2], а некоторые из проблем в них даже не обсуждаются.

Здесь предлагаются некоторые мало распространённые рекомендации по организационным методам профилактики компьютерных преступлений. Прежде всего, следует перечислить виды преступлений согласно действующей редакции Уголовного кодекса Российской федерации. В 28 главе «Преступления в сфере компьютерной информации» имеется 3 статьи: 272. Неправомерный доступ к компьютерной информации; 273. Создание, использование и распространение вредоносных программ для ЭВМ; и 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. Рассмотрим организационные методы профилактики неправомерного доступа к компьютерной информации.

Как говорится: «Спасение утопающих – дело рук самих утопающих».

Во-первых. Для профилактики неправомерного доступа к компьютерной информации предлагается хранить ценную и конфиденциальную информацию на съёмных носителях – внешних винчестерах большой ёмкости.

---

[1] См., напр.: http://www.lib.ua-ru.net/diss/cont/124687.html; http://sesia5.ru/blok/10/a5_1.htm; http://ru.wikipedia.org/wiki; http://www.fssr.ru/hz.php?name=News&file=article&sid=281; http://www.crime-research.ru/articles/Xomkolov; http://www.securitylab.ru/contest/382194.php; http://www.crime-research.ru/news/06.11.2004/1591; http://ndki.narod.ru/links/Scientists.html и др.

[2] Напр., http://www.comp-bezopasnost.spb.ru/3.html.

Во-вторых. В компьютере, через который осуществляется взаимодействие с другими компьютерами посредством глобальных сетей, желательно, чтобы вовсе не было такой информации.

В-третьих. Временные носители информации (флэшки), используемые для записи или чтения информации на чужих компьютерах, должны быть по возможности либо пустыми, либо содержать только ту информацию, которую предлагается прочесть на чужом компьютере. Это позволит быстрее проверять их на отсутствие вредоносных программ и легче выявить такие программы простым просмотром.

В-четвёртых. Обычно вирусы имеют свойство скрытости своего имени в каталоге. Поэтому каталоги рекомендуется настраивать так, чтобы видеть «скрытые» файлы. При этом они имеют иную, чем обычные файлы яркость и бросаются в глаза.

В-пятых. Все незнакомые файлы на флэшках лучше сразу удалять. В случае если они не удаляются, надо заново форматировать внешний носитель. При этом удобно форматировать в файловой системе NTFS. Тогда появляется возможность запрета записи в корневой каталог, куда вредоносные программы обычно пытаются записать свой autoexec.inf, а также другие ограничения.

Кроме того, желательно работать в режиме пользователя, а не администратора и использовать оплачиваемый (а не бесплатный) антивирус. Бесплатным бывает только сыр в мышеловке.

Kabanov A.
Russland, St. Petersburg,
St. Petersburger Universität für Management und Ökonomie

Organisatorischen Methoden der Prophylaxe von einigen Computerstraftaten

Wenn die Geldbörse auf der Bank in dem Park gelassen ist, gilt der Verlust als ein Diebstahl nicht. Unbeaufsichtigt gelassenes geistiges Eigentum kann auch verschwinden oder beschädigt werden. Dabei der Eigentümer oder der Benutzer, der selbst schuldig für das Kopieren oder die Schädigung eines Eigentums ist, glaubt manchmal, dass ein Verbrechen gegen ihn begangen ist. Eigentümern und Benutzer der Information, die als ein so genannten geistigen Eigentum gilt, haben selbst die Prophylaxe von Computerstraftaten zu führen.

Die Verhütung von Computerverbrechen diskutiert man recht aktiv bei Internet-Community[3]. Aber einige Reihe von Artikeln ist veraltet[4], und einige der Probleme aus denen werden nicht behandelt.

Hier stellt man einige nicht gut verbreitete Empfehlungen zur organisatorischen Methoden von der Verhütung der Computerkriminalität auf. Vor allem muss man laut dem Strafgesetzbuch der Russischen Föderation Arten von Straftaten nennen. Im Kapitel 28, «Verbrechen aus Bereich Computerinformation» gibt es 3 Artikel: 272. Illegalen Computerinformationenzugang; 273. Schaffung, und. Verwendung und Verbreitung der bösartigen Programmen für Computer; und 274. Regelnverletztung der Durchführung von Computer und des Computersystems oder seines Netz. Blicken wir die organisatorische Methoden der Verhütung illegalen Computerinformationenzugang.

Es gibt eine Sprichwort: «Die Rettung des Ertrinkenden in den Händen des Ertrinkenden liegt».

Erstens. Für die Verhütung illegalen Computerinformationenzugang ist ratsam wertvolle und konfidentielle Information auf Wecheldatenträger – Äußerfestplattenaufwerk zu bewahren.

Zweitens. Im Computer, durch denen mit anderen Computern eine Wechelwirkung über globale Netzwerke passiert, ist es wünschenswert solche Information dort nicht lassen.

Drittens. Temporäre Wecheldatenträger (USB-Sticke), die für Aufnahme und Lesen der Information aus fremdem Computer verwendet ist, sollte (wie es möglich ist) entweder leer sein oder nur solche Information enthalten, die auf einem anderen Computer zu lesen ist. Dadurch schneller Scan für Malware fehlen und es ist einfacher, solche Programme einfach anzeigen zu identifizieren. Das hilft schneller sie zu prüfen, ob sie bösartige Programmen haben, und leichter solche Programmen mit einfachem Durchsicht aufzudecken.

Viertens. Gewöhnlich haben Virusen eine Eigenschaft der Heimlichkeit seines Namen im Verzeichnis Daher wird empfohlen, die Kataloge in solchem Weise konfigurieren, um «versteckte» Dateien zu finden. Dabei sie weichen aus den normalen Dateien ab und haben eine besondere scheinbare Helligkeit.

---

[3] Siehe z.B.: http://www.lib.ua-ru.net/diss/cont/124687.html; http://sesia5.ru/blok/10/a5_1.htm; http://ru.wikipedia.org/wiki; http://www.fssr.ru/hz.php?name=News&file=article&sid=281; http://www.crime-research.ru/articles/Xomkolov; http://www. securitylab.ru/contest/382194.php; http://www.crime-research.ru/news/06.11.2004/1591; http://ndki.narod.ru/links/Scientists.html und andere.

[4] Siehe z.B.: http://www.comp-bezopasnost.spb.ru/3.html.

Fünftens. Es ist besser alle unbekannten Dateien auf USB-Stick sofort wegzumachen. Wenn sie nicht wegmachen werden, muss man den Äußerwecheldatenträger formatieren. Dabei ist es bequemer dies im NTFS-Dateisystem machen. Dann erscheint die Möglichkeit für die Einträge im Root-Verzeichnis wo die Malware in der Regel versuchen, ihre autoexec.inf sowie andere Einschränkungen zu verbieten.

Außerdem ist es wünschenswert, im Benutzer-Modus (nicht Administrator) arbeiten und bezahltes Antivirus verwenden (aber nicht kostenlos). Nur der Käse in der Mausfalle ist umsonst.

Жаркой М.Э.
Россия, Санкт-Петербург,
Санкт-Петербургский университет управления и экономики

ПРАВОВАЯ ПРИРОДА ОТНОШЕНИЙ ПРАВООХРАНИТЕЛЬНЫХ ОРГАНОВ СО СРЕДСТВАМИ МАССОВОЙ ИНФОРМАЦИИ (ТЕОРЕТИКО-ПРАВОВОЙ АСПЕКТ)

Специфические отношения, сложившиеся между средствами массовой информации (СМИ) и подразделениями информационного сопровождения (пресс-службами, центрами связи с общественностью, официальными представительствами и т.п.) правоохранительных органов в сфере информационного обеспечения политики борьбы с преступностью и охраны общественного порядка Российского государства, имеют свои особенности, обуславливающие их природу. Не подлежит сомнению, что эти отношения, являясь разновидностью отношений общественных, имеют не только свойственные им черты, но и подлежат именно в силу своей специфики определённой социальной регуляции. При этом, исходя из природы участников рассматриваемых отношений (с одной стороны – государственные органы или учреждения, с другой – представители «третьего сектора»), можно утверждать, что особым, официальным, государственным регулятором этих отношений выступает право. Именно с помощью нормативного воздействия государственная власть переводит эти отношения под свою юрисдикцию и таким образом придаёт им стабильность, упорядоченность и желаемую направленность. Следовательно, указанный вид общественных отношений можно в самом общем смысле определить как отношения, урегулированные правом, т.е. правовые.

Тем не менее, указанная разновидность правоотношений относится к группе частично регулируемых, ибо следует иметь в виду, что не любое отношение может быть подвергнуто правовому регулирова-

нию, во многих случаях необходимость в этом просто не возникает. Наиболее характерными признаками рассматриваемых правоотношений является то, что:

а) они возникают и прекращаются только на основе юридических норм, содержащихся в Конституции России и развитых в соответствующем федеральном законодательстве: в Законах РФ «О средствах массовой информации», «Об авторском праве и смежных правах», «Об учреждениях и органах, исполняющих уголовные наказания в виде лишения свободы», Федеральных законах «О содержании под стражей подозреваемых и обвиняемых в совершении преступлений», «Об информации, информатизации и защите информации», «О Прокуратуре РФ», «О полиции», «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации», Уголовном кодексе РФ, Уголовно-исполнительном кодексе РФ и Уголовно-процессуальном кодексе России, а также других нормативных правовых актах. Как видно, регулятивную функцию права в данном случае осуществляют как материальные, так и процессуальные юридические нормы;

б) субъекты этих отношений связаны между собой субъективными правами и обязанностями, которые собственно и образуют юридическое содержание правоотношения. В его рамках праву одной стороны соответствует обязанность другой и наоборот. В данном случае, субъекты правоотношения выступают по отношению друг к другу как управомоченные и правообязанные лица, в результате чего интересы одной стороны могут быть реализованы только посредством другой. Участниками этих правоотношений являются субъекты права, под которыми в данном случае понимаются люди (представители СМИ, сотрудники правоохранительных органов) и их объединения (информационные агентства, редакции СМИ, подразделения информационного обеспечения правоохранительных структур, а также должностные лица обеих сторон), выступающие в качестве носителей предусмотренных законом прав и обязанностей;

в) рассматриваемые отношения имеют волевой характер, т.к. они не могут появиться и функционировать без волеизъявления их участников или хотя бы одного из них;

г) как и другие виды правоотношений, изучаемая группа отличается строгой определённостью взаимного поведения субъектов, их индивидуализированностью и персонификацией прав и обязанностей. И, наконец, эти отношения охраняются государством, т.е. в случае неисполнения или ненадлежащего исполнения правовых предписаний,

возможно применение мер государственного принуждения, ибо охрана законности и правопорядка означает и охрану правоотношений. Таковы основные особенности данного вида правоотношений.

В тоже время следует иметь в виду особенности взаимоотношений представителей СМИ с различными правоохранительными органами, специфику информационной политики представителей последних, опосредованную теми задачами, которые поставлены перед ними законодателем (например, прокуратуры, следственного комитета, органов предварительного следствия и дознания, подразделений, наделённых правом проведения оперативно-розыскной деятельности и т.д.).

Рассмотрим, в частности, наиболее типичные ситуации, возникающие в процессе информационного обеспечения деятельности уголовно-исполнительной системы федеральной службы исполнения наказаний (ФСИН) Минюста России, учреждения и органы которой и по сей день справедливо относятся к наиболее закрытым от общества элементам государственного механизма. Здесь в содержании правоотношений можно обозначить как минимум пять аспектов:

1) Порядок посещения учреждений и органов, исполняющих наказания чётко регламентирован чч. 2,3,4 ст.24 Уголовно-исполнительного кодекса (УИК) РФ – представители СМИ и иные лица имеют право посещать учреждения и органы по специальному разрешению администрации этих учреждений и органов, либо вышестоящих органов (УФСИН). При этом под представителями СМИ понимаются журналисты радио, телевидения, периодических печатных изданий, других масс-медиа, имеющие соответствующие лицензии и поручения руководителей СМИ и изданий. В соответствии со ст.ст. 39,40 Закона РФ «О средствах массовой информации», редакция издания оформляет запрос информации и направляет его в УФСИН (управомочивает). В результате последний приобретает обязанность уведомить редакцию: а) в трёхдневный срок со дня письменного запроса об отказе и причинах, по которым запрашиваемая информация не может быть предоставлена; б) в тот же срок об отсрочке в предоставлении информации, если требуемые сведения не могут быть представлены в семидневный срок; в) руководители УФСИН посредством пресс-службы, либо другие уполномоченные ими лица в пределах своей компетенции предоставляют информацию.

2) Свои особенности имеет посещение представителями СМИ следственных изоляторов (СИЗО). В них содержатся в основном подозреваемые и обвиняемые в совершении преступлений. В соответствии с УПК России и ст.18 Федерального закона РФ от 21.06.1995. подозре-

ваемые и обвиняемые могут встречаться с представителями СМИ только на основании письменного разрешения лица или органа, в производстве которых находится уголовное дело. Однако, это разрешение не является основанием для принятия решения начальником СИЗО о посещении журналистами учреждения, ибо, как сказано в ч.5 ст.38 Закона РФ «Об учреждениях и органах исполняющих уголовные наказания в виде лишения свободы» они «… посещают… следственные изоляторы по специальному разрешению руководства… или вышестоящих органов управления уголовно-исполнительной системы…».

3) Отправляя заявку в территориальное УФСИН на аккредитацию при пресс-службе своих журналистов (ст.48 Закона РФ от 27.12.1991), редакция в случае положительного решения и при соблюдении правил аккредитации приобретает право присутствовать на открытых заседаниях, совещаниях и других мероприятиях, проводимых в аппарате УФСИН, (данное правило не распространяется в отношении посещения учреждений УИС, но и специального запроса также не требуется, т.к. пресс-служба самостоятельно должна составлять список аккредитованных журналистов и получить разрешение, кроме этого, таков же порядок посещения учреждений по инициативе самой пресс-службы). В свою очередь пресс-служба УФСИН обязана предварительно извещать аккредитованных журналистов обо всех мероприятиях, обеспечивать информационными ресурсами и пресс-релизами, создавать благоприятные условия для производства записи и т.д.

4) В соответствии с положениями Федерального закона РФ «Об информации, информатизации и защите информации» информационные ресурсы (документы, массивы документов в архивах, фондах, информационных системах) могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации. Однако не являются объектами авторского права (и соответственно источниками извлечения прибыли) сообщения о событиях и фактах, имеющие информационный характер (ст. 8 Закона РФ «Об авторском праве и смежных правах» – в ред. ФЗ от 19.07.1995 №110-ФЗ).

5) Данный вид отношений рассматриваемого типа касается доступа граждан и организаций к информации о себе уже распространённой в СМИ. При этом действующее законодательство обязывает журналиста проверять достоверность сообщаемой информации, получать согласие на распространение сведений о личной жизни гражданина (в том числе осуждённого), не допустить под видом достоверных сообщений распространение слухов. В свою очередь УФСИН приобретает право: во-первых, при распространении несоответствующих действи-

тельности сведений на опровержение в течение десяти дней со дня получения редакцией требования об опровержении или его текста, или в течение месяца уведомления о предполагаемом сроке распространения опровержения, либо об отказе в его распространении с указанием основания отказа (ст.ст. 43, 44 Закона РФ от 27.12.1991 – в ред. ФЗ от 02.03.1998 №30-ФЗ); во-вторых, на ответ (комментарий, реплику) в отношении которых применяются правила указанных выше статей закона; в-третьих, на доступ и уточнение информации о себе в целях обеспечения её полноты и достоверности, а также кто и в каких целях использует или использовал эту информацию. Владелец информации (СМИ) обязан предоставить информацию бесплатно по требованию тех лиц, которых она касается (ч. 1,2 ст.14 ФЗ от 25.01.1995). Практика показывает, что в последнем случае участники правоотношений далеко не всегда выполняют свои обязанности. В этих случаях юридические лица (УФСИН) в судебном порядке могут требовать опровержения распространённых о СМИ сведений или опубликование ответа истца (ст. 43 Закона о СМИ).

Кроме сказанного свою особую специфику имеет построение взаимоотношений при посещении лечебных учреждений, находящихся в ведении уголовно-исполнительной системы и специальных психиатрических лечебных учреждений, находящихся под охраной ФСИН, что обусловлено врачебной этикой и правилами, установленными законодательством о порядке и условиях оказания психиатрической помощи населению в Российской Федерации.

В заключение необходимо остановиться на дефиниции «общественные интересы», которую законодатель использует в ст. 50 Закона РФ от 27.12.1991 и о соотношении диффамации с конституционными положениями о неприкосновенности частной жизни, защите своей чести и доброго имени. В данном случае речь идёт об этических аспектах работы журналистов. При этом мы считаем, что положения, закреплённые в указанной статье, должны соответствовать технологии «честного профессионализма». Последняя предполагает: обязательную проверку материала перед публикацией; отделение факта от мнения; уважение чести и достоинства людей, соблюдение принципа «не виновен» до решения суда и обязательность исправления ошибки, если она допущена. Эти элементы изложены в Кодексе профессиональной этики российского журналиста (1994 г.), хартии телерадиовещателей, Меморандуме Национальной ассоциации телевещателей России и Московской хартии журналистов и профессиональным журналистам должны быть известны.

Отметим и факт того, что вышеуказанные общие принципы взаимоотношений со СМИ характерны и для других представителей правоохранительных органов, в первую очередь полиции.

Таким образом, отношения сложившиеся в сфере информационного обеспечения деятельности правоохранительных органов и СМИ, являются ярко выраженными правовыми отношениями, они урегулированы соответствующими юридическими нормами, имеют для их участников правовые последствия и в силу сказанного находятся под охраной государства.

Zharkoj M.
Russland, St. Petersburg,
St. Petersburger Universität für Management und Ökonomie

Die rechtliche Natur der Beziehungen zwischen Strafverfolgungsbehörden und Massenmediensmitteln (theoretische und rechtliche Aspekte)

Die spezifische Beziehungen, die zwischen Massenmedienmitteln und Einheiten der Informationswartung (Presse-Service, Mittelpunkte Öffentlichkeitsarbeit, offizielle Vertretern usw.) der Strafverfolgungsbehörden im Gebiet der Informationssicherstellung von die Kriminalitätbekämpfungspolitik und Geselschaftsordnungsschutz Russischer Föderation gebildet sind, haben ihre Besonderheiten, die ihre Natur ausbedingen. Ohne Zweifeln haben diese Beziehungen, die einer der Arten von sozialen Beziehungen sind, nicht nur ihre typische Merkmale, sondern auch unterliegen der Regulierung aufgrund ihrer Spezifität. Dabei, aufgrund der Natur von Subjekten betrachteter Beziehungen (an einer Seite – staatliche Behörde oder Einrichtungen, an andere – Vertretern von „dritter Sektor“), kann man behaupten, dass das Recht als einer besonderen, offiziellen, staatlichen Regler vorsteht. Nämlich führt die staatliche Macht diese Beziehungen mit der Hilfe normativer Einwirkung unter ihre Gerichtsbarkeit hinüber und solchergestalt gibt Stabilität, Ordnung und gewünschtener Orientierung zu. Folglich kann man die hingewiesene Art der sozialen Beziehungen im allgemeintesten Sinne als die rechtlich geregelte Beziehungen bestimmen, d.h. rechtliche.

Dennoch gehört die genannte Beziehungsart zur teilweise geregelte Gruppe, denn man muss in Vormerkung behalten, dass nicht jede Beziehung rechtlicher Regelung sich unterworfen kann, aber in vielen Fällen entsteht diese Notwendigkeit einfach nicht. Die betrachtete Rechtsverhältnisse haben folgende typische Merkmale:

a) sie entstehen und beenden nur aufgrund der Rechtsnormen, die in der russischen Verfassung und in den entsprechenden Bundesgesetzen enthalten: «Über Massenmedien», «Über Urheber- und Leistungsschutzrecht», «Über Einrichtungen und Behörden, die Strafen als Haft durchführen», «Über Erhaltung unter der Verwahrung der Verdächtigen und Angeklagten», «Über Information, Informatisierung und Informationsschutz», «Über Staatanwaltschaft der Russischen Föderation», «Über Polizei», «Über Ordnung der Tätigkeitsbeleuctung der Behörde von der Staatsmacht in staatlichen Massenmedien», im Strafgesetzbuch der Russischen Föderation, Strafvollzugsgesetzbuch der Russischen Föderation und Russlands Strafprozessgesetzbuch, und auch in anderen normativen Rechtsakten. Es ist klar, dass die regulatorische Rechtsfunktion in diesem Fall wie materielle so auch prozessuale Rechtsnormen verwirklichen;

b) Subjekte dieser Beziehungen sind zwischen einander mit subjektiven Rechten und Pflichten verbunden, die, eigentlich, die rechtliche Inhalt des Verhältnisses schaffen. Im Rahmen dieses Verhältnis entspricht der Recht einer Seite zu dem Pflicht anderer Seite und umgekehrt. In diesem Fall führen die Subjekte des Rechtverhältnisses als berechtigte und rechtsverpflichtete Personen zueinander durch. Infolge können Interesse einer Seite nur mittels anderer realisieren sein. Die Beteiligte dieses Rechtsbeziehungen sind die Subjekten des Rechtes, unter denen man in diesem Fall die Menschen (Massenmedienvertreter, Vollzugsbeamte) und ihre Verein (Informationsagenturen, Einheiten der informativen Unterstützung der Strafverfolgungsbehörden und auch Beamte beider Seiten) versteht, die als Rechts- und Pflichtsträger durch das Gesetz durchführen;

c) betrachtete Verhältnisse haben willensstarken Charakter, weil sie ohne den Willen ihrer Mitglieder, oder mindestens eine von ihnen nicht wirken und funktionieren können;

d) wie andere Arten Rechtsbeziehungen, unterscheidet sich untersuchtere Gruppe von der genau Gewissheit gegenseitiges Benehmens des Subjektes, ihrer Individualisierung und Personifizierung Rechten und Pflichten Schließlich werden diese Beziehungen durch den Staat geschützt, nämlich, wenn die rechtliche Vorschriften sich nicht überhaupt nicht oder mangelhafter erfüll, ist Anwendung von Maßnahmen der staatlichen Zwang möglich, weil der Schutz der Legitimität und Rechtsordnung den Rechtsbeziehungsschutz bedeutet. Das sind die wichtigsten Merkmale dieser Art von Beziehungen.

Gleichzeitig muss man in Vormerkung die Besonderheiten der gegenseitigen Beziehungen Massenmediensvertretern mit verschiedene Strafverfolgungsbehörden, der Spezifität von Informationspolitik der Letzteren,

die durch die Staatsaufgabe vermittelt sind (z.B., Staatsanwaltschaft, der Untersuchungsausschuss des Ermittlungsverfahrens und Anfrage, Einheiten, die das Recht der Durchführung von operativer suchender Tätigkeit haben), behalten.

Betrachten wir insbesondere die typischen Situationen, die in Prozess der Informationsbereitsstellung der Tätigkeit des Strafvollzugsystem des Bundesdienstes von der Ausführung der Strafe des Ministerium für Justiz, dessen Einheiten und Behörden bis heute zu den geschlossenen von Gesellschaft Elementen des Staates Mechanismus treu gehören. Hier im Rechtsverhältnisinhalt kann man mindestens fünf Aspekte benennen:

1) Die Reihenfolge der Besuche der Behörden und Einrichtungen der Ausführung von Strafen ist klar mit dem Art. 24 des Strafvollzugsgesetzbuches geregelt – Massenmediensvertretern und andere Personen sind berechtigt Einheiten und Behörden mit spezieller Bewilligung der Verwaltung von diesen Einheiten und Behörden oder von den übergeordneten Behörden (Leitung des Bundesdienstes von der Ausführung der Strafe) zu besuchen. Dabei versteht man unter dem Massenmediensvertretern Journalisten von Rundfunk, Fernsehen, Zeitschriften und anderen Medien, die entsprechende Lizenzen und Leitungsbestellungen der Medien und Publikationen haben. Laut dem Art. 39, 40 des Gesetzes «Über Massenmedien» formalisiert die Publikationsredaktion Anfrage für Informationen und sendet sie in die Leitung des Bundesdienstes von der Ausführung der Strafe). Als Folge erhält die letztere die Pflicht die Redaktion zu in informieren: a) während drei Tagen von dem Tag der schriftlichen Anfrage über die Ablehnung und die Gründe für die angefragte Information, die sich nicht vorstellen kann.; b) in denselben Frist über die Verzögerung bei der Vorstellung der Information, wenn die erforderliche Information innerhalb sieben Tagen nicht eingereicht werden können; c) Leitern des Bundesdienstes von der Ausführung der Strafe legen die Information durch das Presse-Amt oder durch andere berechtigte Personen in ihrem Hoheitsbereich vor.

2) Das Massenmediensvertreterbesuch der Untersuchungshaft haben ihre Besonderheiten. In diesen Untersuchungshaften enthalten sich Verdächtigen und Angeklagten bei der Verbrechen. Laut dem Russlands Strafprozessgesetzbuch und dem Art. 18 des Bundesgesetzes von Russischer Föderation von 21.06.1995 können Verdächtigen und Angeklagten mit Massenmediensvertretern nur aufgrund einer schriftlichen Bewilligung des Personen oder der Behörden, die mit konkreter Strafsache arbeiten. Aber diese Bewilligung ist keiner Grund für die Entscheidung vom Leiter der Untersuchungshaft über die Besuche von Journalisten der Einheit, weil, wie es im Art. 38 des Gesetzes «Über Einrichtungen und Behörden, die Strafen

als Haft durchführen», sie «… besuchen… Untersuchungshaften durch spezielle Bewilligung der Leitung… oder übergeordneten Verwaltungsbehörden des Strafvollzugsystem…».

3) Wenn die Redaktion den Anwendung für die Akkreditierung des Presse-Amts von den Journalisten in territorialer Leitung des Bundesdienstes von der Ausführung der Strafe sendet (Art.48 Gesetzes von 27.12.1991), erhaltet sie (im Falle einer positiven Entscheidung und in Übereinstimmung mit den Regeln der Akkreditierung) das Recht der Besuch der öffentlichen Sitzungen, Konferenzen und anderer Veranstaltungen, die man in Leitungsapparat des Bundesdienstes von der Ausführung der Strafe durchführt (diese Vorschrift verbreitet auf Besuche der Strafvollzugsystemseinheiten, aber es fordert sich keine spezielle Anfrage, weil das Presse-Amt eine Liste der akkreditierten Journalisten selbständig bilden muss und auch Bewilligung erhalten muss, außerdem ist Reihenfolge des Besuches von Einheiten mit Initiative des Presse Amts dieselbe. Ebenfalls muss die Pressedienst der Leitung des Bundesdienstes von der Ausführung der Strafe zuerst akkreditierten Journalisten über alle Veranstaltungen informieren, Informationsquellen und Pressemitteilungen bereitzustellen, günstige Bedingungen für die Aufnahmeproduzierung schaffen usw.

4) Laut der Vorschriften des Bundesgesetzes der Russischer Föderation «Über Information, Informatisierung und Informationsschutz» Informationsquellen (Dokumenten, Dateien von Dokumenten in Archiven, Sammlungen, Informations-Systeme) können Ware sein (außer der Fallen, die in der Gesetzgebung von Russischer Föderation vorausgesetzt sind). Aber sind Nachrichten über Ereignisse und Fakten, die informationelle Charakter haben (Art. 8 Gesetzes «Über Urheber- und Leistungsschutzrecht») keine Objekten des Urheberrecht (und demnach keine Gewinnsquelle);

5) Dieses Beziehungsart vom betrachteten Typ geht des Zugangs der Bürger und Organisationen zur Information über sich selbst an, die in Medien schon verbreitet ist. Dabei verpflichtet die geltende Gesetzgebung den Journalisten die Gültigkeit der gemeldeten Information zu prüfen, Zustimmung für die Informationsverbreitung über das Privatleben der Bürger (einschließlich des Verurteilten) zu erhalten, Gerüchten unter dem Deckmantel der gültigen Berichte nicht zu zulassen. Ebenfalls erhielt die Leitung des Bundesdienstes von der Ausführung der Strafe: erstens – das Recht für eine Wiederlegung (bei der Verbreitung von unwahren Informationen) während 10 Tagen vom Erhaltstag in Redaktion der Forderung über die Widerlegung oder ihres Texte, oder während eines Monates der Benachrichtigung über übergenommenen Frist der Wiederlegungsverbreitung, oder über eine Ablehnung ihrer Verbreitung mit der Angabe der Gründe (Art. 43, 44 des Ge-

setzes von 27.12.1991 №30-ФЗ); zweitens – das Recht für die Antwort (Kommentar, Bemerkung), die mit den Normen der oben bezeichneten Artikels des Gesetzes geregelt ist; drittens, das Recht für den Zugang und der Verfeinerung der Information über sich selbst, um ihre Vollständigkeit und Genauigkeit zu gewährleisten, und auch wen und mit welchen Zielen diesen Information benutzt oder irgendwann benutztet hat. Der Informationsbesitzer (Massenmedien) muss die Information nach der Forderung die Personen, deren sie angeht, kostenlos liefern verpflichten. Die Praxis zeigt, dass im letzteren Fall haben die Teilnehmer der Rechtsbeziehungen nicht immer ihre Pflichten erfüllen. In diese Fälle juristische Personen (Leitung des Bundesdienstes von der Ausführung der Strafe) können gerichtlich die Wiederlegung der in Medien verbreitete Information oder die Veröffentlichung der Klägersantwort fordern (Art. 43 des Bundesgesetzes «Über Massenmedien»).

Außer genanntes hat ihre besondere Spezifität Aufbau von Beziehungen bei einem Besuch in Krankenhäusern, die in Durchführung des Strafvollzugsystems und der speziellen psychiatrischen Krankenhäusern, die unter dem Schutz des Bundesdienstes von der Ausführung der Strafe sind, und das ist bei ärztlicher Ethik und Regeln, die mit Gesetzgebung über Reihenfolge und Bedingungen der psychiatrischen Versorgung in der Russischen Föderation festgesetzt sind, bedingt.

Zum Schluss müssen wir die Definition von «öffentlichen Interesse», die der Gesetzgeber in Art. 50 des Gesetzes von 27.12.1991. benutzt und betrachten den Bezug auf die Diffamierung der verfassungsrechtlichen Vorschriften zum Schutz der Privatsphäre, Schutz der Ehre und guten Namen. In diesem Fall geht die Rede über die ethischen Aspekte der Arbeit von Journalisten. Dabei glauben wie, dass die Vorschriften, die in diesem Artikel konsolidiert sind, der Technologie von «ehrlicher Professionalität» entsprechen müssen. Die Letztere deutet: obligatorische Prüfung des Materials vor der Veröffentlichung; Trennung Meinungen von Tatsachen; Respekt für die Ehre und Würde der Menschen, Befolgung vom „nicht schuldig“ Prinzip vor der gerichtliche Entscheidung. Verpflichtung der Korrektur der Fehler, wenn sie zugelassen sind. Diese Elemente sind in dem Gesetzbuch der professionalen Ethik des russischen Journalisten (J. 1994), in Charta der Fernseh- und Rundfunkanstalten, im Memorandum der Nationale Assoziation von Fernsehanstalten Russlands und in Moskauer Charta des Journalisten. Und professionale Journalisten müssen das kennen.

Beachten wie den Fakt, dass oben beachtete gemeinde Prinzipien von Beziehungen mit Massenmedien für andere Vertreter von Strafverfolgungsbehörden (in erster Linie – für Polizei) typisch sind.

Damit sind die Beziehungen im Bereich der informativen Unterstützung der Tätigkeit von Strafverfolgungsbehörden und Medien wohldefinierte Rechtsverhältnisse. Sie sind mit entsprechenden rechtlichen Normen geregelt, haben Rechtsfolgen für ihre Subjekten und sind unter staatlichem Schutz.

Чумлякова В.А.
Россия, Санкт-Петербург,
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. Северо-Западный институт

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ НА ОФИЦИАЛЬНЫХ САЙТАХ

Без развития и совершенствования информационных технологий невозможно обеспечить достижение стратегически важных национальных интересов. Но одновременно с формированием информационного общества появляются и серьёзные угрозы в виртуальном пространстве.

В 2011 г. в Томске прошло выездное совещание Совета Безопасности России, на котором вопрос о правовом обеспечении защиты информации на государственных сайтах стал одним из наиболее актуальных и злободневных.

По словам секретаря Совета безопасности РФ Николая Патрушева, «процесс информатизации общества, органов государственной власти и бизнеса породил в стране рост компьютерной преступности. Преступная деятельность в этой сфере стала общественно опасной и зачастую совершается организованными преступными группами (ОПГ). Нередко ОПГ используют профессиональных хакеров, квалификация которых с каждым годом растёт».

По мнению Патрушева, одновременно повышается интерес зарубежных спецслужб к закрытой информации военного, политического и экономического характера. И этот интерес не просто растёт – закрытую информацию пытаются получить, используя самые современные технологии.

В 2010 году значительно возросло количество попыток целенаправленного воздействия на информационные системы органов государственной власти.

Поэтому вопрос защиты информации на всех уровнях власти и управления имеет важнейшее значение с точки зрения обеспечения национальной безопасности России.

Что касается регионального уровня, то здесь этот вопрос стоит тоже очень остро. По данным спецслужб, в 2010 году только в Сибирском федеральном округе зафиксировано более 18 миллионов компьютерных атак, включая попытки захвата или блокирования порталов и сайтов. По данным экспертов, часть из этих атак была направлена на проверку уязвимости систем защиты сайтов. То, что совещание Совета безопасности по данной тематике проходило именно в Сибирском федеральном округе (СФО), не случайно. Округ имеет стратегическое значение, и на его территории расположено большое количество режимных предприятий, вся деятельность которых составляет государственную тайну и поэтому требует дополнительных мер по защите информации.

Между тем, по словам Николая Патрушева, в ряде субъектов СФО, например, в республиках Алтай и Тыва, в Алтайском и Красноярском крае, Новосибирской и Кемеровской областях очень медленно реализуются требования Указа президента «О мерах по обеспечению информационной безопасности...». В частности до сих пор не до конца укомплектованы подразделения, которые должны заниматься технической защитой информации органов исполнительной власти.

Нередко сведения, составляющие государственную тайну, обрабатываются на компьютерах с программным обеспечением, которые не прошли соответствующей аттестации (категорирования) в федеральной службе безопасности (ФСБ).

Как заявил Николай Патрушев, для решения этих и других вопросов требуется переход в информационно-телекоммуникационных сетях и информационных системах на сертифицированные ФСБ России средства обнаружения компьютерных атак. Также для противодействия информационным угрозам потребуется принятие комплекса мер в области защиты информации, не подлежащей разглашению и несанкционированное распространение которой способно повлечь негативные социально-политические последствия.

Что же касается конкретных источников правового обеспечения защиты информации на государственных сайтах, то здесь следует обратиться к Федеральному закону от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», а также к Указу Президента РФ от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Согласно Федеральному Закону от 27.07.2006 № 149-ФЗ ст. 16 п. 5, требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем, используемые в целях защиты информации методы и способы её защиты должны соответствовать указанным требованиям.

Согласно Указу Президента РФ от 17.03.2008:

- подключение информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети "Интернет", не допускается, а при необходимости подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, указанных выше, к информационно-телекоммуникационным сетям международного информационного обмена такое подключение производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данного требования является обязательным для операторов информационных систем, владельцев информационно-телекоммуникационных сетей и (или) средств вычислительной техники;

- государственные органы в целях защиты общедоступной информации, размещаемой в информационно-телекоммуникационных сетях международного информационного обмена, используют только средства защиты информации, прошедшие в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие

подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;

- размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях.

Проанализировав два данных документа, можно сделать вывод о том, что защитой информации на государственных сайтах, проведением сертификации специально предназначенных средств защиты информации, в том числе шифровальных (криптографических) средств, осуществлением противодействия техническим разведкам занимается Федеральная Служба Безопасности РФ.

Говоря о правовом обеспечении защиты информации на государственных сайтах, также следует сказать об ответственности, предусмотренной за правонарушения в сфере информации, информационных технологий и защиты информации.

В целом за нарушение требований Федерального закона «Об информации, информационных технологиях и о защите информации» согласно ст. 17 п. 1 данного закона предусмотрена дисциплинарная, гражданско-правовая, административная или уголовная ответственность в соответствии с законодательством Российской Федерации.

Что же касается ответственности, предусмотренной за нарушение законодательства в области защиты информации на государственных сайтах, то пока что отдельных норм за такие правонарушения ни в Уголовном кодексе, ни в Кодексе об административных правонарушениях, нет, однако Министерство юстиции РФ опубликовало проект федерального закона, вводящего уголовную ответственность за «взлом» государственных информационных ресурсов, в том числе находящихся в Интернете.

В соответствии с законопроектом, которое правительство внесло на рассмотрение Государственной думы, УК РФ предлагается дополнить ст. 272.1. Санкцию за такое преступление предлагается установить на уровне до 3 лет лишения свободы.

Статья 272.1. подразумевает ответственность за неправомерный доступ к государственным информационным системам и (или) содержащимся в них государственным информационным ресурсам, причём для наступления уголовной ответственности необходимо будет, чтобы

такой «взлом» повлёк уничтожение, блокирование, модификацию либо копирование информации, нарушение функционирования государственной информационной системы.

Те же деяния, совершённые группой лиц по предварительному сговору или организованной группой либо лицом, имеющим доступ к государственным информационным системам, в том числе функционирующим в составе критически важных объектов, и (или) содержащимся в них государственным информационным ресурсам в силу его служебного положения, должны наказываться лишением свободы на срок от 3 до 7 лет.

При этом под критически важными объектами понимаются объекты, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики страны, субъекта РФ либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный срок.

В Кодекс РФ об административных правонарушениях предлагается также ввести состав такого правонарушения, как «несоблюдение установленного порядка взаимодействия операторов услуг сети "Интернет" с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности РФ».

Хотя данные нормы официально ещё не нашли свое отражение в российском законодательстве, факт того, что правительство России занимается их разработкой ввиду необходимости принятия этих норм, является очевидным и их законодательное закрепление – это лишь вопрос времени. Ведь от этого зависит благополучие и благосостояние всей России, всего российского общества.

Tschumljakowa W.
Russland, Sankt-Petersburg,
Der Russischen Akademie der Volkswirtschaft und Staatliches Dienstes unter dem Präsidenten der Russischen Föderation. Nordwestliches Institut der Unternehmensführung

Die rechtliche Bereitstellung vom Informationsschutz an offiziellen Webseiten

Es ist unmöglich, die Ereignis der strategisch wichtigen nationalen Interessen ohne der Entwicklung und Verbesserung der Informationstechnologie достижение bereitzustellen. Aber gleichzeitig erscheinen mit der Bildung der Informationsgesellschaft die ernsthaften Bedrohungen im virtuellen Raum.

Im Jahre 2011 war eine wichtige rückzugige Besprechung des Sicherheitsrates Russlands in Tomsk vergangen, wo die Frage über rechtliche Bereitstellung vom Informationsschutz an staatlichen Webseiten eine der aktuelle und topische würde.

Der Sekretär der Besprechung des Sicherheitsrates Russlands Nikolay Patruschew sagte: «Der Prozess der Informatisierung der Gesellschaft, den Behörden und Unternehmen brachte im Land das Wachstum der Computer-Kriminalität hervor. Kriminelle Tätigkeit in diesem Bereich wurde sozial gefährlich und wurde auch oft von organisierten kriminellen Gruppen (OKG) durchgeführt. Häufig benutzen OKG die professionellen Hacker, deren Qualifikation immer wächst».

Patruschew glaubt, dass Interesse von ausländischen speziellen Diensten zur verschlossenen Information des militärischen, politischen und wirtschaftlichen Charakters sich gleichzeitig erhöht. Und dieses Interesse erhöht nicht einfach – man versucht der verschlossenen Information mit moderntesten Technologien benutzend erhalten.

2010 stieg die Anzahl der Versuche von zielgerichteter Auswirkung von Informationssystemen der staatlichen Behörden wesentlich.

Deshalb hat die Frage des Informationsschutzes auf allen Stufen der Regierung und Verwaltung eine wichtigste Bedeutung vom Standpunkt der nationalen Sicherheit Russlands.

Auf der regionalen Ebene steht die Frage sehr scharf. Laut Angaben der speziellen Dienste fixiert im Jahre 2010 über 18 Millionen Computer-Attacken nur im Sibirischen Bundesregion (einschließlich der Versuche von Fangen oder Blockierung der Portale und Webseite). Laut Expertenangaben wurde ein Teil von diesen Attacken nach Verletzlichkeitsprüfung des Webseitenschutzsystems gerichtet. Es ist nicht zufällig, dass die Besprechung

des Sicherheitsrates nämlich im Sibirischen Bundesregion (SBR) vergangen war. Der Region hat eine strategische Bedeutung und sein Gebiet fasst eine große Anzahl von modalen Unternehmen, all deren Aktivität ist ein Staatsgeheimnis und deshalb fordert sie zusätzliche Maßnahmen zum Informationsschutz.

Mittlerweile, wie Nikolay Patruschew sagte, realisiert die Anforderungen der Erlass des Präsidenten "Über Maßnahmen zur Gewährleistung der Informationssicherheit ..." in einigen Subjekten des SBR, z.B., in den Republiken Altai und Tuwa, in den Krajen Altai und Krasnojarsk, Nowosibirsk und Kemerowo Gebieten sehr langsam. Insbesondere sind die Abteilungen noch nicht gut ausgestattet, die mit dem technischen Informationsschutz von der vollziehenden Gewalt beschäftigen müssen.

Die Staatsgeheimnis enthaltende Information verarbeitet sich häufig auf Computern mit Software, die nicht die entsprechende Zertifizierung (Kategorisierung) der Bundesagentur für Sicherheit der Russischen Föderation bestanden haben.

Nach Nikolaj Patruschew fordert sich für die Lösung dieser und anderer Fragen Übergang in den Informations-und Telekommunikations-Netzen und Informationssystemen zu bei Bundesagentur für Sicherheit der Russischen Föderation zertifizierten Mitteln Erkennung von Computer-Attacken. Für Bewältigung der Informationsbedrohungen wird auch die Annahme von Maßnahmen zum Informationsschutz erfordert, die offenlegen nicht kann und unbefugtere Verbreitung von deren zu negativen sozialen und politischen Folgen führen kann.

Als besondere Quellen rechtliche Bereitstellung vom Informationsschutz an staatlichen Webseiten muss man das Bundesgesetz von 27.07.2006 № 149-ФЗ «über die Information, Informationstechnologie und Informationsschutz» und den Erlass des Präsidenten der Russischer Föderation von 17.03.2008 № 351 «Über Maßnahmen für Bereitstellung der Sicherheit der Russischen Föderation mit der Verwendung Informations-und Telekommunikations-Netzwerke des internationalen Informationsaustauschs» nennen.

Laut dem Art. 16 des Bundesgesetzes von 27.07.2006 № 149-ФЗ, legen sich Anforderungen über den Schutz der in staatlichen Informationssystemen enthaltende Information mit der Bundesbehörde der vollziehenden Gewalt im Bereich der Sicherheitsgewährleistung und mit der Bundesbehörde der vollziehenden Gewalt, die im Bereich der Bekämpfung mit technischer Intelligenz und technischem Informationsschutz im Rahmen ihrer Kompetenz. Bei der Schaffung und Benutzung der staatlichen Informationssysteme, die für den Informationsschutz verwendet werden, müssen die

Methoden und Weisen ihres Schützes der genannten Anforderungen entsprechen.

Laut dem Erlass des Präsidenten der Russischen Föderation von 17.03.2008:

- Verbindung der IT-Systemen, Informations-und Telekommunikationsnetze und den Mitteln der Computer-Technik, die für Speicherung, Verarbeitung und Übertragung der Informationen anwendet, die Dateien von Staatsgeheimnis hat oder die Information enthalten, deren Besitzer staatliche Behörden sind, und, die Dateien, die Amtsgeheimnis, zugelässt sich zu Informations- und Telekommunikationsnetzen einschließlich der internationalen Computernetz "Internet", die die Übertragung der Information durch staatliche Grenzen möglich macht, nicht. Und wenn die Verbindung von IT-Systemen, Informations- und Telekommunikationsnetzen und den Mitteln der Computer-Technik Informations-und Telekommunikationsnetze von internationalen Informationsaustausch, die oben genannt sind, notwendig ist, wird solche Verbindung nur mit dafür speziell bestimmterer Anwendung der Mittel von Informationsschutz und einschließlich Verschlüsselungsmitteln (Kryptographiemitteln), die der festgelegener bei der russischen Gesetzgebung Zertifizierung in Bundesagentur für Sicherheit der Russischen Föderation der Russischen Föderation vorgegangen sind, und (oder), die die Bestätigung über die Einhaltung des Föderalen Dienstes für technische und Exportkontrolle erhaltet haben, gemacht. Umsetzung dieser Anforderung ist für die Betreiber von Informationssystemen, die Besitzer Informations- und Telekommunikationsnetzen und die Mitteln der Computer-Technik obligatorisch;

- staatliche Behörden anwenden für die Schutz der öffentlichen Information, die in der Informations-und Telekommunikations-Netzwerke des internationalen Informationsaustausches nur Mitteln der Schutzinformation, die der festgelegener bei der russischen Gesetzgebung Zertifizierung in Bundesagentur für Sicherheit der Russischen Föderation vorgegangen sind, und (oder) die die Bestätigung über die Einhaltung des Föderalen Dienstes für technische und Exportkontrolle erhaltet haben.

- Platzierung der technischen Mitteln, die zu Informations- und Telekommunikations-Netzwerken des internationalen Informationsaustausches verbinden, in Raumen, die für der Verhandlungsführung anwendet werden, während deren man sich die staatliches Geheimnis enthaltende Fragen diskutiert, verwirklicht sich nur wenn es der Zertifikat gibt, der die Anwendung solcher technischer Mitteln in genannten Räumen sich erlaubt.

Nach dem Analyse beider Dokumenten kann man folgern, dass Bundesagentur für Sicherheit der Russischen Föderation sich mit dem Informa-

tionsschutz auf staatlichen Webseiten, mit der für Zertifizierungsführung, die für speziell Mitteln der Informationsschutz einschließlich Verschlüsselungsmitteln (Kryptographiemitteln) anwendet ist, und mit der Verwirklichung der Bekämpfung von technischer Intelligenz beschäftigt.

Über der rechtlichen Bereitstellung der Information auf staatlichen Webseiten muss man auch sagen über die Verantwortlichkeit, die für Delikte im Bereich der Information, Informationstechnologie und Informationssicherheit vorgesehen sind.

Bei Verletzung der Anforderungen der Bundesgesetz (Art. 17) «Über Information, Informationstechnologie und Informationsschutz» ist disziplinar-, zivil-, verwaltungs-oder strafrechtliche Verantwortlichkeit, die bei der Gesetzgebung der Russischer Föderation vorgesehen sind.

Über die Verantwortlichkeit, die für Verletzung der Gesetzgebung im Bereich der Information auf staatlichen Webseiten vorgesehen sind, gibt es noch keine einzige Normen weder im Strafgesetzbuch noch im Gesetzbuch über Verwaltungsdelikte, aber Ministerium für Justiz der Russischer Föderation hat einen Projekt des Bundesgesetzes, der strafrechtliche Verantwortlichkeit für «Hacking» der staatlichen Informationsressourcen einschließlich im Internet eingeführt.

Laut dem Gesetzesprojekt, der die Regierung in Staatsduma eingetragen hat, wird es in Strafgesetzbuch der Russischen Föderation den Art. 272.1. vorausgesetzt. Die Sanktion für solche Straftat wird bis 3 Jahren der Haft festsetzen vorgeschlagen.

Der Artikel 272.1. übernimmt die Verantwortung für den unberechtigten Zugriff zu staatlichen Informationssystemen und (oder) enthaltenden darin staatlichen Informationsressourcen. Sowie wird es für dem Stammen der strafrechtlichen Verantwortung solche «Haking» Zerstörung, Blockierung, Modifizierung oder Kopieren der Information, der Verletzung der Funktionsfähigkeit von staatlichem Informationssystem zu verursachen notwendig.

Dieselbe Taten von einer Gruppe von Personen nach vorheriger Verschwörung oder einer organisierten Gruppe, oder der organisierten Gruppe oder einem Person, die Zugang zu staatlichen Informationssystemen, einschließlich in Zusammensetzung der funktionierenden kritisch wichtigen Objekte und (oder) darin enthaltenden staatlichen Informationsressourcen aufgrund seiner Amtsstellung gemacht sind, müssen mit Freiheitsstrafe von 3 bis 7 Jahren bestrafen.

Dabei unter kritisch wichtigen Objekten versteht man die Objekten, deren Verletzung oder Einstellung der Funktionierung zum Kontrollverlust, der Zerstörung der Infrastruktur, unumkehrbarer negativer Veränderung

oder Zerstörung der Wirtschaft des Landes, des Subjekten der Russischer Föderation oder administrativ-territorialer Einheit bringt, oder die Sicherheit der Lebensqualität von Bevölkerung, die in diesen Territorien lebt, langfristig verschlechtert.

In Gesetzbuch von Russischer Föderation über Verwaltungsdelikte wird die Einführung solcher Delikte wie «Nichteinhaltung der bestehenden Ordnung des Zusammenwirkens von Operatoren der Netzwerkdienste "Internet" mit den staatlichen Behörden, die die operative suchende Tätigkeit oder die Sicherheitsgewährleistung von Russischer Föderation verwirklichen» angenommen.

Obwohl diese Regeln noch nicht offiziell in der russischen Gesetzgebung anwenden, ist die Tatsache, dass die Regierung von Russland sich mit ihren Entwicklung wegen die Notwendigkeit von diesen Normen beschäftigt, klar. Und ihre rechtliche Konsolidierung ist nur eine Frage der Zeit. Das Wohlbefinden und den Wohlstand von ganzem Russland, ganze russische Gesellschaft hängt davon ab.

Препияло О.С.
Россия, Санкт-Петербург,
СПбЮИ(ф)А ГП РФ

ИНТЕРНЕТ КАК СРЕДСТВО РАЗВИТИЯ ПРЕСТУПНОГО БИЗНЕСА

Интернет настолько прочно вошёл в нашу жизнь, что многие просто не представляют себе учёбу, работу, общение без использования его ресурсов. Можно долго перечислять плюсы сети, но не стоит забывать, что и мошенники, преступные группы ценят достоинства Интернета. Уже на протяжении многих лет организованная преступность активно развивается, используя информационные ресурсы Интернета. То, как Интернет становится средством развития преступного бизнеса, рассмотрим на примере наркоторговли, торговли людьми и в порно бизнесе.

Интернет в современном обществе является одним из самых доступных источников информации. Благодаря относительной бесцензурности общения в сети, любой пользователь может не только прочесть отзывы и рекомендации по применению тех или иных наркотических средств, но и приобрести их. Проводились исследования, по результатам которых распространённый поисковый сервер «Google»

выдал информацию о 305 тыс. сайтов на тему наркотиков[5]. Нельзя не отметить, что в последние годы русскоязычные поисковые системы настроены так, что по запросам наркотической направленности в первую очередь выдают ссылки на сайты, предлагающие профилактику наркомании. Но это не решает всей проблемы, как и не решает её то, что правоохранительным органам известны практически все возможные способы торговли наркотическими средствами в глобальной сети. Продавцы активно обращают в плюс возможность анонимного общения в Интернете. Связаться с администрацией и обговорить условия сделки можно с помощью известных программ «Skype» и «ICQ», «QIP», естественно, без аудио- и видеозвонков. Заключение сделки производится по закрытым каналам, вход на которые покупателю сообщает администратор. Оплата производится через платёжные системы («WebMoney», «Yandex-Деньги») или платёжные терминалы («Элекснет»). Кроме того, при регистрации доменов и создании вебсайтов используют неверные данные или данные подставных лиц, производят неоднократную переадресацию обращений пользователей, периодически изменяют место размещения ресурса.

Обратимся теперь к такому бизнесу организованной преступности, как торговля людьми. Уже давно не являются новшеством так называемые брачные агентства, международные брачные организации. Они собирают информацию о лицах, готовых заключить брак с иностранным гражданином, организуют знакомства и помогают с выездом за границу. Основной риск при использовании услуг таких организаций заключается в том, что клиент не всегда получает полную и объективную информацию, как о предполагаемом будущем супруге, так и о самой деятельности данной организации. В первом случае может иметь место многоженство, бытовое насилие, продажа мужем сутенерам. Таким образом, организация не выполняет в полном объёме свои функции по сбору информации или же намеренно поставляет «живой товар» на определённые цели. В любом случае, получает от своих действий доход. Второй случай предполагает развитие налаженного бизнеса по вывозу людей за границу с целью, например, получения бесплатной рабочей силы или привлечения их к занятию проституцией под прикрытием совершения действий, направленных на заключение

[5] Бряндина А.С. Особенности борьбы с преступным оборотом наркотиков в сети Интернет // Вестник Московского университета МВД России. 2009. № 2. С. 85.

интернационального брака. Как правило, клиенты, ставшие уже жертвами, лишаются документов, удостоверяющих личность, и средств связи с родными, подвергаются насилию и устрашению, нередко «накачиваются» наркотиками. Несмотря на известность таких схем торговли людьми, многие женщины, к сожалению, до сих пор попадаются на уловки преступников, обещающих безбедную жизнь с заграничным мужем или хорошо оплачиваемую работу за границей.

По данным Госдепартамента США, ежегодно в рамках трафика через границу перебрасывается от 700 тысяч до 2 миллионов женщин и детей. Представители ФБР считают, что около 200 российских организованных преступных групп поддерживают связи с группировками в США и большинство из них подключены к схемам секс-трафика. В сотрудничестве с организованной преступностью такие брачные агентства обмениваются анкетами клиентов, информацией о них, а также информацией о способах беспрепятственного вывоза товара, о наличии коррумпированных чиновников.

Ещё одним прибыльным преступным бизнесом, осуществляемым с помощью ресурсов Интернета, является порно индустрия. Наверное, каждый пользователь хотя бы раз сталкивался с рекламой недвусмысленного содержания. Глобальная сеть может предоставить более 4 миллионов порно сайтов, запрос «порно», по статистике «Яндекса», вбивают около 4,5 миллионов раз в месяц. По разным данным порно индустрия приносит прибыль от 15 до 25 миллиардов долларов США. Доходы от продажи порно в «рунете» составляет около 250-300 миллионов долларов США.

Таким образом, мы видим, что Интернет, действительно, является одним из средств развития и процветания преступного бизнеса. Организованные преступные группы активно используют ресурсы Интернета для налаживания наркоторговли, торговли оружием, порно бизнеса, торговли людьми. Нередко одна преступная группа одновременно использует все возможные пути получения прибыли посредством глобальной сети. Попытки преодоления данной проблемы предпринимаются на протяжении многих лет. Об этом свидетельствуют и международные договоры (например, Конвенция ООН против транснациональной организованной преступности 2000 года, Конвенция Совета Европы по противодействию торговле людьми 2005 года), и совершенствование федерального законодательства. Но всегда стоит помнить, что развитие технологий, появление новых способов получения прибыли преступным путём всегда будет существенно опережать соответствующую реакцию законодателя. Поэтому нужно не только

развивать международное сотрудничество в соответствующей сфере, но и пытаться предупреждать возможные преступные действия в сети, обладать высококвалифицированными кадрами правоохранительных органов. Для противодействия незаконному обороту наркотических средств в Интернете и распространению порнографической продукции сеть нужно подвергать цензуре: использовать фильтры на конкретные слова у провайдера, активно отслеживать информацию на сайтах, отказывать в размещении информации на сайте при отсутствии достоверных сведений о его владельце. Кроме того, развитие преступного бизнеса, как и любую проблему, нужно решать комплексно. Показательным, например, является то, что процветание торговли женщинами коренится, в том числе, в социально-экономическом развитии общества, из которого у них появляется желание уехать.

Prepijalo O.
Russland, St. Petersburg,
St. Petersburger Rechtsinstitut (Niederlassung) der Akademie der
Generalstaatsanwaltschaft der Russischen Föderation

Internet als Mittel der kriminellen Entwicklung vom Unternehmen

Internet hat in unseres Leben so fest eingekommen, so stellen meistens Studium, Arbeit, Kommunikation, ohne seiner Ressourcen benutzend, nicht vor. Man kann Vorteile des Netzes lange zählen, aber soll man nicht vergessen, dass Gauner, kriminelle Gruppen auch die Vorteile des Internets schätzen. Seit vielen Jahren entwickelt sich schon organisierte Kriminalität aktiv mit Hilfe der Internet-Ressourcen. Sehen wir den Drogenhandel, Menschenhandel und Porno-Unternehmen als Muster durch, wie Internet ein Mittel der Entwicklung vom kriminellen Unternehmen wird.

In moderner Gesellschaft ist der Internet einer der zugänglichsten Quellen der Information. Dank der relativ unzensierten Netzkommunikation kann jeder Benutzer nicht nur der Kritik und Empfehlungen für den Einsatz von bestimmten Drogen lesen, sondern auch sie kaufen. Man hat Forschungen durchgeführt, nach deren Ergebnisse der verbreiteten Suchmaschine «Google» der Information über 305 Tausend Webseiten unter dem Thema „Drogen“[6]. Es ist unmöglich keine Bemerkung machen, dass die russisch-

[6] Brjandina A., Merkmale der Bekämpfung mit kriminellem Drogenhandel im Internet // Westnik (=Messenger) von Moskauer Universität des Innenministerium Russlands. 2009. № 2. S. 85.

sprachige Suchmaschinen in letzten Jahren so eingestimmt sind, dass auf drogen-orientierten Anfragen in erster Linie die Linken zeigen, die die Prophylaxe der Drogensüchtigkeit vorschlagen. Aber das löst ganzes Probleme nicht, wie löst es auch nicht, dass fast alle mögliche Wegen des Drogenmittelhandels im globalen Netz der Strafverfolgungsbehörden bekannt sind. Händler machen aus der Möglichkeit von anonymer Kommunikation im Internet dem Vorteil aktiv. Man kann mit der Hilfe der bekannter Programmen wie «Skype», «ICQ» und «QIP» natürlich ohne Audio- und Videoanrufe mit der Administration kontaktieren und die Bedingungen der Abmachung besprochen. Der Abmachungsabschluss setzt auf geschlossenen Kanäle durch, der Eingang zu denen der Administrator einem Käufer berichtet. Die Bezahlung erfolgt sich durch Zahlungssysteme («WebMoney», «Yandex-Geld») oder Zahlungsterminals («Elecsnet»). Außerdem verwendet man bei der Registrierung Domain-Namen und Erstellung von Webseiten unrichtige Dateien oder Dateien der Strohmänner, macht wiederholter Anfragen der Kontakte von Benutzern, ändert den Speicherort der Ressource regelmäßig.

Kommen wir jetzt zum solchen Unternehmen der organisierten Kriminalität wie Menschenhandel. Seit langem sind so genannte Ehe-Agenturen, internationale Organisationen von Ehe nicht neu. Sie sammeln Information über Menschen, die mit fremdem Bürger fertig zu verheiraten sind, organisieren Bekanntschaften und helfen mit Reisen ins Ausland. Das Hauptrisiko bei der Nutzung der Dienste solcher Organisationen ist, dass der Kunde nicht immer volle und objektive Information wie über angenommenen zukünftigen Ehepartner so auch über die Tätigkeit der Organisation. Im ersten Fall kann man mit Gewalt in der Familie, den Verkauf bei Ehemann den Zuhältereien. So erledigt die Organisation ihre Funktionen über Informationssammlung nicht voll oder liefert absichtlich liefert "Live-Waren" für bestimmte Ziele. In jedem Fall erhaltet sie von ihren Aktionen ein Einkommen. Der zweite Fall setzt die Entwicklung von einem etablierten Unternehmen für die Ausfuhr der Menschen im Ausland mit Ziele, zum Beispiel, Erhaltung ein freierer Arbeitskraft oder Beteiligung ihr an die Prostitution unter dem Deckmantel von Einnahme der Aktionen auf den Abschluss den internationalen Ehe voraus. Typischerweise entbehren Kunden, die schon Opfer geworden sind, Ausweisdokumenten und Kommunikationsmitteln, sind um Gewalt und Einschüchterung ausgesetzt, treten zu Drogen häufig bei. Trotz der Popularität solcher Systeme von Menschenhandel, fallen vielen Frauen bis jetzt leider auf Tricks der Verbrechern, die ein komfortables Leben mit einem fremden Mann oder eine gut bezahlte Job im Ausland versprechen.

Nach der Information aus dem Außenministerium der Vereinigten Staaten übertragen sich von 700 Tausend bis 2 Millionen Frauen und Kinder Tausend jährlich, im Rahmen Trafik durch der Grenze. Vertretern von FBI glauben, dass etwa 200 russische organisierte kriminelle Gruppen Kontakte mit Gruppen in den USA unterhalten und die meisten von ihnen mit dem Schema der Sextrafik verbunden sind. In Zusammenarbeit mit der organisierten Kriminalität tauschen sich solche Ehe-Agenturen mit Fragebögen der Kunden, Information über ihnen und auch Information über Weisen von ungehinderten Export von Waren, die Anwesenheit von korrupten Beamten aus.

Noch eines der profitablen kriminellen Unternehmen, der sich mit Hilfe Internet-Ressourcen verwirklicht, ist Porno-Industrie. Wahrscheinlich hat sich jeder Benutzer mindestens einmal mit der Werbung solches Inhalts getroffen. Das globale Netzwerk kann mehr als 4 Millionen Porno-Seiten zeigen und die Anfrage «Porno» schreiben laut der Statistik von «Yandex» etwa 4,5 Millionen pro Monat. Nach verschiedenen Erhebungen bringt Porno-Industrie den Gewinn von 15 bis 25 Milliarden von US-Dollar. Einnahmen aus dem Verkauf von Pornos sind im russischen Internet etwa 250-300 Millionen US-Dollar.

So sehen wie, dass Internet wirklich einer der Mittel von Entwicklung und Wohlstand des kriminellen Unternehmens. Organisierte kriminelle Gruppen benutzen aktiv Internet-Ressourcen für die Verbesserung der Bedingungen von Drogenhandel, Waffenhandel, Porno-Unternehmen, Kinderhandel. Häufig wendet eine kriminelle Gruppe gleichzeitig alle möglichen Wege von Erhaltung des Profites durch globales Netzwerk an. Versuche vom Überwinden dieser Probleme führen sich über viele Jahre durch. Daran zeugen auch die internationalen Verträge (z.B. Übereinkommen gegen die grenzüberschreitende organisierte Kriminalität des Jahres 2000, Konvention vom Europarat über Bekämpfung des Menschenhandels des Jahres 2005), und Verbesserung der Bundesgesetzgebung. Es lohnt sich aber immer zu erinnern, dass die Entwicklung der Technologien, die Entstehung neuer Arten der Gewinnerzielung durch kriminellen Weg immer vor der entsprechenden Reaktion des Gesetzgebers wird. Deshalb muss man nicht nur internationale Zusammenarbeit in entsprechendem Bereich entwickeln, sondern auch die Kriminalpolitik von möglichen kriminellen Handlungen im Internet durchführen zu versuchen, und auch hoch qualifizierte Strafverfolgungsbehörden haben. Für die Bekämpfung des illegalen Drogenhandels im Internet und Verbreitung der Porno-Produktion muss man dem Netz zensieren: Filter auf bestimmte Wörter beim Provider verwenden, Information an Webseiten aktiv nachverfolge, bei Platzierung der Information an Websei-

ten mit Abwesenheit der zuverlässigen Angaben über ihren Besitzer verweigern. Außerdem muss man die Entwicklung des kriminellen Unternehmens wie auch andere Problemen komplex lösen. Als Indikativ gilt auch, dass die Wohlstand des Frauenhandels auch in sozialer und ökonomischer Entwicklung wurzelt, wegen deren bei ihnen den Lust wegzufahren erscheint.

Серова В.Е.
Россия, Санкт-Петербург,
СПб ЮИ (ф) АГП РФ

ИНТЕРНЕТ КАК ИСТОЧНИК ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ПО ДЕЛАМ О НЕЗАКОННОМ ОБОРОТЕ ОРУЖИЯ

Интернет-ресурсы нередко являются источниками информации о преступлениях, в частности, связанных с незаконным оборотом оружия. В сети Интернет преступники договариваются о сделках, ищут коммерческих партнёров, демонстрируют свои действия по подбору оружия и непосредственно действия с оружием и т.д. Указанные сведения могут поступать в правоохранительные органы различными путями и из различных источников, и при надлежащем процессуальном оформлении могут выступать как в качестве поводов и основания для возбуждения уголовного дела, так и в качестве доказательств по делу.

Интернет-сеть, выступая одним из источников получения информации о совершении преступлений, связанных с незаконным оборотом оружия, определяет дальнейшие формы деятельности по проверке этих сведений.

Прежде всего, информация о размещении в сети Интернет сведений, связанных с незаконным оборотом оружия, может быть получена оперативными сотрудниками специальных подразделений органов МВД и ФСБ Российской Федерации в рамках оперативно-розыскной деятельности. В таком случае документирование должно осуществляться по правилам, определяемым ведомственными правовыми актами. Например, оперативным сотрудником составляется соответствующий рапорт. После возбуждения уголовного дела материалы, полученные оперативным путём, подлежат следственному осмотру, при необходимости могут быть назначены судебные экспертизы (программно-техническая, видео-фоноскопическая и др.). Кроме того, следователь и сам имеет возможность получить информацию непосредственно из Интернета, например, путём осмотра сайта или страницы в соци-

альной сети, на которых размещена имеющая значение для дела информация.

В ряде случаев информация о факте совершения действий, связанных с незаконным оборотом оружия, и об отражении этой информации в сети Интернет может поступить от граждан, представителей общественных организаций и должностных лиц государственных органов. Если указанные лица сами проявляют инициативу по информированию правоохранительных органов, они обращаются либо в оперативно-розыскной орган, либо и в орган предварительного расследования. Порядок оформления такого сообщения предполагает, в первом случае, составление оперативно-служебных документов и последующую оперативную проверку поступившей информации, во втором случае – документирование в рамках уголовно-процессуальной деятельности и проведение проверки сообщения о преступлении, регламентированной ст.ст. 140, 144, 145 УПК РФ. Причём после получения как устного, так и письменного заявления необходимо опросить заявителя. Наряду с этим известные им сведения указанные лица могут сообщить в ходе допросов по уже возбуждённым уголовным делам. В этом случае следователь должен подробно выяснить у них адрес соответствующего Интернет-ресурса, дату обращения, не копировались ли эти данные на компьютер допрашиваемого лица. В дальнейшем указанные данные подлежат проверке, в том числе путём осмотра компьютера и Интернет-ресурса.

Для выявления и раскрытия преступлений данного вида могут проводиться не только следственные действия, но и оперативно-розыскные мероприятия (ОРМ) (опрос, наведение справок, исследование предметов и документов, наблюдение, оперативное внедрение, снятие информации с технических каналов связи и др.). Однако следует помнить, что любые данные, полученные в ходе ОРД, в дальнейшем должны проверяться процессуальным путём.

Опрос – оперативно-розыскное мероприятие по сбору информации в процессе непосредственной беседы сотрудника оперативного подразделения (лица, действующего по его поручению) с любыми лицами, которые могут сообщить сведения о лицах, фактах и обстоятельствах, представляющих оперативный интерес для решения задач оперативно-розыскной деятельности (ОРД). При выявлении фактов незаконного оборота оружия целесообразно проводить опрос лиц, разместивших в сети Интернет данную информацию, лиц, которым была известна данная информация (например, ограниченный список Интернет-друзей, для которых эта запись является открытой, лица, создав-

шего сайт и поддерживающего его функционирование, администраторов и модераторов сайта. Опрос может быть проведён как в гласной, так и негласной форме, с зашифровкой и без зашифровки его цели, а также при необходимости с легендированным прикрытием сотрудника оперативного подразделения и лица, действующего по его поручению или заданию. В дальнейшем опрошенные лица должны быть допрошены в качестве свидетелей. В ходе допроса выясняют те же обстоятельства, по которым проводился опрос.

С целью установления лиц, причастных к организации сайта, содержащего информацию о незаконном обороте оружия, выяснения технических условий его функционирования и обновлений допустимо использовать наведение справок. Это ОРМ по сбору информации, представляющей интерес для решения задач ОРД, осуществляемое путём направления запросов и изучения представленных документов, а также информации, полученной в иной форме. Порядок взаимодействия органов связи и уполномоченных государственных органов установлен в Правилах взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность. Согласно п.п.12 и 14 этих Правил на операторов связи возлагается обязанность по предоставлению круглосуточного доступа уполномоченным органам к базам данных об абонентах и о расчётах за оказание услуг связи, в т.ч. о соединениях, трафике и платежах абонентов.

Исследование предметов и документов – ОРМ, направленное на изучение предметов и документов, которые сохранили или могли сохранить на себе следы преступления, являлись или могли являться орудием совершения преступления или результатом преступной деятельности, в целях выявления следов и орудий совершения преступления и результатов преступной деятельности. В качестве предмета исследования может выступать материальный носитель информации о факте, субъекте незаконного оборота оружия и т.д., зафиксированных техническим способом, в качестве документа – распечатка с технического носителя информации. После возбуждения уголовного дела указанные лица подлежат опросу, при необходимости назначаются судебные экспертизы.

Наблюдение – ОРМ, направленное на получение информации об объекте оперативной заинтересованности путём визуального, слухового, электронного радиолокационного и иных способов контроля. В ходе наблюдения могут быть решены следующие частные задачи: выявление и техническая фиксация сайта, содержащего информацию о

незаконном обороте оружия; получение сведений о преступнике либо преступной группе, распределении ролей, функциях каждого участника, характере их взаимоотношений; добывание информации об элементах оперативной обстановки, а также данных, необходимых для планирования других ОРМ и следственных действий.

Оперативное внедрение – ОРМ, основанное на легендированном вводе сотрудников оперативного подразделения либо лиц, оказывающих им содействие, в криминальную среду («объекты оперативного внедрения») в целях разведывательного сбора информации, необходимой для решения задач ОРД по борьбе с преступностью, нейтрализации и разобщения членов преступной группы. При этом составляются следующие документы: мотивированный рапорт о наличии законных оснований для проведения ОРМ с информацией о предполагаемом объекте и субъекте внедрения; постановление о проведении оперативного внедрения, утверждённое руководителем оперативно-розыскного органа; план оперативного внедрения; задание (поручение) субъекту внедрения; легенда; иные документы.

Для получения информации об обновлениях сайта, участниках гостевой книги, форумах, дискуссиях и помещаемых материалах может быть применено снятие информации с технических каналов связи – ОРМ, связанное с получением информации, имеющей значение для решения задач противодействия преступности, передаваемой по незащищённым техническим каналам связи, либо содержащейся в компьютерных и иных технических системах. Результаты снятия информации с технических каналов связи оформляются справкой или рапортом (при проведении ОРМ лично сотрудником оперативного подразделения); сводкой, справкой, актом или иными установленными документами (при проведении ОРМ с использованием штатных негласных сотрудников подразделений оперативно-технических мероприятий и оперативных подразделений радиоэлектронной безопасности оперативно-розыскных органов); агентурным сообщением (если снятие информации осуществляется при содействии лиц, оказывающих конфиденциальное содействие); актом (при зашифрованном гласном снятии информации с участием других лиц и специалистов).

Сотрудники органов, осуществлявших названные мероприятия, в дальнейшем допрашиваются об обстоятельствах проведения ОРМ и полученных результатах.

Serova W.
Russland, St. Petersburg,
St. Petersburger Rechtsinstitut (Niederlassung) der Akademie der Generalstaatsanwaltschaft der Russischen Föderation

Internet als Quelle der Beweisinformation von Strafsachen über illegalen Waffenhandel

Häufig sind Internet-Ressourcen die Informationsquellen von Verbrechen, insbesondere, die mit illegalem Waffenhandel verbunden sind. Im Internet verhandeln die Verbrecher über Abmachungen, suchen nach Handelspartnern, demonstrieren ihre Handlungen die Auswahl der Waffen und direkte Aktionen mit Waffen usw. Die oben genannte Information kann bei verschiedenen Wegen und aus verschiedenen Quellen in Strafverfolgungsbehörden kommen und können auch bei ihren richtigen prozessualen Ausfertigung wie als Weise oder Grund für Strafsachenwirkung und auch als Beweismittel nach einer Strafsache handeln.

Internet, als eine der Quellen Informationserhaltung über Verbrechen, die mit illegalem Waffenhandel verbunden sind, herauskommend, bestimmt weitere Form der Überprüfung dieser Information.

Vor allem kann die Information über Platzierung im Internet von Angaben, die mit illegalem Waffenhandel verbunden sind, durch operative Mitarbeiter spezieller Einheiten des Innenministeriums oder Bundesagentur für Sicherheit der Russischen Föderation in Rahmen der operativen suchenden Tätigkeit erhaltet werden. In solchen Fall muss die Dokumentation nach den Regeln von bei Abteilungen festgelegenen rechtlichen Vorschriften durchgeführt werden. Zum Beispiel, wird ein entsprechender Bericht bei einem Operationsoffizier erstellt. Nach der Strafsachenwirkung unterliegen Materialien, die durch operativen Weg erhaltet sind, der Untersuchung und, wenn es notwendig ist, können gerichtliche Expertise zugeordnet werden (programmierte-technologische, video-phonoskopische und andere). Außerdem hat der Untersuchungsführer eine Möglichkeit von Erhaltung der Information direkt aus Internet, zum Beispiel durch Untersuchen der Webseite oder der Seite in einem sozialen Netzwerk, wo sich die für eine Strafsache wichtige Information platziert.

In einigen Fälle kann die Information über Faktum des Handlungen, die mit Waffenhandel verbunden sind, und über die Spiegelung dieser Information im Internet von Bürgern, Vertretern der gesellschaftlichen Organisationen und Beamten der staatlichen Behörden eintreten. Wenn die genannten Personen selbst die Initiative ergreifen, um der Strafverfolgung zu informieren, sprechen sie darüber mit der operativen suchenden Behörde

oder mit Voruntersuchungsbehörde an. Die Reihenfolge der Eintragung solcher Meldung übernimmt im ersten Fall die Ausarbeitung von operativen dienstlichen Dokumenten und anschließende operative Kontrolle der erhaltenen Information und in zweiten Fall – die Dokumentierung in Rahmen strafprozessualler Tätigkeit und die Prüfung der Meldung über Verbrechen, die in Art. 140, 144, 145 des Strafprozessgesetzbuches der Russischen Föderation festgelegt ist. Nach der Erhaltung wie mündlicher und auch schriftlicher Bewerbung ist es notwendig den Bewerber umzufragen. Daneben können diese Personen die ihnen bekannte Information während der Vernehmung von schon eingeleiteten Strafsachen berichten. In diesem Fall muss der Untersuchungsführer bei ihnen detailliert Adresse von entsprechender Internet-Ressource, das Datum des Ansprechens klarstellen und auch ob diese Information auf Computer des vernehmenden Personen kopiert worden sind. Weiter sind die genannte Information der Prüfung einschließlich durch der Untersuchung der Computer und der Internet-Ressource unterworfen.

Für Identifizierung und Lösung dieses Artes von Verbrechen können nicht nur Untersuchengen sondern auch operative suchende Maßnahmen (OSM) durchgeführt werden (Umfrage, Einziehen der Erkundigungen, Forschung der Sachen und Dokumenten, Besichtigung, operative Implementierung, Entfernung der Information von technischen Kommunikationskanälen und andere). Aber muss man erinnern, dass jede Information, die von operativer suchender Tätigkeit gesammelt ist, weiter durch prozessualen Weg überprüfen soll.

Umfrage ist die operative suchende Maßnahme um Informationssammlung in den Prozess der direkten Gespräche des Mitarbeiters von operativen Einheiten (des in seinem Namen handelnden Personen) mit solchen Personen, die Angaben über Personen, Fakten und Umstände, die für operative Tätigkeit Interesse für die Aufgabenlösung schafft, berichten können. Bei der Identifizierung der Fakten von illegalem Waffenhandel ist nützlich die Umfrage der Personen durchzuführen, die diese Information wissen (z.B., begrenzte Liste von Internet-Freunden, für deren diese Schreibung der Person, der diesem Webseite besitzt und die Funktionierung unterstützt, und auch der Administratoren und Moderatoren, offen ist). Die Umfrage kann wie in offener so auch in verdeckter Form, mit der Kodierung oder ohne der Kodierung, und auch, mit wenn es notwendig ist, mit legendierter Abschirmung des Mitarbeiters operativen Einheiten und des Personen, der in seinem Namen oder nach der Aufgabe handelt, durchgeführt werden. Weiter müssen die umgefragte Personen als Zeugen vernommen werden. Während

der Vernehmung identifiziert man dieselben Umstände, nach denen die Umfrage durchgesetzt worden sind.

Einziehen der Erkundigungen ist zur Benutzung zulässig, wenn die Feststellung der Personen, die zur Organisation von Webseite, die Information über illegalen Waffenhandel enthaltet, und die Bestimmung von technischen Bedingungen ihrer Funktionierung als Ziel dient. Diese operative suchende Maßnahme um die Sammlung der Information, die Interesse für operative Tätigkeit für die Aufgabenlösung schafft, die sich durch Anfragensenden und Analyse der vorgelegten Dokumente und auch durch anderem Weg bekommende Information verwirklicht. Die Reihenfolge der Wechselwirkung von Kommunikationsbehörden und autorisierten staatlichen Behörden ist in Regelung der Wechselwirkung Operatoren mit den staatlichen Behörden, die sich mit operativer suchender Tätigkeit beschäftigen, festgelegt. Laut Punkten 12 und 14 dieser Regelung sind die Operatoren der Kommunikation verpflichtet, um die um die Uhr Zugang der autorisierten Behörde zu autorisierten Personen auf die Datenbank des Abonnenten und über Auszahlungen für Kommunikationsdienstleistungen einschließlich über Verbindungen, Trafik und Zahlungsbedingungen der Abonnenten zu gewähren.

Forschung der Sachen und Dokumenten ist die operative suchende Maßnahme, die nach der Analyse von Sachen und Dokumenten einrichtet ist, die Spuren des Verbrechens speichern oder speichern könnten, und, die Instrument der Straftat oder die Folge von strafbarer Handlung waren oder sein könnte, um diese Spuren zu erkennen. Als Gegenstand der Forschung kann Materialträger von Information über die Tatsache, den Subjekt des illegalen Waffenhandels hervorstehen, die durch technische Mittel wie das Dokument aufgezeichnet ist – Drucken aus Materialträger der Information. Nach dem Strafsachenwirkung sind diese Personen der Umfrage unterlagen werden sind und wenn es notwendig ist, wird man gerichtliche Expertisen ernannt.

Besichtigung ist die operative suchende Maßnahme, die nach der Erhaltung der Information vom Objekt der operativen Interesse durch visuellen, akustischen, elektronischen radio-lokalisierten Methoden von Kontrolle einrichtet ist. Während der Besichtigung können folgende Aufgaben gelöst werden: Ermittlung und technische Festlegung der Seite, der Information über illegalen Waffenhandel enthaltet; Erhaltung der Information über den Verbrecher oder kriminelle Gruppe, über die Verteilung der Rollen und Funktionen von jedem Teilnehmer, über die Natur ihrer Beziehung; Gewinnung von Informationen über die Elemente der operativen Situation und

auch über Information, die für Planung anderer operativen suchenden Maßnahmen und Untersuchungsaktionen notwendig sind.

Operative Implementierung ist die operative suchende Maßnahme, die auf legendierten Eingang der Mitarbeiter der operativen Einheit oder ihnen unterstützenden Personen in kriminellen Umfeld («Objekten der operativen Implementierung»), um Intelligenzen Information, zu sammeln, die für Aufgabenlösung der operativen suchende Tätigkeit notwendig ist, und um Mitgliedern der kriminellen Gruppen zu neutralisieren und abzutrennen. Dabei wird folgende Dokumente vorbereitet: motivierte Bericht über Anwesenheit der legalen Grunde für Durchführung der operativen, suchende Maßnahme mit Information über angenommenen Objekt oder Subjekt der Implementierung; Entscheidung über Durchführung der operativen Implementierung, die bei der Leiter der operative suchende Behörde genehmigt; Plan der operativen Implementierung; die Aufgabe (Order) für den Subjekt der Implementierung; Legende; andere Dokumente.

Für die Enthaltung der Information über Aktualisierung der Webseiten, Teilnehmer an den Gastbücher, Foren, Diskussionen und gestellte Materialen kann die Entfernung von Information aus technischen Kommunikationskanäle eingesetzt werden – die operative suchende Maßnahme, die mit dem Bekommen der Information, die für Aufgabenlösung von Bekämpfung der Kriminalität, die nach ungeschützterer technischer die Kommunikationskanäle oder in Computer-und Techniksystemen enthaltende Information. Ergebnisse der Entfernung der Information aus technischer Kommunikationskanäle fertigen mit dem Zeugnis oder Bericht (während der operativen suchende Maßnahme bei dem Mitarbeiter der operativen Einheiten persönlich durchgeführt ist); bei zusammenfassendem Zeugnis, Akt oder einem anderen festgelegten Dokument (während der operativen suchende Maßnahme mit der Benutzung von festangestellten heimlichen Mitarbeitern der Einheiten der operativen technischen Maßnahme von radio-elektronischer Sicherheit der operativen suchenden Behörde); beim Agenturbericht (wenn die Entfernung der Information bei der konfidentiellen Mitwirkung); beim Akt (bei verschlüsselter öffentlicher der Information Entfernung mit anderen Personen und Fachleuten).

Die Mitarbeiter der Behörde, die diese Maßnahmen verwirklichen, werden über Umstände von der Durchführung der operativen suchenden Maßnahmen und der bekommene Ergebnisse vernehmen.

Суховаров Ю.
Россия, Санкт-Петербург,
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации. Северо-Западный институт управления

ИСПОЛЬЗОВАНИЕ ИНТЕРНЕТ ТЕХНОЛОГИЙ В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

1. Стремительное развитие современных информационных технологий поставило перед правоохранительными органами новые сложные и постоянно изменяющиеся проблемы. Сегодня, наряду с традиционными направлениями деятельности, следователям и оперативным работникам приходится сталкиваться с новыми видами преступлений, связанных с использованием компьютеров, чему, безусловно, способствует широкое внедрение компьютерных технологий на основе использования локальных и глобальных информационных сетей.

2. В процессе расследования преступлений новые информационные технологии эффективно применяются для проведения допросов, опознаний и других следственных действий путём видеосвязи и т.п.

3. В настоящее время использование видеотрансляций в ходе следственных действий признаётся приемлемым методом получения доказательств, одна из сфер использования данной технологии – дела, связанные с организованной преступностью. По этой категории дел свидетели данных преступлений порой отказываются давать показания из-за вполне обоснованных опасений за свою жизнь. Дистанционные (прежде всего видео) показания эффективно решают проблемы защиты свидетелей от давления и запугивания. Видеосвязь также всё больше применяется при получении показаний свидетелей, живущих за границей, которые по каким-либо причинам уклоняются от явки в суд по месту жительства.

4. Выявление Интернет мошенников по их IP-адресам (по IP-адресу можно узнать страну, регион, город, в некоторых случаях даже улицу).

5. Выявление нарушений на выборах при помощи WEB-камер и Интернета.

6. Использование GPS систем, связанных с Интернетом. Предотвращение угона и помощь в поиске угнанных машин (камеры на автомагистралях).

7. Создание в России Интернет-полиции для борьбы с киберпреступностью.

8. Создание веб-сайтов правоохранительных органов (например, сайт МВД).

Suchowarow Jurij
Der Russischen Akademie der Volkswirtschaft und Staatliches Dienstes unter dem Präsidenten der Russischen Föderation. Nordwestliches Institut der Unternehmensführung

Die Verwendung von Internet-Technologien in der Verbrechensbekämpfung

1. Die rasante Entwicklung der modernen Informationstechnologie hat den Strafverfolgungsbehörden neue schwere und sich immer verändernde Probleme gesetzt. Neben den traditionellen Richtungen von Aktivitäten stoßen Untersuchungsführer und operative Mitarbeiter heute mit neuen Arten der Straftaten, die mit Benutzung des Computers zusammen. Dazu trägt, unbedingt, breite Einführung von Computer-Technologie durch die Verwendung von lokalen und globalen Informationsnetzen.

2. Während der Untersuchung der Verbrechen verwendet man effektiv neue Technologien für Vernehmung, Erkennung und andere Untersuchungsmaßnahmen durch Video usw.

3. Zurzeit gilt die Verwendung der Videokonferenzen während der Untersuchung als annehmbares Methode zum Bekommen der Beweismitteln und eine der Gebieten von der Benutzung dieser Technologie sind Strafsachen, die mit organisierten Kriminalität verbunden sind. Manchmal verweigern Zeugen nach dieser Kategorie der Strafsachen die Zeugeneinvernahme geben wegen der wohlbegründeten Furcht um ihr Leben. Fernzeugeneinvernahme (insbesondere Video) lösen effektiv die Schutzprobleme von Druck und Einschüchterung der Zeugen. Videokonferenzen benutzen immer mehr beim Bekommen der Einvernahme der Zeugen, die im Ausland leben und nach irgendeinem Grund weichen von Gerichtstermin nach Wohnort.

4. Die Identifizierung der Internet-Betrügereien auf ihrer IP-Adresse (nach IP-Adresse kann man das Land, den Region, die Stadt, in einige Fälle sogar die Straße).

5. Aufdeckung von Verstößen während der Wahlen mit Hilfe der WEB-Kameras und des Internets.

6. Verwendung von GPS-Systemen, die mit Internet verbunden sind; Verhindern von Diebstahl und Hilfe bei der Suche nach gestohlenen Autos (камеры на автомагистралях).

7. Schaffung in Russland einer Internet-Polizei für Bekämpfung der Cyberkriminalität.

8. Schaffung von Webseiten der Strafverfolgungsbehörden (z-B-der Webseite des Innenministeriums).

Казымова А.А. кызы
Россия, Санкт-Петербург,
Санкт-Петербургского Инженерно-экономического Университета

ЗАКЛЮЧЕНИЕ ДОГОВОРА ЧЕРЕЗ ИНТЕРНЕТ

Когда речь идёт о заключении договора, мы, прежде всего, имеем в виду получение акцепта на оферту. Так, офертой является выражением намерения заключить договор. Оферта должна содержать существенные условия договора (напр., предмет или цену). Одной из форм выражения намерения к заключению договора является публичная оферта, которая особенно распространена в электронной коммерции. Публичность оферты означает, что каждый, кто хочет принять оферту, может стать акцептантом по договору, т.е. оферент должен заключить договор с любым, кто отзовется.

При формировании публичной оферты информация о продукте (о предмете, цене, количестве, условиях покупки и доставки) определяется вследствие акцепта покупателя, который тоже имеет определённую форму. Это всё необходимо должно быть указано в тексте публичной оферты. Назначение товара, его индивидуальные качества, технические инструкции, срок хранения, гарантийный срок и прочая информация размещается в разделах, в которых эти товары предлагаются. Такую информацию целесообразнее указывать в самой оферте. Но описывать правила покупки на определённые товары в опубликованной оферте автор не считает необходимым, достаточно лишь разместить в ней соответствующую ссылку на выделенный для этого специальный раздел на сайте под названием «правовая информация».

Во время пользования интернетом простой обыватель может с первого взгляда не заметить разницу между публичной офертой и рекламой. Реклама – это лишь приглашение делать оферту (ст. 437 ч. 1 Гражданского кодекса Российской Федерации – далее «ГК РФ»). Согласно Федеральному Закону РФ от 13.03.2006 «О рекламе» реклама – это «информация, распространённая любым способом, в любой форме и с использованием любых средств, адресованная неопределённому кругу лиц и направленная на привлечение внимания к объекту рекла-

мирования, формирование или поддержание интереса к нему и его продвижение на рынке». Так, мы видим важнейшую разницу: реклама – это приглашение к оферте, которое вообще может не содержать существенных условий будущего договора. Главной целью рекламы является придание товару известности и узнаваемости. А в публичной оферте к тому же не только точно разъяснены условия приобретения товара, но и порядок предъявления претензий и условий возврата покупки.

Также очень важно, в какой форме заключается договор. Ст. 434 ГК РФ называет способы, при которых договор признается заключённым в письменной форме. К одному из таких способов она относит заключение договора с использованием электронной связи. Ч. 3 ст. 160 ГК устанавливает требования к письменной форме сделки: Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон. Единственным законом в России, регулирующий использование аналогов собственноручной подписи является ФЗ от 6.04.2011 «Об электронной подписи» (№ 63-ФЗ). Некоторые считают, что этот закон является большим шагом с точки зрения соответствия техническому развитию правового состояния государства. Другие довольно консервативны и полагают, что новый закон, как и предыдущий, не будет эффективным. Действительно, предыдущий закон от 10.01.2003 имел много правовых пробелов. Было не ясно, в каких сферах можно использовать электронную цифровую подпись. Сфера была определена следующим положением: «Использование электронной цифровой подписи распространяется на отношения, возникающие из гражданско-правовых сделок, и в других случаях, предусмотренных законодательством Российской Федерации». Согласно новому закону эти отношения абсолютно точно регламентированы. Однако в новом законе тоже имеются некоторые недостатки. Он по-прежнему предусматривает применение простой электронной подписи только в случаях, предусмотренных законом, правовыми актами и соглашениями сторон (в отличие от «усиленной» и «квалифицированной» электронной подписи). И остаётся по-прежнему вопрос о том, в какой форме может быть совершено соглашение о возможности сделки в электронной форме. Также интересно, что же это за нормативный акт, который, в соответствии с п. 2 ст. 6 Закона, определяет случаи, когда допускается использование простой электронной

подписи. Сам этот закон не определяет такие случаи, – он определяет лишь правовой режим такой подписи.

Также в качестве недостатка противники заключения договора с использованием электронных подписей находят, что это очень сложная и непонятная большинству граждан процедура, поскольку не все разбираются в её технологических особенностях. Но всё же это ведь не обязанность каждого заключать договоры с помощью электронной подписи. Это лишь альтернатива.

Существуют и другие споры по данному вопросу, но если в праве нет споров, то не следует ожидать его развития. И это относится к исследуемой теме в целом. Россия за последние 10 лет пережила так называемую «электронную революцию» и необходимо развиваться дальше, чтобы иди в ногу со временем, как и другие развитые страны.

Kasimowa A.
Russland, St. Petersburg,
Der Sankt-Petersburgen Ingenieuren und Ökonomischen Universität

Der Vertragsabschluss im Internet

Wenn die Rede über den Vertragsschluss geht, meinen wir vor allem die Erhaltung der Annahme eines Angebots. So ist das Angebot eine Willenserklärung, die auf den Abschluss eines Vertrags gerichtet ist. Das Angebot muss erhebliche Bedingungen des Vertrags enthalten (z.B., der Gegenstand, der Preis). Es gibt solche Form des Willenerklärungsangebot wie ein öffentliches Angebot, der in elektronischem Kommerz besonders verbreitet ist. Die Öffentlichkeit des Angebots bedeutet, dass jeder, der diesen Angebot akzeptieren will, kann Annehmer sein.

Bei der Schaffung des öffentlichen Angebots bildet sich die Information über ein Produkt (der Preis, die Anzahl, die Verkaufs- und Lieferbedingungen) aus Käufersannahme, der sich an bestimmterer Form gründet. Dieser Punkt muss man im Angebotstext beschreiben. Funktionen der Ware, ihre individuelle Eigenschaften, technische Vorschriften, Haltbarkeit- Gewährleistungsfristen und auch andere individuelle Information platziert direkt in Abschnitten, in denen diese Waren angeboten werden. Es ist ratsam solche Information im Angebot anzuzeigen, aber es wird nützlicher im Annahmestext sie zu veröffentlichen. Aber findet der Verfasser des Artikels keine Notwendigkeit die Verkaufsregeln für bestimmtere Waren im öffentlichen Angebot beschreiben, weil es darin nur entsprechende Link mit dem

Begriff «Die Rechtliche Information» in besonderem Abschnitt von Website genug ist.

Aber wenn ein Benutzer im Internet surft, kann er mit erstem Augenblick nicht den Unterschied zwischen dem öffentlichen Angebot und der Werbung bemerken. Die Werbung ist nur eine Einladung zum Angebot (Art. 437 Abs. 1 Bürgerliches Gesetzbuch Russischer Föderation – weiter «BGRF»). Laut dem russischen Bundesgesetz von 13.03.2006 «Über die Werbung» ist die Werbung «die Information, die mit irgendeinen Wegen, in irgendeiner Form, mit der Benutzung irgendeine Mittel verbreitet ist, zum unbestimmteren Kreis der Menschen adressiert ist, und an die Anziehung der Aufmerksamkeit zum Objekt der Werbung, an die Schaffung oder die Unterhaltung der Interesse für dieses Objekt, an seine Promotion auf dem Markt gerichtet ist». So sehen wir die wichtigste Unterschiede: die Werbung ist die Einladung zum Angebot, der nicht alle oder überhaupt keine erhebliche Bedingungen des zukünftigen Vertrags hat. Der Hauptziel der Werbung ist die Ware nur bekannt machen. So sind im öffentlichen Angebot nicht nur die Kaufsregeln genau zu erklärt, sondern auch Anspruch- und Zurückgebungsregeln.

Es ist auch sehr wichtig, in welcher Form der Vertrag geschlossen wird. Der Art. 434 BGRF nennt die Weisen, mit deren der Vertrag in schriftlicher Form als ein geschlossener Vertrag erkennt. Zu eine der Weise gehört er den Vertragsschluss durch elektronische Kommunikation. Abs. 3 Art. 160 stellt die Forderung zur schriftlichen Abmachung auf: die Benutzung bei der Abmachung einer faksimile Wiedergabe der Unterschrift durch mechanische oder einen anderen Kopierensmittel, der elektronischen digitalen Unterschrift oder ein anderes Analogen von handschriftlichem Unterschrift ist in solchen Fällen und Weisen erlaubt, die durch Gesetz oder durch eine Vereinbarung von Parteien vorausgesetzt ist. Das einzige Gesetz in Russland, das die Benutzung des Analogen von handschriftlicher Unterschrift reguliert, ist das Bundesgesetz von 6.04.2011 «Über die elektronische Unterschrift». Einige meinen, dass dieses Gesetz ein großer Schritt in technologischer Seite des Rechts ist. Andere haben konservative Meinung und glauben, dass neues Gesetz wie das voriges nicht effektiv wird. Wirklich, das Voriges Gesetz von 10.01.2002 war hätte viele rechtliche Lochen. Es war nicht klar, in welchen Gebieten konnte man die elektronische digitale Unterschrift benutzen. So war es geschrieben: «Die Benutzung der elektronischen digitalen Unterschrift ist an die Beziehungen verbreitet, die aus bürgerrechtlichen Abmachungen und aus anderen durch die Gesetzgebung der Russischen Föderation vorgeschriebenen Fällen entstehen». Aber im neuen Gesetz gibt es auch einige Nachteile. Laut neuem Gesetz diese Be-

ziehungen sind ganz klar beschrieben. Dieses Gesetz konsolidiert ebenso die Benutzung von eine einfache elektronische Unterschrift nur in Fälle, die bei den Gesetzen, rechtlichen Vorschriften und der Vereinbarung von Seiten vorgeschrieben sind (im Gegensatz den «verstärkten» und «qualifizierten» Unterschriften). Und trotzdem bleibt die Frage, in welcher Form diese Vereinbarung über die Möglichkeit der Abmachung in elektronischer Form kann sein Es ist auch interessant was für ein normative Akt, der laut dem Art. 6 des Gesetzes bestimmt die Fälle, wenn die Benutzung von einfacher elektronischer Unterschrift zulässig ist. Dieses Gesetz bestimmt solche Fälle nicht – es erklärt nur das rechtliche Regime solcher Unterschrift.

Auch als eine Nachteil sehen die Gegnern elektronischen Vertragsabschluss mit solchen Unterschriften, dass er sehr schwere und nicht klare für meisten Menschen Prozedur hat, weil nicht alle technologische Besonderheiten verstehen. Aber doch ist es nicht die Pflicht die Vertrag durch die elektronische Unterschriften abschließen. Das ist nur alternativ.

So es gibt auch anderer Streit dazu aber, wenn das Recht ohne Streiten ist, muss man auf keine Entwicklung warten. Und das gehört zum erforschteten Thema in Ganzem. Russland erlebt etwa 10 Jahre eine elektronische Revolution, und es ist notwendig noch weiter zu gehen, um wie andere entwickelte Länder auf der Höhe der Zeit zu sein.

Выдрыган А.Ф.
Россия, Москва,
РПА МЮ РФ

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОПРИМЕНЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В условиях модернизации законодательства в сфере компьютерной информации, Интернет-технологий, возникает проблема определения единой для всех дисциплин терминологии. Так, сформулированные термины, помимо отражённых понятий, должны быть признаны как в технической, так и в юридической науках.

Следует отметить, что сеть Интернет – не единственная глобальная сеть, и на основе компьютерной техники создаются также иные технологии. Чтобы отделить Интернет-преступность от других видов правонарушений, нам необходимо выделить особенности сети Интернет не только как технологии, но и как социально-информационного и субкультурного явления. Преступность в сети Интернет является частью компьютерной преступности.

Т.П. Кесареева выделяет преступления в сети Интернет как преступления, совершённые путём вхождения в сеть Интернет. Но, поскольку вхождение в сеть, исходя из физических параметров человека, невозможно, в действительности происходит взаимодействие компьютерной техники и компьютерных сетей посредством принципов и алгоритмов, задокументированных в протоколах IP, TCP и других. Поэтому, следует выделить Интернет-преступления как новый вид общественно опасных деяний, выбрав критериями выделения способы или средства совершения преступлений.

Проведённый «пилотный» анализ используемых в юридической литературе определений позволяет считать Интернет-преступлениями любые запрещённые уголовным законом общественно опасные деяния, совершённые посредством или с помощью ресурсов Интернет. Сюда входят преступления, когда ресурсы Интернета используются и на стадии приготовления к совершению преступления. Так, например, поиск средств компьютерного взлома банковских карт по сети Интернет следует признавать Интернет-преступлением, хотя необходимо различать интенсивность использования данного ресурса в случае, когда Интернет является лишь средством совершения преступления или выступает в качестве способа.

Определив используемые понятия Интернет-преступления и Интернет-преступности, представляется возможным выделить их отличительные характеристики. Так, Интернет-преступление характеризуется следующими свойствами: удалённость, неперсонифицированность, доступность. Интернет-преступность, в свою очередь, отличают крайне высокая латентность, интеллектуальность, транснациональность, быстрый рост. При этом Дремлюга Р.И. выделяет в качестве подвида такую наиболее опасную и качественно новую преступность, как совокупность преступлений, где Интернет является способом совершения преступлений, то есть используется непосредственно для совершения общественно опасного деяния.

Хотя в УК РФ термина «компьютерное преступление» нет, в законе используется понятие «компьютерная информация». Так, под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. В ходе реформы в Уголовный кодекс РФ были внесены изменения, в том числе и в главу 28 «Преступления в сфере компьютерной информации». Список преступлений в данной сфере расширился. Факультативные признаки субъективной и объективной стороны становятся обязательными для некото-

рых новых составов преступлений. К таким признакам относятся, например, мотив в виде корыстной заинтересованности (ч. 2 ст. 272 УК РФ), последствия в виде крупного ущерба. Но объект Интернет-преступления не всегда относится исключительно к преступлениям в сфере компьютерной информации, он может относиться и к другому родовому и видовому объекту, охраняемому законом.

Исходя из поправок в УК РФ следует сделать вывод о том, что любое преступление в Интернете является компьютерным преступлением, но не любое компьютерное преступление относится к Интернет-преступлениям.

Исследуем данные утверждения на примере статистики Интернет-мошенничеств. Так, если в 1999 году было зарегистрировано лишь 148 случаев мошенничества (ст. 159 УК РФ), совершённого с использованием компьютерных и телекоммуникационных технологий, то спустя десять лет в суд было передано 2799 уголовных дел. В 2010 году наблюдался значительный прирост мошенничества, связанного с использованием глобальной сети Интернет и средств мобильной связи. За 2010 год в связи с данными преступлениями по ст. 159 УК РФ («Мошенничество») было возбуждено 6762 уголовных дел, направлено в суд – 3751. Из всей совокупности преступлений, совершённых с использованием компьютерных технологий (зарегистрировано в 2010 году 11636 преступлений), доля мошенничества составляет – 58 %, в 2011 году количество преступлений снизилось в несколько раз и составило 3256, из них направлены в суд – 2231 уголовное дело. Уровень мошенничеств остается неизменным.

В качестве типичного примера компьютерного преступления можно привести извлечение из приговора Басманного районного суда города Москвы от 6 мая 2011 года, установившего, что в августе 2010 года, граждане РФ Б., Д., и К. вступили в предварительный сговор с неустановленными лицами на неправомерный доступ к охраняемой законом банковской тайне путём незаконного копирования данных о ПИН-кодах и реквизитах банковских карт с помощью использования специальных устройств, заведомо приводящих к несанкционированному копированию информации, сборе сведений, составляющих банковскую тайну, незаконным способом, и квалифицировавшего действия подсудимых по ч. 2 ст. 272 УК РФ и по ч. 1 ст. 183 УК РФ. Из данного примера видно, что понятие компьютерных преступлений шире, чем преступления в сети Интернет. В соответствии с последними изменениями УК РФ вышеупомянутый состав преступления подвергся криминализационным преобразованиям, что, безусловно, по-

может в борьбе не только с преступностью, но и с её латентной составляющей.

Как представляется, использование возможностей Интернет для совершения преступлений выводит часть из них в категорию транснациональных (например, мошеннические действия по хищению денежных средств со счетов зарубежных банков, независимо от страны нахождения преступника), а также позволяет характеризовать такого рода преступления как значительно более сложные с точки зрения их выявления, с одной стороны, а с другой – позволяющей преступникам совершать масштабные преступные акции, использующие ресурсы Интернет, как специфическое орудие совершения преступления. Поэтому представляется возможным в рамках затронутых в данной статье вопросов рассмотреть предложение о включении в ч.1 ст.63 УК РФ такого отягчающего уголовную ответственность обстоятельства, как совершение преступления с использованием Интернет-технологий.

Widrigan A.
Russland, Moskau
Russischen Rechtliche Akademie Ministerium der Justiz der Russischen Föderation

Aktuelle Probleme der Durchsetzung im Bereich der Computerinformation

In Bezug auf die Modernisierung der Gesetzgebung im Bereich Computerinformation, Internet-Technologien entsteht das Problem der Bestimmung einer gemeinsamen Terminologie für alle Disziplinen. So müssen formulierte Definitionen neben den gegebenen Bestimmungen als die technischen und gesetzlichen Wissenschaften anerkannt werden.

Es ist zu beachten, dass das Internet nicht nur weltweites Netzwerk ist und basierend auf Computertechnik entstehen auch andere Technologien. Um Internet-Kriminalität von anderen Arten der Unrechtshandlung zu trennen, brauchen wir die Besonderheit vom Internet nicht nur als Technologie sondern auch soziale informative und subkulturelle Veranstaltungen zu markieren. Die Kriminalität im Internet ist einer der Teilen von der Computerkriminalität. Kesarejeva T. unterscheidet die Kriminalität im Internet als ein Verbrechen durch ein Eingang im Internetnetzwerk. Aber da der Eingang im Netzwerk beziehend auf physikalischen Parameter der Mensch unmöglich ist, passiert die Wechselwirkung von Computertechnik und Computernetzen tatsächlich durch die Prinzipien und Algorithmen, die in

den Aufzeichnungen der IP, TCP und andere Aufzeichnungen dokumentiert sind. Deshalb, muss man Internet-Verbrechen als eine neue Art der sozial gefährlichen Handlungen auswählend Kriterien der Verteilung die Methoden und Mitteln der Begehung von Verbrechen.

Durchgeführte «Pilotanalyse» von in juristischer Literatur verwendete Begriffe lasst für Internet-Verbrechen alle unter das Strafrecht verbotenen sozial gefährlichen Handlungen halten, die mit Hilfe oder durch Internet-Ressourcen gemacht sind. Dazu gehören die Straftaten, wenn die Ressourcen vom Internet auch auf der Stufe der Vorbereitung zur Begehung des Verbrechens genutzt wird. So, zum Beispiel, muss man Suche nach Computer-Hacking der Kreditkarten über das Internet als Internet-Verbrechen erkennen, obwohl man Intensität der Nutzung dieser Ressource vergleichen muss, wenn Internet nur die Mittel oder Methode der Begehung des Verbrechens ist.

Wenn man verwendete Definitionen des Internet-Verbrechens und der Internet-Kriminalität bestimmt werden, wird es möglich ihre Merkmale zu markieren. So charakterisiert sich das Internet-Verbrechen durch die folgenden Eigenschaften: Abgelegenheit, Unpersonifizierenheit, Verfügbarkeit. Die Internet-Kriminalität unterscheidet ihrerseits eine sehr hohe Latenz, Intelligenz, Transnationalität, das schnelle Wachstum. Dabei verteilt Dremljuga A. als eine der gefährlichsten und qualitativ neuen Unterart der Kriminalität wie eine Menge von Straftaten, wo das Internet ein Weg der Begehung von Verbrechen ist, nämlich benutzt sich direkt für die Begehung einer sozial gefährlichen Handlung.

Obwohl es im Strafgesetzbuch der Russischen Föderation kein Begriff «Computer-Straftat» gibt, verwendet sich im Gesetz die Definition «Computer-Information». So versteht man unter der Computer-Information die Information (Berichte, Angaben), die in der Form von elektrischen Signalen unabhängig von ihrer mittels Speicherung, Verarbeitung und Übertragung dargestellt ist. Im Laufe der Reformen im Strafgesetzbuch wurde einige Änderungen auch in die Kapitel 28 «Straftaten im Bereich der Computer-Information eingeführt». Die Liste der Straftaten in diesem Bereich hat sich erweitert. Fakultative Merkmale des subjektiven und objektiven Tatbestandes werden für einige neue Straftatbestände obligatorisch. Zu solchen Merkmalen gehören, zum Beispiel, Motiv in Form von eigennützigen Interessen (Art. 272 des Strafgesetzbuches der Russischen Föderation) und die Folgen als ein größerer Schaden. Aber das Objekt des Internet-Verbrechens gehört ausschließlich zu Straftaten im Bereich der Computer-Information nicht immer, es kann auch zum anderen generischen und spezifischen Objekt gehören, das durch das Gesetz geschützt ist.

Basierend auf den Änderungen im Strafgesetzbuch der Russischer Föderation muss man eine Schlussfolgerung machen, dass jedes Verbrechen im Internet ist ein Computerverbrechen, aber nicht jeder Computerverbrechen gehört zu Internet-Verbrechen.

Erforschen wir diese Behauptungen auf Beispiel von der Statistik des Internet-Betrugs. So wurde im Jahre 1999 nur 148 Fälle der Betruge registriert (Art. 159 des Strafgesetzes der Russischen Föderation), die mit Benutzung der Computer- und Telekommunikationstechnologien begangen waren, und nach zehn Jahren wurde 2799 Strafsachen zum Gericht übertragen. Im Jahre 2010 wurde es ein erheblicher Anstieg der Betrugsfälle, die mit der Verwendung des globalen Netzwerk Internet und Mobilfunk. Während des Jahres 2010 wurde 6762 Strafsachen im Bezug dieser Verbrechen nach dem Artikel 159 des Strafgesetzbuches der Russischen Föderation («der Betrug») entstanden, und wurde 3751 davon an Gericht verweist. Aus ganzer Menge der Straftaten, die mit Benutzung der Computer-Technologien begangen werden sind (im Jahre 2010 – 11636 Straftaten), ist der Anteil des Betrugs 58%; 2011 sank der Zahl der Verbrechen um mehrmals und wurde 3256, und 2231 Strafsachen davon wurden an Gericht verweist. Die Höhe des Betrugs bleibt unverändert.

Als typischen Beispiel von Computerverbrechen kann man bei der Entfernung des Urteils von Basmannij Bezirksgericht in Moskau am 6. Mai 2011 führen, das errichtet hat, dass Bürger B., D. und K. am August des Jahres 2010 in eine vorläufige Vereinbarung mit unidentifizierter Personen auf den unbefugten Zugriff auf die bei dem Gesetzt geschütztenen Bankgeheimnis durch illegalem Kopieren von Daten über PIN-Codes und Angaben von Bankkarten durch der Benutzung der speziellen Geräten eintraten, die sicherlich auf die unberechtigte Vervielfältigung, das Sammeln der Information, die Bankgeheimnis bilden, durch illegale Weise führen. Das Gericht qualifizierte die Handlungen der Angeklagten nach dem Teil 2 des Artikels 272 und Teil 1 des Artikels 183 vom Strafgesetzbuch der Russischen Föderation. Aus diesem Beispiel ist es klar, dass die Definition der Computerverbrechen breiter als der Verbrechen, die sich im Internet begehen. Laut der letzten Änderungen des Strafgesetzbuches der Russischen Föderation wurde der oben genannte Strafbestand kriminalisierten Veränderungen durchgemacht, und das hilft unbedingt in der Bekämpfung nicht nur mit der Kriminalität sondern auch mit ihrem latentem Komponente.

Wie es vorausgesetzt wird, führt die Verwendung der Möglichkeit vom Internet für die Begehung der Straftaten einen Teil daraus in einer Kategorie von transnationalen Verbrechen hinaus (z.B. Betrugshandlungen um dem Geldstehlen von den Konten ausländischer Banken, unabhängig von

dem Land, wo sich der Täter befindet), und auch ermöglicht sie diese Art von Kriminalität einerseits als sehr viel komplexer in ihrer Identifizierung zu charakterisieren und andererseits – groß angelegte kriminelle Aktionen den Verbrechern zu begehen, die Internet-Ressourcen wie ein spezifischer Instrument zum Verbrechen benutzen. Deshalb glaube ich möglich den Angebot über der Einbeziehung im Teil 1 vom Artikel 63 des Strafgesetzbuches der Russischen Föderation in Rahmen der angesprochenen in diesem Beitrag Probleme solcher erschwerenden Umstände der strafrechtlichen Verantwortlichkeit wie die Begehung der Straftat mit Benutzung der Internet-Technologien zu betrachten.

Содержание

Составление и перевод:
доцент кафедры трудового права и охраны труда
юридического факультета
Санкт-Петербургского университета управления и экономики
Кабанов Андрей Александрович,
кандидат юридических наук, доцент,
e-mail: ***akabanov@inbox.ru;***
студентка 4 курса
Санкт-Петербургского Инженерно-экономического университета
Казымова Амина Айдын кызы
e-mail: ***aminka.92@mail.ru***

Под общ. ред. А.А. Кабанова.

Правовое регулирование в сети «Интернет»

Сборник статей
на русском и немецком языках

Печатается в авторской редакции

Подписано в печать и свет 29.10.2012. Формат 60×84 1/16
Печать офсетная Объём 3,3 п.л. Тираж 50 экз.

Отпечатано в ООО «Копи-Р Групп»
190000, Санкт-Петербург, пер. Гривцова, д. 6