Институт государства и права

Российской Академии наук

Научное исследование

“ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ”

Научный сотрудник сектора уголовного права и криминологии ИГП РАН, кандидат юридических наук

Клебанов Л.Р.

“THE PROTECTION OF CONFIDENTIAL INFORMATION RESOURCES FROM THE INFLUENCE OF ORGANIZED CRIME AND CORRUPTION”

Research fellow of the sector of criminal law and criminology of ISL RAN, candidate of law science

Klebanov L.R.

Москва

2001

The present study deals with the problem of influence of organized criminality and corruption on confidential information resources. In order to estimate a degree of danger of this influence one must understand the role of information, including confidential one, in the modern life in Russia. It is to be noted that significance of the information may not be overestimated. Global computer nets ensnare the world, computer (on-line) economy became a pant of the world economy at all, no achievements in any sphere of activity couldn't be achieve without information supporting. Taking into account all aforesaid it is to be emphasized that under this circumstances confidential information must be protected especially. Transition to the now democratic society demands increasing a transparency of the Russian state and society. But from the other side, confidential information resources must be defended from various threats, including, first of all, influence of organized criminality and corruption. Holding the confidential information and controlling over information flows allow to organized criminality to control Russian economy, to commute new crimes using information technologies, to active successfully against law enforcement agencies and etc. Illicit access to the confidential information resources in many cases is impossible without helping from the side of corrupted officials. Illegal disclosure of confidential information is one of the form of corruption.

The present study consists of three chapters. The first chapter includes three paragraphs which tell about social danger of negative influence of organized criminality and corruption, kinds of it, determinants of it. The second chapter also consists of three paragraphs which deal with countermeasures against this influence, including law, technical and organization methods of protection. The last chapter gives information covering forecasting of new kinds and trends of this negative influence.

ПЛАН

Стр.

1. ОБЩЕСТВЕННАЯ ОПАСНОСТЬ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ НА КОНФИДЕНЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ 3

1.1. Организованная преступность и корррупция как источники угроз безопасности конфиденциальных информационных ресурсов 3

1.2. Виды воздействия организованной преступности и коррупции на конфиденциальные информационные ресурсы 20

1.3. Причины и условия воздействия организованной преступности и коррупции на конфиденциальные информационные ресурсы 31

2. СРЕДСТВА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ 34

2.1. Правовые средства защиты 34

2.2. Организационные средства защиты 37

2.3. Технические средства защиты 40

3. ПРОГНОЗИРОВАНИЕ НОВЫХ ВИДОВ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ НА КОНФИДЕНЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ 41

ЛИТЕРАТУРА 44

1. ОБЩЕСТВЕННАЯ ОПАСНОСТЬ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ НА КОНФИДЕНЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ

1.1. Организованная преступность и коррупция как источники угроз безопасности конфиденциальных информационных ресурсов

Общеизвестно, что на современном этапе развития человечества информация играет неоценимую роль, предоставляя уникальные возможности для развития личности, общества и государства. В частности, это актуально для информации, обеспечивающей развитие экономических отношений, – информационные ресурсы уже стали весьма ценным товаром, сопоставимым по стоимости с финансовыми, трудовыми, природными и иными ресурсами. Уже невозможно представить себе деятельность крупных корпораций, банков, промышленных предприятий без внутренней инфраструктуры на базе информационных технологий[1]. Мировое сообщество в XXI веке будет развиваться в направлении глобализации информационного пространства. Роль и место государств в мировой цивилизации будут зависеть не столько от природных богатств и численности населения, сколько от технологического уровня национальных экономик, информационных ресурсов и услуг. Глобализация информационного пространства, возникновение и развитие бурными темпами электронной экономики, основанной на сфере высоких технологий, обусловили подписание “Окинавской хартии глобального информационного общества” во время саммита стран большой восьмерки на Окинаве в 2000 году. Общество XXI века уже называют обществом информационным, а основными его признаками являются:

---

[1] См. Выступление генерального директора ФАПСИ Матюхина В.Г. // Сборник материалов Всероссийской конференции “Информационная безопасность России в условиях глобального информационного общества” / Под общ. ред. А.В.Жукова. – М.: Бизнес + безопасность, 2001. – С. 9.

– наличие эффективной системы формирования необходимой обществу информации;

– эффективный доступ широких слоев населения к различным информационным ресурсам;

– высокий уровень автоматизации переработки информации во всех сферах жизнедеятельности общества;

– преобладание информационных технологий, использующих современные телекоммуникационные и компьютерные сети и системы, при формировании материальной и технологической базы общества[1].

Интеграция России в мировое экономическое и информационное пространство весьма остро ставит проблему информационной безопасности. Ее разрешение затрудняется пробелами нормативно-правового регулирования информационных отношений, недостаточной развитостью информационной инфраструктуры в регионах России, оттоком высокопрофессиональных кадров в области защиты информации из государственных структур, ангажированностью ряда центральных и региональных СМИ, попавших под влияние представителей олигархического капитализма или криминальных сообществ, и т.д.

Озабоченность высшего политического руководства России проблемами информационной безопасности обозначена в Доктрине информационной безопасности. Примечательно, что выступая на заседании Совета безопасности России, посвященном выработке Доктрины, Президент РФ В.В.Путин заметил, что в сфере информационной безопасности “важно определить национальные интересы, возможные угрозы и методы защиты от них”, предварительно подчеркнув, что “завтрашний день в мировой политике и экономике будут определять информационные ресурсы” и что “от решения проблем в этой сфере зависит и будущее нашей страны”. Особое внимание в Доктрине

---

[1] См.: Емельянов Г.В., Стрельцов А.А. Проблемы реализации Доктрины информационной безопасности Российской Федерации // “Информационная безопасность России...”. – С. 15.

уделено сохранности конфиденциальной информации как жизненно важной составляющей любых информационных отношений.

В настоящее время в России сформирована довольно обширная (хотя и во многом противоречивая) нормативно-правовая база, регулирующая отношения по поводу конфиденциальных информационных ресурсов.

Рассмотрим прежде основные понятия, которыми автор оперирует в настоящей работе.

Так, под **информацией** в российском законодательстве понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления[1]. (Такое определение содержится в Федеральном законе “Об информации, информатизации и защите информации”.) Следует заметить, что данный закон распространяет свое действие лишь на документированную информацию (документ), т.е. на зафиксированную на материальном носителе информацию, с реквизитами, позволяющими ее идентифицировать. Закон “Об информации, информатизации и защите информации” также вводит понятие “информационные ресурсы”, которые определяются как отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных), причем документирование информации является обязательным условием для включения в информационные ресурсы. Информационные ресурсы могут находиться в собственности уполномоченных субъектов (физических и юридических лиц, государственных органов, органов местного самоуправления и т.д.), а также выступать товаром, за исключением случаев, предусмотренных законодательством РФ[2]. Исходя из категорий доступа, установленных законом, информация (а следовательно и информационные

---

[1] См.: Статья 2 Федерального закона “Об информации, информатизации и защите информации” // Собрание законодательства РФ. – 1995. – № 8. – Ст. 609.

[2] См.: Статьи 4, 6 Федерального закона “Об информации, информатизации и защите информации”.

ресурсы) подразделяется на *открытую* и *с ограниченным доступом*, а последняя, в свою очередь, подразделяется на *информацию, отнесенную к государственной тайне*, и *конфиденциальную информацию*. Указом Президента РФ был утвержден “Перечень сведений конфиденциального характера”, куда вошли 1) Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в СМИ в установленных федеральными законами случаях; 2) Сведения, составляющие тайну следствия и судопроизводства; 3) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна); 4) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и т.д.); 5) Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен Гражданским кодексом и федеральными законами (коммерческая тайна); 6) Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации о них[1]. Однако данный перечень не является исчерпывающим и в ряде нормативно-правовых актов содержатся указания и на иные сведения конфиденциального характера, прямо в вышеупомянутом Перечне не указанные (налоговая тайна, банковская тайна, сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, производственная тайна и т.п.).

Как известно, преступные посягательства на конфиденциальные информационные ресурсы чреваты наступлением весьма негативных последствий для личности, общества, государства. Под угрозу в данном случае ставятся безопасность

---

[1] См.: Указ Президента РФ “Об утверждении перечня сведений конфиденциального характера” // СЗ РФ. – 1997. – № 10. – Ст. 1127.

личности, права и свободы человека и гражданина, законные интересы субъектов экономической деятельности, нормальная деятельность государственных органов и т.п.

В действующем уголовном законодательстве России содержится целый ряд норм, предусматривающих ответственность за посягательства на тот или иной вид информации, а отечественные криминологи уже рассматривают в рамках структуры преступности новую подсистему – преступность информационную. Последняя, в свою очередь, по мнению Н.Ф.Кузнецовой, сама состоит из двух подсистем: а) первая включает в себя преступления, посягающие на информационные правоотношения (посягательства на информационную безопасность государства, на интеллектуальную собственность, компьютерные преступления и т.п.); б) вторая охватывает корыстные преступления, средствами совершения которых являются информационные системы[1].

Прежде чем перейти к характеристике организованной преступности и коррупции как источников угроз безопасности конфиденциальных информационных ресурсов, следует определить само понятие такой безопасности применительно к рассматриваемой в работе проблеме. Под *безопасностью конфиденциальных информационных ресурсов автор понимает состояние защищенности данных ресурсов от угроз преступных посягательств. Под источниками угроз данным ресурсам* понимаются те, от кого исходит угроза совершения подобных преступных посягательств.

Насколько же опасны организованная преступность и коррупция для конфиденциальных информационных ресурсов? В Доктрине информационной безопасности напрямую названа “неблагоприятная криминогенная обстановка, сопровождающаяся тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к

---

[1] См.: Криминология: Учебник / Под ред. проф. Н.Ф.Кузнецовой, проф. Г.М.Миньковского. - М.: БЕК, 1998. – С. 95-96.

конфиденциальной информации, усиления влияния организованной преступности на жизнь общества...”[1].

Примечательно, что в ходе социологического опроса, проведенного автором в рамках исследования незаконных получения и разглашения сведений, составляющих коммерческую или банковскую тайну, при ответе на вопрос, от кого, по мнению опрашиваемых, исходит угроза совершения этого преступления, печальную “пальму первенства” (48 % опрошенных) респонденты отдали организованным преступным группировкам (ОПГ). Опрос проводился среди сотрудников правоохранительных органов, налоговой и таможенной служб, представителей бизнеса, сотрудников одного из ведущих охранно-детективных объединений, сотрудников служб безопасности ряда компаний, а коммерческая и банковская тайна, напомним, выступает в качестве вида конфиденциальной информации.

Сбор и передачу информации уже выделяют как обязательные признаки организованной преступности[2].

Чем же обусловлено определение организованной преступности и коррупции в качестве источников угроз безопасности конфиденциальным информационным ресурсам? Для этого необходимо определить уголовно-правовые и криминологические критерии организованного преступного поведения. Так, В.В.Лунеев справедливо отмечает, что “организованная преступность постоянно и целенаправленно ищет высокодоходные и малорискованные преступные деяния. Поэтому можно перечислить почти все преступления, предусмотренные в уголовных кодексах различных стран, совершение которых может стать делом организованных преступников: одни (торговля наркотиками, оружием...) как основная целевая деятельность, другие (убийства, террор...) как способ устранения конкурентов, третьи (подкуп, коррупция...) как форма

---

[1] См.: Доктрина информационной безопасности Российской Федерации // Российская газета. – 28.09.2000.

[2] См.: Пристанская О.В. // Организованная преступность. Проблемы, дискуссии, предложения. “Круглый стол” / Отв. ред. А.И.Долгова, С.В.Дьяков. – М., 1989. – С. 150.

самозащиты от разоблачения, четвертые (неуплата налогов, отмывание денег...) как спасение преступного капитала, пятые (создание фиктивных предприятий...) как метод легализации своей деятельности и т.д. и т.п. Определив совершение каких-либо преступлений своим основным делом, организованные преступники не могут объективно и субъективно остановиться перед любым другим деянием, дающим им шанс процветания, выживания или спасения”[1].

Исходя из вышеизложенного, можно с уверенностью утверждать, что контроль за субъектами экономической деятельности, над финансовыми потоками, успешное противодействие правоохранительным органам и органам судебным, тщательная подготовка, планирование и совершение различных преступлений немыслимы без активной разведывательной деятельности, без надлежащего информационного обеспечения.

Например, сведения, составляющие коммерческую, банковскую или налоговую тайну, могут быть использованы при совершении *корыстных и корыстно-насильственных преступлений*.

Так, преступная группировка, состоящая из уроженцев Грузии, которую возглавлял один из лидеров оргпреступности Я.Саркисянц (Бешеный), получив секретную информацию об условиях сделки, заключенной фирмой “Коммерс”, занимающейся операциями с недвижимостью, и о месте и времени хранения денег, полученных по сделке, совершила нападение на офис этой фирмы. При попытке вытащить железный сейф (где, кстати, денег не оказалось) преступники были задержаны[2].

По информации службы безопасности РАО “Газпром” дочерние предприятия концерна в регионах уже столкнулись с попытками организованных преступных

---

[1] См.: Лунеев В.В. Преступность XX века. Мировой криминологический анализ. – М.: Норма, 1999. – С. 285.

[2] См.: Борисов И. Поминальная молитва при свечах. Взяли Яшу Бешеного // Версия. – 1999. – № 27. – С. 14.

группировок прибегнуть к шантажу и вымогательству. Это стало возможным, в частности, в силу шпионской деятельности преступников, а также ввиду утечки информации по техническим каналам связи[1].

По данным управления службы налоговой полиции по Московской области, ОПГ, обладая информацией о размерах прибыли, полученной коммерческими структурами, вымогают у предпринимателей до 25–30 % их доходов в виде наличных денег[2].

Аналогичным образом действовала в Санкт-Петербурге группировка преступного авторитета по кличке “Пудель”. В состав его группировки входило оснащенное подразделение, занимавшееся сбором коммерческой информации с помощью технических средств. Прежде чем вымогать деньги с какой-либо фирмы, “Пудель” тщательно изучал ее финансовую деятельность и только потом требовал определенную сумму[3].

Еще пример – из международной деятельности российской организованной преступности. Перехватив факс-сообщение, направленное крупной фирмой США российским партнерам о времени и месте прибытия “груза большой ценности”, преступники этот груз выкрали (таково, во всяком случае, мнение частных детективов)[4].

Обладая конфиденциальными сведениями экономического характера (о доходах физических и юридических лиц, о размерах полученной прибыли и т.п.), организованные преступники могут взять тот или иной субъект экономической

---

[1] См.: Шахов А.В. Электронные взломщики – преступники под маской романтиков // Защита информации. – 1997. – № 1. – С. 88.

[2] См.: Куксин И.Н., Смирнов М.П. Проявление организованной преступности в сфере налогообложения и меры борьбы с ней // Организованная преступность–3 / Отв. ред. А.И.Долгова и С.В.Дьяков. – М.: Криминологическая Ассоциация, 1996. – С. 150.

[3] См.: Соколов А.В., Степанюк О.М. Шпионские штучки. Методы информационной защиты объектов и компьютерных сетей. – М., СПб., Полигон АСТ, 2000. – С. 30.

[4] См.: Андреев А. Нью-Йорк остается “шпионским гнездом” // Новости разведки и контрразведки. – 1994. – № 21-22. – С. 6.

деятельности под свой контроль, совершить в отношении него или его клиентов любое преступление и т.д.

Так, по словам И.Н.Куксина и М.П.Смирнова, “для установления контроля над предприятиями и втягивания их в сферу незаконной деятельности преступные группировки используют широкий набор средств, включая тонко организованную разведку в банках, в которых сосредотачиваются не только денежные средства, но и информация о доходах физических и юридических лиц”[1].

Например, в одном из московских банков был установлен факт утечки конфиденциальной информации. Впоследствии выяснилось, что информация “уходила” к одной из преступных группировок через агента этой ОПГ – скромную прилежную оператора ЭВМ. Как установили сотрудники охранно-детективного объединения “Аргус”, обеспечившего безопасность банка, ОПГ пыталась взять банк под свой контроль, и лишь умелые действия сотрудников “Аргуса” по нейтрализации агента предотвратили захват банка преступниками[2].

По данным МВД РФ, отечественная оргпреступность контролирует до 40 % частных предприятий, 60 % государственных предприятий, 50–80 % всех банков; 40 % всех выявленных и поставленных на оперативный учет ОПГ прикрывают свою деятельность различными легальными структурами. По приблизительным подсчетам, около 2/3 всей российской экономики находится под контролем у мафиозных кланов. Таких негативных для общества и государства результатов организованная преступность добилась благодаря, среди прочего, и использованию методов работы разведки в своих целях, в частности при получении конфиденциальной информации[3]. Ведь, с одной стороны, ОПГ представляют собой преступные деловые предприятия,

---

[1] См.: Куксин И.Н., Смирнов М.П. Вышеуказ. работа. – С. 150.

[2] См.: Левицкий Ю. “Аргус” не снимает “крыш” // Частный сыск, охрана, безопасность. – 1995. – № 9.

[3] Политика криминализируется, криминал политизируется (По материалам проекта Центра по международным и стратегическим исследованиям г. Вашингтона “Российская организованная преступность”) // Новости разведки и контрразведки. – 1997. – № 23. – С. 1-8; Геворгян Г. Преступные этнические формирования // Законность. – 1999. – № 9. – С. 36.

преследующие извлечение максимальной прибыли и сверхприбыли в минимально короткий срок, причем в некоторых международных документах организованную преступность обозначают “преступностью в форме бизнеса”[1] (а в любом бизнесе, в т.ч. и в преступном, информация – ключ к успеху). С другой же стороны, функционируют ОПГ по принципу спецслужб высочайшего класса[2]. Отсюда и прекрасно организованные разведывательно-информационные службы в их составе, оснащенные необходимой техникой. В настоящее время практически все российские ОПГ имеют в своем составе такие разведподразделения[3]. (О чем еще будет сказано ниже.)

Однако организованные преступники стремятся получить не только конфиденциальные сведения экономического характера. В сфере их интересов находятся сведения, составляющие, например, личную или семейную тайну лица. Поскольку организованная преступность находится в состоянии постоянного противоборства с правоохранительными органами и, следовательно, их интересуют *данные предварительного расследования (следственная тайна)*; *сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (тайна безопасности участников правосудия)*; *сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (тайна безопасности субъектов порядка управления)*; *сведения, связанные с интересами государственной службы и службы в органах местного самоуправления (должностная служебная тайна)*; *тайна, связанная с интересами службы в коммерческих и иных организациях (иная служебная тайна)*, и т.п.[4]

---

[1] См.: Лунеев В.В. Вышеуказ. работа. – С. 286.

[2] См.: Никифоров А.С. Что нам делать с организованной преступностью? // Изучение организованной преступности: российско-американский диалог. – М., 1997.

[3] См.: Организованная преступность–2 / Отв. ред. А.И.Долгова, С.В.Дьяков. – М.: Криминологическая Ассоциация, 1993. – С. 87, 100, 113, 119, 150.

[4] См.: Кибальник А.Г., Кузьмин С.В., Соломоненко И.Г. Тайна в уголовном праве. – Ставрополь: Ставропольсервисшкола, 2000. – С. 19.

Нередко возможности (и весьма широкие) для разведывательной и контрразведывательной работы у преступников существуют даже в исправительно-трудовых учреждениях, где технические средства для негласного получения информации (в частности, для контроля телефонных переговоров) позволяют им подслушивать разговоры с абонентами, находящимися вне исправительных учреждений. Это позволяет успешно противодействовать и администрации и конкурирующим группировкам осужденных. Разведки группировок в ИТУ используют также и агентурные методы получения информации, в частности, использование “двойных” агентов, работающих и на администрацию и на преступников.

Вот один из примеров[1]. Свердловским (тогда еще городу Екатеринбургу не было возвращено его историческое наименование) УВД был арестован преступный авторитет К. Накануне допроса в кабинете следователя побывал двойной агент, работавший и на милицию и на одну из группировок в ИТУ, разведку которой возглавлял авторитет Седой, и бросил в мусорную корзину подслушивающее радиопередающее устройство. Весь допрос был записан на магнитную пленку принимающего устройства, находящегося в стоявшей неподалеку от кабинета автомашине. После окончания допроса тот же агент вновь зашел в кабинет и сказал следователю, что ему необходимо, якобы, сообщить важную информацию, после чего незаметно изъял устройство из корзины[2].

Как уже упоминалось, организованную преступность интересуют, прежде всего, данные, характеризующие деятельность правоохранительных органов по нейтрализации ОПГ, данные следствия, информация о мерах безопасности участников уголовного процесса и т.п. Ради ее получения ОПГ используют все имеющиеся у них в арсенале средства и методы. Даже в служебном кабинете заместителя Генерального прокурора России, курировавшего расследование особо важных уголовных дел, была

---

[1] См.: Подлесских Г., Терешонок А. Воры в законе: бросок к власти. – М., 1994. – С. 109.

[2] См.: Подлесских Г., Терешонок А. Вышеуказ. работа. – С. 109-110.

обнаружена акустическая радиозакладка. По своим техническим характеристикам она позволяла транслировать разговоры, происходящие в кабинете, на расстоянии в несколько сот метров[1].

Мы уже не раз говорили о том, что те задачи на современном этапе, которые стоят перед организованной преступностью, и новые условия, в которых она действует, обуславливают и внутреннюю структуру организованных преступных группировок. Практически в каждой из них существует служба безопасности, разведки и контрразведки (о чем уже упоминалось).

Наиболее ярким примером может служить структура ОПГ братьев Ларионовых, действовавшей во Владивостоке в 1992–1993 гг. и обезвреженной в январе 1994 г. Эта группировка была создана, как полагает следствие, с одной стороны, для защиты коммерческих предприятий, принадлежавших братьям, с другой стороны – для завоевания экономического пространства не только во Владивостоке, но и в Приморском крае. На счету группировки значилось 18 убийств и 6 покушений на убийство. По своей структуре, технической оснащенности и профессиональной подготовке группировка напоминала хорошо отлаженную военную организацию. В структуру банды входили: 1. Начальник штаба. 2. Начальник службы безопасности. 3. Коммерческие структуры. 4. Службы боевого и хозяйственного обеспечения (содержание конспиративных квартир, добывание и хранение оружия). 5. Аналитический центр (анализ информации). 6. Спецназ (силовое воздействие, физическое устранение противников). 7. Разведка (сбор информации в криминальных и коммерческих структурах, органах государственной власти, вербовка агентов, подготовка убийств). 8. Контрразведка (выявление в группировке неблагонадежных и агентов). Группировка имела свой собственный архив, где содержалась документированная информация о ее деятельности, об обязательствах ее участников и т.д. Вот лишь одно извлечение из инструкции для начальника разведки: “Начальник

---

[1] См.: Практика уголовного сыска. Научно-практический сборник / Составитель А.Ваксян. Научн. ред. А.И.Алексеев. – М.: Лига разум, 1999. – С. 215.

разведки... осуществляет сбор и анализ информации по всем видам обстановки: а) статической: юридической, структурно-должностной, коммерческий, криминальной; б) динамической: коммерческая деятельность конкурентов; планируемые сроки, деятельность криминальных структур, отклонения от общепринятых норм поведения отдельных физических и должностных лиц". Группировка обладала широко разветвленной агентурной сетью и вербовала информаторов в коммерческих структурах, преступных группировках и в органах государственной власти. Агентурные сообщения касались в основном коммерческой деятельности фирм, их связей с японскими бизнесменами, заключенных и готовящихся к подписанию контрактов[1].

Аналогичную структуру, включая разведку и контрразведку, имела печально известная "слоновская" группировка, базировавшаяся в Рязани и обезвреженная недавно правоохранительными органами[2].

Хорошо организованные службы безопасности действуют и в составе чеченских группировок, орудующих в Москве. Их разведподразделения имеют коррумпированные связи среди сотрудников правоохранительных органов, получая от них информацию о возможных операциях против бандитов, а также ведут наблюдение за действиями возможных конкурентов[3].

Следует особо отметить, что посягают организованные преступники и на сведения, составляющие государственную тайну, в частности, на сведения о негласных оперативно-розыскных мероприятиях, о сотрудниках, внедренных в преступные организованные группы, о методах, планах негласных оперативно-розыскных мероприятиях и т.п. (Согласно Закону РФ "О государственной тайне"[4], Федеральному

---

[1] См.: Корольков И. Тень летучей мыши // Московские новости. – 2000. – № 51. – С. 8.

[2] См.: Беловецкий Д. "Слоновая" болезнь // Литературная газета; ч. 11. – 1998. – № 44. – С. 7.

[3] См.: Данн Г. Основные криминальные группировки современной России // Российская организованная преступность: новая угроза? / Под ред. Ф.Вильямса; пер. с англ. А.Гостева. – М.: Крон-Пресс, 2000. – С. 130.

[4] См.: Российская газета 21.09.93; Собрание законодательства РФ. – 1997. – № 41. – Ст. 4673.

закону “Об оперативно-розыскной деятельности в Российской Федерации”[1], Указу Президента “О Перечне сведения, отнесенных к государственной тайне”[2] вышеперечисленные сведения относятся к государственной тайне.) Так, при обыске на московской квартире одного преступного авторитета были обнаружены два документа. Один из них содержал перечень различных заведений, где собирались представители других преступных группировок и имелись возможности для получения информации с помощью технических средств. А вот в другом был также список аналогичных заведений (гостиниц, казино, ресторанов), на которых активно использовались оперативно-технические возможности городского уголовного розыска. Иными словами, те места, где хозяину квартиры и членам его группировки появляться не следовало[3].

В нынешних условиях правоохранительные органы вынуждены прибегать к активным мерам защиты от шпионажа со стороны ОПГ, поскольку доступ преступников к информации правоохранительных органов может повлечь самые печальные последствия.

Вот трагический пример из деятельности правоохранительных органов США. Через окно здания, расположенного на расстоянии 50 метров от объекта наблюдения, с использованием длиннофокусного объектива, были сделаны снимки документов, изобличающих в коррупции крупных американских чиновников. В момент съемки документы находились на столе одного из руководителей оперативной службы, занимавшейся их разработкой. Текст на фотографиях и документах читался без труда. Данный случай получил огласку, в результате чего погиб ценный агент – преступники инсценировали его самоубийство[4].

---

[1] См.: Собрание законодательства РФ. – 1995. – № 33. – Ст. 3349.

[2] См.: Собрание законодательства РФ. – 1995. – № 49. – Ст. 4775.

[3] См.: Практика уголовного сыска. – С. 216.

[4] См.: Практика уголовного сыска. – С. 219.

Воздействие организованной преступности на конфиденциальные информационные ресурсы было бы крайне затруднительным, а в ряде случаев и невозможным, без содействия коррумпированного чиновничества, обладающего конфиденциальной информацией в силу служебного положения.

Определений коррупции в юридической литературе предостаточно, и настоящая работа не ставит своей целью дать всеобъемлющее ее понятие.

В свете рассматриваемой проблемы следует, тем не менее, обратить внимание на Межамериканскую конвенцию против коррупции от 1996 г. Конвенция содержит статью, посвященную перспективам развития борьбы с коррупцией, которая носит характер рекомендации. Среди действий, которые государства-участники считают коррупционными преступлениями, особо выделено "*незаконное использование должностным лицом в интересах собственной выгоды иди выгоды третьей стороны любого вида закрытой информации, которой лицо обладает благодаря своему служебному положению*"[1] (курсив мой – Л.К.).

Как видим, Конвенция прямо называет вышеуказанное воздействие на конфиденциальные информационные ресурсы в качестве одного из проявлений коррупции.

В этой связи хотелось бы привести слова профессора В.В.Лунеева, сказанные им на конференции, посвященной предупреждению организованной и коррупционной преступности средствами различных отраслей права: "Государственному чиновнику нет нужды выходить с дубинкой на большую дорогу, он тысячекратно может обогатиться от продажи конфиденциальной информации".

По мнению ряда исследователей организованной преступности, "если ранее должностные лица передавали преступникам, в основном, информацию, касающуюся разведывательной или контрразведывательной деятельности, то в нынешних условиях стало наблюдаться предоставление предпринимателям конфиденциальной информации

---

[1] См.: Лукашук И.И., Наумов А.В. Международное уголовное право: Учебник. – М.: Спарк, 1999. – С. 195.

о других структурах в бизнесе”[1]. И такое предоставление конфиденциальной информации чиновниками (преступникам ли, предпринимателям или кому-либо еще) представляет собой опасную завуалированную форму коррупции, которая имеет самое широкое распространение в нашей стране[2].

В качестве иллюстрации можно привести пример с отставкой в 1997 г. небезызвестного Альфреда Коха с поста председателя Госкомимущества, который он в то время занимал. Причиной отставки стали обвинения в адрес Коха в том, что во время аукциона по продаже государственных акций телефонной компании “Связьинвест” он разгласил информацию Онексим-банку (участнику аукциона)[3].

По данным МВД, за 1997–1999 гг. вскрыто более 700 случаев связи правительственных чиновников с представителями организованной преступности[4]. По некоторым экспертным оценкам, организованные преступные группировки тратят от 30 до 50 % преступно нажитых средств на коррумпированные связи среди чиновников государственного аппарата, которые, по мнению тех же экспертов, оказывают содействие каждой десятой группировке[5]. Однако, по данным многих сотрудников МВД, почти *у каждой преступной группировки имеется свой источник информации в правоохранительных органах или во властных структурах*[6].

К сожалению, ситуация с сохранностью конфиденциальной информации во властных структурах во многом оставляет желать лучшего. Так, в Москве практически

---

[1] См.: Нургалиев Б.Н. Организованная преступная деятельность (уголовно-правовые, процессуальные и криминологические аспекты). – Караганда, 1997. – С. 66.

[2] См.: Углубление социального контроля преступности – одна из предпосылок решения социально-экономических проблем (материалы “круглого стола”) / Подготовил В.В.Лунеев // Государство и право. – 1999. – № 9. – С. 64.

[3] См.: Глинкина С.П. К вопросу о выборе стратегии экономических реформ и характере российской коррупции // Коррупция: политические, экономические, организационные и правовые проблемы / Под ред. В.В.Лунеева. – М.: Юрист, 2001. – С. 101.

[4] См.: Глинкина С.П. Вышеуказ. работа. – С. 99.

[5] См.: Бурмистров И.А. Коррупция: ее сущность и меры предупреждения // Коррупция: политические, экономические, организационные и правовые проблемы. – С. 231.

[6] См.: Воронин Ю. Криминальная революция в государстве: экономические и политические аспекты организованной преступности в России // Российская организованная преступность: новая угроза? – С. 107.

любой желающий, пользующийся, скажем, Интернетом, способен получить доступ к базам данных о политиках и их биографиях, о руководящем составе МВД, Налоговой полиции, Правительства, Прокуратуры, РАО “Газпром” с указанием соответствующих телефонов, о собственниках жилья, о получении заграничных паспортов, о лицах, находящихся в федеральном розыске, о регистрации в Москве жителей города и т.д.[1] Аналогичные базы данных можно приобрести на нескольких радиорынках и других торговых точках, реализующих компьютерные компакт-диски и прочее оборудование. Следует особо подчеркнуть, что эти базы, как правило, имеют официальное происхождение, формируются в государственных структурах и, более того, у подпольных дилеров регулярно появляются обновленные их версии. Без внутренней утечки информации из соответствующих государственных структур наладить такой “информационный бизнес” невозможно.

Как видно из всего вышеизложенного, негативное воздействие организованной преступности и коррупции действительно пагубно сказывается на правах и интересах физических и юридических лиц, нормальном характере экономической деятельности, социальной стабильности и общем успехе борьбы с оргпреступностью и коррупцией.

1.2. Виды воздействия организованной преступности и коррупции на конфиденциальные информационные ресурсы

Как следует из вышеперечисленного, негативное воздействие организованной преступности и коррупции заключается, прежде всего, в совершении организованными преступниками и коррумпированными чиновниками определенных преступлений. То есть тех, которые входят в структуру информационной преступности. А если быть совсем точным, то речь идет о преступлениях, входящих в т.н. первую подсистему

---

[1] См.: Гуськова Т. Купите базу данных о себе // Бизнес и безопасность в России. – 2001. – № 2. – С. 26-27.

информационной преступности (о которой уже упоминалось). Иными словами, негативное воздействие организованной преступности и коррупции заключается, в первую очередь, в совершении организованными преступниками и коррумпированными чиновниками преступлений, посягающих на совокупность общественных отношений, возникающих по поводу создания, распространения, преобразования и потребления конфиденциальной информации, а также в способах совершения таких преступлений.

К таким преступлениям необходимо отнести прежде всего следующие деяния: а) Нарушение неприкосновенности частной жизни, которое выражается в незаконном собирании или распространении сведений, составляющих личную или семейную тайну лица, причем квалифицирующим признаком считается совершение этих деяний лицом, с использованием своего служебного положения (ст. 137 УК РФ); б) Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений граждан (ч. 1 ст. 138 УК), совершение того же деяния с использованием специальных технических средств, предназначенных для негласного получения информации (ч. 2 ст. 138), а также незаконные производство, сбыт или приобретение в целях сбыта таких специальных технических средств (ч. 3 ст. 138); в) Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183). Следует подчеркнуть, что с 1 февраля 2002 г. эта статья начнет действовать в новой (измененной и дополненной) редакции: во-первых, перечень сведений, за незаконные получение, разглашение или использование которых предусмотрена уголовная ответственность, пополнился налоговой тайной; во-вторых, законом прямо устанавливается, что субъектом незаконных разглашения или использования является лицо, которому эти сведения доверены по службе или работе; в-третьих, состав теперь содержит квалифицирующие признаки; г) Разглашение данных предварительного расследования (ст. 310 УК); д) Разглашение сведений о мерах безопасности,

применяемых в отношении судьи и участников уголовного процесса (ст. 311 УК); е) Разглашение сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (ст. 320 УК); ж) Разглашение государственной тайны (ст. 283); е) Неправомерный доступ к компьютерной информации (ст. 272).

К сожалению, изучать рассматриваемую проблему на основе данных официальной статистики о вышеперечисленных деяниях крайне затруднительно по ряду причин. Тем не менее некоторые статистические данные по части вышеперечисленных преступлений следует, все же, привести.

Таблица 1

Преступления – ст. ст. УК РФ	Зарегистрировано преступлений в течение года				Выявлено лиц, совершивших преступления[1]			
Г о д ы	1997	1998	1999	2000	1997	1998	1999	2000
Нарушение неприкосновенности частной жизни (ст. 137)	6	17	17	21	5	2	13	8
Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138)	51	52	78	159	26	29	54	117
Незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183)	10	17	12	53	2	6	0	14
Разглашение данных предварительного								

расследования (ст. 310)	3	2	7	3	1	1	4	2
Неправомерный доступ к компьютерной информации (ст. 272)	21	54	206	584	1	17	35	130

[1] Указаны либо лица, которые совершили только данное преступление, либо – в случае совокупности преступлений данное преступление относится к числу наиболее тяжких из совершенных.

Данные по оставшимся из вышеперечисленных деяний мизерны, поэтому в таблице не приводятся.

На этом фоне представляется небезынтересным привести данные о количестве осужденных за преступления, перечисленные в таблице 1.

Таблица 2

Преступления – ст. ст. УК РФ	Число осужденных по основной статье				Число осужденных по дополнительной квалификации			
Г о д ы	1997	1998	1999	2000	1997	1998	1999	2000
Нарушение неприкосновенности частной жизни (ч. 1 ст. 137)	8	6	3	6	8	6	2	2
Те же деяния, совершенные лицом с использованием служебного положения (ч. 2 ст. 137)	0	1	0	0	1	0	1	1
Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ч. 1 ст. 138)	0	1	1	1	0	1	0	0

То же деяние, совершенные лицом с использованием служебного положения (ч. 2 ст. 138)	0	0	0	3	0	3	1	2
Незаконные производство, сбыт или приобретение специальных технических средств для нелегального получения информации (ч. 3 ст. 138)	7	6	22	22	0	0	0	0

Окончание таблицы 2

Преступления – ст. ст. УК РФ	Число осужденных по основной статье				Число осужденных по дополнительной квалификации			
Г о д ы	1997	1998	1999	2000	1997	1998	1999	2000
Незаконное собирание сведений, составляющих коммерческую или банковскую тайну (ч. 1 ст. 183)	1	0	2	2	1	2	0	0
Незаконные разглашение или использование таких сведений (ч. 2 ст. 183)	0	0	0	1	0	0	1	0
Разглашение данных предварительного расследования (ст. 310)	0	2	5	4	0	1	0	0
Неправомерный доступ к компьютерной информации								

(ч. 1 ст. 272)	0	2	4	5	0	0	2	5
То же деяние, совершенное группой лиц по предварительному сговору, организованной группой, либо лицом с использованием его служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети (ч. 2 ст. 272)	3	5	10	19	0	0	6	3

Учитывая, что воздействие ОПГ на конфиденциальные информационные ресурсы заключается, прежде всего, в незаконном получении конфиденциальной информации, представляется необходимым более подробно рассмотреть *способы* такого получения.

Так, в ходе уже упоминавшегося социологического опроса, посвященного изучению незаконных получения и разглашения сведений, составляющих коммерческую или банковскую тайну, наиболее “популярными” способами получения этих сведений, по мнению опрошенных, являются: а) Подкуп сотрудников из ключевых отделов фирмы – 55,7 % респондентов; б) Незаконное получение информации у государственных чиновников, имеющих интересующие сведения (работников правоохранительных органов, суда и т.д.) – 55,7 %; в) Получение информации с использованием технических средств (контроль телефонных переговоров и т.д.) – 51 %; г) Незаконный доступ к компьютерной информации – 51 %; д) Засылка агентов на фирму или в близкое окружение ведущих специалистов – 32 %.

Все вышеуказанные способы ОПГ используют в полном объеме для получения любого вида конфиденциальной информации. Например, *компьютерный шпионаж* давно используется преступными группировками как средство собирания необходимой

информации. Так, в ГУВД Москвы прямо заявляют о том, что “знания хакеров все чаще используют преступные группировки”, которых, в частности, особо интересует “взламывание” банковских тайн”[1]. По словам одного профессионального московского хакера, к его “коллегам по ремеслу” обращаются представители оргпреступности с просьбой оказать определенные услуги[2]. Хакеры, работающие на преступные группировки, даже разрабатывают специальные компьютерные программы с целью шпионажа[3].

Использование преступниками для получения сведений конфиденциального характера различных *специальных технических средств, предназначенных для негласного получения информации*, также весьма распространено, о чем уже упоминалось. Этому в немалой степени способствует широкий нелегальный оборот шпионской техники, производством которой занимаются целые подпольные цеха. Ее изготовлением занимаются также отдельные специалисты, как правило, ранее работавшие на оборонных предприятиях, предприятиях по производству электроники и т.д.

Так, сотрудники Управления ФСБ по Омской области задержали бывшего работника одного из омских оборонных предприятий, у которого было изъято 42 изделия для негласного получения информации. Желающих приобрести такие устройства оказалось немало[4].

Недавно на российском черном рынке спецтехники появилось уникальное подслушивающее устройство, разработанное для разведки России. Устройство вмонтировано в обычную сигарету: сгораемый источник питания прячется в сигаретном табаке, а сам микрофон монтируют в фильтре. Стоит закурить такую

---

[1] См.: Гришина Е. Хакеры воруют миллиардами // Аргументы и факты–Москва. – 1999. – № 20. – С. 3.

[2] См.: Компьютер с “черного хода” // Клиент. – 1999. – № 38.

[3] См.: Загайнов М. Война с преступностью. Вопросов пока больше, чем ответов // Новости разведки и контрразведки. – 1996. – № 5. – С. 12.

[4] См.: Федосенко В. “Жучки” от безработного // Российская газета. – 25.05.2000. – С. 8.

сигарету, и микрофон начнет передавать все происходящее на приемник. Стоимость такой сигареты-“жучка” на черном рынке – 500 долларов[1].

В Москве сотрудники управления по борьбе с преступлениями в сфере высоких технологий МВД РФ (управление “Р”, к сожалению, уже расформированное) задержали торговца уникальными подслушивающими устройствами, являющимися секретной разработкой одного из секретных НИИ. Это устройство под названием “Флай” позволяет подключаться практически к любому междугороднему каналу связи на территории бывшего СССР, через него выйти на интересующего абонента (пользователя местной городской телефонной сети) и прослушивать его переговоры. Особая ценность прибора в том, что его практически невозможно обнаружить. Об этом устройстве стало широко известно несколько лет назад, когда один из бывших сотрудников НИИ–разработчика выпустил брошюру, где указал необходимую информацию для изготовления прибора. Эта информация вызвала живой интерес, в том числе и у преступных группировок. В конечном итоге выпуск прослушивающих устройств был быстро налажен[2].

В настоящее время преступники активно применяют следующие группы специальных технических средств, предназначенных для негласного получения информации: средства наблюдения; средства подслушивания; средства фотографирования; средства звуко- и видеозаписи; средства съема информации с проводов, стен и окон. К таким средствам могут относиться: миниатюрные фотокамеры, вмонтированные в зажигалки, часы, пачки сигарет; малогабаритные микрофонные радиопередатчики (“радиозакладки”), закамуфлированные под предметы быта; стетоскопы - приборы, используемые для прослушивания переговоров через стены, потолки, полы; лазерные микрофоны, работа которых основана на использовании невидимых лазерных лучей, направляемых на окна подслушиваемых

---

[1] См.: Разведчиков заставят курить на благо России // Московский комсомолец. – 2000. – № 48. – С. 1.

[2] См.: Игорев А. Предпринимателя взяли за “Флай” // Коммерсантъ. – 14.02.2001. – С. 12.

помещений, автомобилей. Отраженный от окон луч несет на себе акустический сигнал, который затем поступает на обрабатывающее устройство и на наушники[1].

Как явствует из всего вышеизложенного, техническое оснащение ОПГ ни в чем не уступает соответствующему оснащению правоохранительных органов и спецслужб, и организованные преступники придают огромное значение техническому вооружению своих криминальных разведок. На техническое оснащение своей преступности деятельности ОПГ расходуют не менее *одной трети* преступных доходов. Известен случай, когда лидер одной из ОПГ, орудующей в Подмосковье, выложил три тысячи долларов за копию совершенно секретной инструкции КГБ СССР по установке специальной аппаратуры для прослушивания помещений[2].

При расследовании уголовного дела о вымогательстве у одного известного московского совместного предприятия было установлено, что преступники организовали прослушивание телефонных переговоров предприятия и службы безопасности. Использовались портативные устройства для съема информации с телефонных линий, которые весьма популярны у сотрудников ФБР США. Примечательно, что стоимость таких устройств достигает 200 тысяч долларов[3].

Одним из излюбленных приемов получения информации со стороны ОПГ является *использование завербованных сотрудников субъектов экономической деятельности в качестве информаторов*. По мнению специалистов, в 70–80 % случаев сведения, составляющие, к примеру, коммерческую тайну предприятия, добываются с помощью его сотрудников[4].

В России (и не только в России) материальная неудовлетворенность сотрудников, месть, зависть и иные причины толкают их на предательство корпоративных интересов,

---

[1] См.: Ярочкин В. Организованная преступность. Откуда исходит угроза. – М., 1995. – С. 49-63.

[2] См.: Практика уголовного сыска. – С. 215.

[3] См.: Олейников В.В. Делайте бизнес надежным и безопасным. – Рыбинск, 1997. – С. 161.

[4] См.: Криворучко С. Я знаю о Вас все // Бизнес и безопасность в России. – 1997. – № 1. – С. 28.

в том числе и на разглашение сведений конфиденциального характера. Зачастую вербуют даже представителей руководящего звена.

Например, управляющий филиалом Независимого Банка России регулярно информировал одну из преступных группировок Санкт-Петербурга о всех крупных вкладах, поступающих в филиал на депозитные и иные счета физических и юридических лиц, для того, чтобы преступники ставили таких клиентов банка к себе на учет[1].

Нередко для вербовки персонала того или иного предприятия или банка злоумышленники идут на прямо-таки иезуитские способы. Например, выходящую из магазина сотрудницу банка, нагруженную покупками, пробегающий мимо мальчишка толкает на мужчину, который идет женщине навстречу. Мужчина не успевает остановиться и наступает женщине на ногу, да к тому же и выбивает из ее рук покупки. Женщине больно, она рассержена, и смущенный мужчина бросается поднимать ее покупки. Пострадавшая от раздражения готова наброситься на своего невольного обидчика, она поднимает глаза и вдруг видит перед собой красавца с внешностью голливудской кинозвезды. Мужчина галантно извиняется, и дама, уже сменив гнев на милость, принимает извинения. А красавец, желая загладить свою вину, представляется художником, открывает свой дипломат и просит женщину принять маленький сувенир собственного изготовления. Он достает восемь одинаковых сувениров, каждый в упаковке определенного цвета, и предлагает даме выбрать наиболее понравившийся. Та смущена, отказывается, однако под воздействием его обаяния все же берет цветную коробку. Но мужчина не успокаивается и просит взять еще сувенир. Совершенно очарованная женщина выбирает один за другим семь цветов подряд. Дама и представить себе не может, что она в данной ситуации лишь изучаемый объект, а перед ней никакой не художник, а профессиональный актер либо прожженный мошенник. И что рядом незаметно стоит психолог или его ассистент и фиксируют порядок

---

[1] См.: Куксин И.Н., Смирнов М.П. Вышеуказ. работа. – С. 165.

выбранных ею цветов. Суть же разыгранного “спектакля” заключается в том, что сотрудницу банка подвергли т.н. тесту Люшера. Смысл данного теста в том, что порядок последовательного выбора цветов отражает устойчивые личностные черты тестируемого. После обработки результатов такого теста можно приступать к дальнейшей работе с объектом с целью его последующей вербовки[1].

Получение информации у чиновников государственных правоохранительных и контролирующих органов, которым в силу своих служебных обязанностей известны сведения конфиденциального характера, также “популярный” у ОПГ прием, о чем, в свою очередь, мы также упоминали.

Субъектами, обязанными хранить конфиденциальные сведения, могут быть сотрудники Центробанка России Счетной палаты, судьи, прокуроры, сотрудники налоговой службы, органов предварительного расследования[2] и все другие государственные служащие. Особое внимание следует уделить работе служб собственной безопасности правоохранительных органов, которые должны оперативно выявлять коррупционеров в своих рядах и пресекать их противоправную деятельность.

Особенно актуален вопрос “чистоты рядов” для тех подразделений, которые непосредственно осуществляют борьбу с организованной преступностью. Так, по данным известного московского журналиста А.Хинштейна, некоторые сотрудники Главного управления по борьбе с оргпреступностью МВД РФ передавали секретную информацию некоему М.Бекмурзаеву об оперативно-розыскных мероприятиях, проводимых в его отношении сотрудниками МУРа и ФСБ, о силах и средствах этих мероприятий. Причем вышеозначенный Бекмурзаев подозревается в прямой причастности к взрыву на Пушкинской площади, в результате которого погибли тринадцать человек[3].

---

[1] См.: Москвин В. Внутренняя защита банка // Бизнес и банки. – 1996. – № 24. – С. 12.

[2] См.: Петрухин И.Л. Личные тайны (Человек и власть). – М.: ИГП РАН, 1998. – С. 181.

[3] См.: Хинштейн А. Лицензия на террор // Московский комсомолец. – 3.11.2001.

Нередко чиновники-перевертыши входят сами в состав ОПГ и участвуют в совершаемых ими преступлениях. Так, Пленум Верховного Суда РФ в своем постановлении “О применении судами законодательства об ответственности за бандитизм” от 17.01.1997 г. разъяснил, что под совершением бандитизма с использованием своего служебного положения (ч. 3 ст. 209 УК РФ) следует понимать, в том числе, и *использование сведений, которыми лицо располагает в связи со своим служебным положением* (выделено мной – Л.К.), к примеру при подготовке или совершении бандой нападения[1].

Все чаще и чаще правоохранительные органы сталкиваются с агентурным проникновением в свои ряды, когда преступники внедряют агентов в правоохранительные структуры. Только в 1994 г. зафиксировано 134 попытки внедрения преступной агентуры в налоговые органы и органы налоговой полиции, а за 9 месяцев 1995 г. таких попыток было 118[2]. По данным заместителя министра внутренних дел РФ Е.Соловьева, выступавшего перед депутатами Государственной Думы по вопросу борьбы с коррупцией, в 2000 г. зафиксировано 820 попыток внедрения организованными преступными группировками своих людей в правоохранительные органы. За 9 месяцев 2001 г. таких случаев зафиксировано 510 (передача “Парламентский час” на телеканале РТР от 25.11.2001 г.).

Соответственно *внедрение своих агентов на предприятия, в кредитные организации и иные субъекты экономической деятельности* также является распространенным способом получения информации. Иногда его называют “инфильтрацией”[3]. Через таких агентов преступники не только получают информацию,

---

[1] См.: Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам. – М., 1997. – С. 555.

[2] См.: Куксин И.Н., Смирнов М.П. Вышеуказ. работа. – С. 166.

[3] См.: Макиенко А. Служба безопасности банка: информация и анализ // Экономическая и банковская безопасность (По материалам журнала “Частный сыск, охрана, безопасность”, с 1997 г. “Мир безопасности”). – М., 1998. – С. 19.

но и пытаются обеспечить агентам доступ к руководящим должностям, что впоследствии облегчает им захват таких субъектов экономической деятельности.

Как видим, способов воздействия на конфиденциальные информационные ресурсы со стороны оргпреступности и коррупции немало, и в будущем они должны стать предметом всестороннего изучения и анализа в целях выработки эффективных мер борьбы с ними.

1.3. Причины и условия воздействия организованной преступности и коррупции на конфиденциальные информационные ресурсы

Рассматривая причины и условия преступности как единый взаимосвязанный комплекс явлений, мы определяем эти причины и условия в качестве *криминогенных детерминант*[1]. Исходя из этого, приведем вначале основные криминогенные детерминанты, *способствующие* негативному воздействию организованной преступности и коррупции на конфиденциальные информационные ресурсы:

– неполнота и противоречия законодательной базы, регламентирующей отношения по поводу конфиденциальных информационных ресурсов;

– широкий, а до недавнего времени практически бесконтрольный, оборот специальной техники для негласного получения информации; (Дело дошло до того, что едва ли не в каждой коммерческой палатке можно было приобрести “шпионскую” аппаратуру[2]. И только после вступления в силу Федерального закона “Об оперативно-розыскной деятельности”, а также соответствующих Указа Президента и Постановления Правительства, регламентирующих оборот такой техники, ситуация несколько улучшилась, хотя и продолжает оставаться весьма сложной.)

---

[1] См.: Криминология: Учебник / Под ред. Н.Ф..Кузнецовой, Г.М.Миньковского – М.: БЕК, 1998. – С. 157.

[2] См.: Гладышев В. “Шпионская техника” доступна не каждому // Все о безопасности. – 1999. – № 1. – С. 154.

– коррумпированность чиновников, “торгующих” сведениями конфиденциального характера, которыми они располагают в силу своих служебных обязанностей;

– недостаточная подготовка сотрудников тех государственных органов, которые должны расследовать посягательства на конфиденциальные информационные ресурсы либо предотвращать их совершение; (Например, в ходе упоминавшегося уже социологического опроса на вопрос задачи, требовавшей элементарных правовых знаний законодательства о коммерческой тайне, ответили правильно лишь около 6 % опрошенных, причем в их числе не оказалось ни одного сотрудника милиции. А предварительное следствие по делам о преступлениях, предусмотренных ст. 183 УК, производится следователями органов внутренних дел. Эти данные опроса конечно же не могут претендовать на абсолютную точность, но пищу для размышлений все же дают.)

– неудовлетворительная деятельность служб безопасности субъектов экономической деятельности;

– незнание персоналом уполномоченных органов и организаций (в т.ч. и их руководством) основ информационной безопасности;

– халатное отношение сотрудников этих органов и организаций к обязанностям хранить конфиденциальные сведения, в результате чего происходит их “утечка”;

– неэффективная кадровая политика, в результате которой на работу в органы, организации, субъекты экономической деятельности принимаются “агенты-информаторы”;

– отток многих профессиональных сотрудников спецслужб и правоохранительных органов в разведслужбы криминальных структур; (Так, с 1991 г. по 1998 г. только из системы МВД ушли 1 600 000 сотрудников[1]. Лишь в 1998 г. из органов внутренних дел уволились 63 тысячи сотрудников, а по оперативным данным

---

[1] См.: Щекочихин Ю. Лев прыгнул в XXI век. Уже в погонах // Новая газета. – 2001. – № 6. – С. 9.

20 % из них перешли в криминальные структуры[1]. Аналитики, оперативники, спецназовцы, разведчики и контрразведчики в криминальных структурах очень ценятся и труд их оплачивается весьма высоко, что и заставляет многих бывших сотрудников правоохранительных органов и спецслужб уходить в криминал. Например, в упоминавшейся уже ОПГ братьев Ларионовых состояли бывшие бойцы десантно-штурмовой бригады и бойцы морского спецназа, бывший сотрудник районной прокуратуры, считавшийся одним из лучших следователей в Приморском крае, бывшие сотрудники Главного разведуправления Генерального штаба[2].)

– неудовлетворенность части бывших и действующих сотрудников субъектов экономической деятельности своим материальным положением, которая вызывает у них решимость “продать” сведения конфиденциального характера преступникам; (Например, по мнению итальянских психологов, из всех служащих любой фирмы 25 % честные и добросовестные сотрудники, 25 % ожидают удобного случая для разглашения секретной информации и 50 % будут действовать в зависимости от обстоятельств[3].)

– иные негативные факторы, способствующие негативному воздействию организованной преступности и коррупции на конфиденциальные информационные ресурсы.

Говоря о *криминогенных детерминантах, которые непосредственно порождают негативное воздействие оргпреступности и коррупции на конфиденциальные информационные ресурсы,* хотелось бы отметить следующее. Как уже не раз говорилось, в современной России информация стала играть определяющую роль в любой сфере деятельности и превратилась в весьма ценный товар. Спрос на этот

---

[1] См.: Мелкобородов В.М. Перспективы изменения структур преступных сообществ и их роль в совершении тяжких преступлений // Насилие: криминальные формы проявления, совершенствование мер борьбы. Ч. II. – Челябинск: Челябинский ЮИ МВД России, 1999. – С. 12.

[2] См.: Корольков И. Вышеуказ. работа. – С. 8-9.

[3] См.: Стрельченко Ю.А. Обеспечение информационной безопасности банков. – М., 1994. – С. 41.

товар обусловлен желанием заинтересованных “потребителей”, в частности организованных преступников, обладать сведениями конфиденциального характера, которые являются для них ключом к достижению определенных целей. Соответственно спрос родит и предложение – коррумпированные чиновники, обладающие такими сведениями по долгу службы, готовы их предоставить представителям организованной преступности, и движут этими “продавцами” информации, как правило, корыстные мотивы.

2. СРЕДСТВА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ

2.1. Правовые средства защиты

Учитывая высокую латентность описанных выше преступных деяний (по мнению специалистов, из всего количества посягательств, в частности на секреты предприятий, раскрывается не более 10–12 %[1], а до широкой общественности доходит лишь 1 %[2]), на первый план выходят меры их предупреждения и профилактики. Эти меры предполагают широкий спектр различных средств, и прежде всего правовых, организационных и технических.

Правовые средства предупреждения рассматриваемых в работе негативных явлений включают в себя три, своего рода, уровня.

Первый уровень – законодательство, не являющееся уголовным, однако регулирующее общественные отношения, связанные с созданием, распространением,

---

[1] См.: Основы безопасности предпринимательства (авторы В.Л.Василенок, В.В.Горшков, М.Ш.Даветов, А.М.Корешков, А.И.Соловьев). – СПб., 1998. – С. 30.

[2] См.: Организация и современные методы защиты информации / Под общ. ред. С.А.Диева, А.Г.Шаеваева. – М., 1998. – С. 9.

преобразованием и потреблением конфиденциальной информации. Речь, в данном случае, идет о нормах административного, гражданского, трудового, финансового и иного права, воплощенных в законодательных актах федерального и регионального уровня. Требуют скорейшего принятия Федеральные законы “О персональных данных”, “О банковской тайне”, “О служебной тайне”, “О коммерческой тайне”, “О борьбе с коррупцией”, “О борьбе с организованной преступностью” и т.п. Должны быть устранены пробелы и коллизии в действующем ныне законодательстве, регулирующем отношения по поводу конфиденциальной информации. Это касается прежде всего тех законодательных актов, которые предусматривают в качестве обязательных субъектов информационных правоотношений государственных чиновников. Необходима обязательная криминологическая экспертиза всех готовящихся нормативных правовых актов соответствующей направленности.

Второй уровень – уголовное законодательство, предусматривающее ответственность за преступления, посягающие на общественные отношения по поводу конфиденциальной информации. Соответствующие уголовно-правовые нормы нуждаются в серьезной законодательной доработке. Имеются в виду прежде всего ст. ст. 137, 138, 183, 310, 311, 320, 283, которые в качестве квалифицирующего признака должны предусматривать совершение указанных преступлений группой лиц по предварительному сговору, организованной группой или лицом с использованием служебного положения. (Напомним, кстати, что последний признак уже предусмотрен в ст. 137, части 2.)

Усиление уголовной ответственности государственных служащих, обладающих конфиденциальными сведениями, за их разглашение вполне обоснованно и отвечает экономическим и политическим реалиям. Аналогичным образом уже давно идет уголовное законодательство ряда зарубежных стран. Например, УК Италии в разделе о должностных преступлениях предусматривает ответственность должностного лица за использование изобретений и открытий, ставших известными ему по службе (ст. 325), и за разглашение и использование служебных секретов. УК Германии предусматривает

ответственность за разглашение служебной тайны должностным лицом, т.е. тайны, доверенной ему или ставшей ему известной именно как должностному лицу. Согласно Своду законов США (§ 1905) должностное лицо или служащий государственных учреждений США, по роду своей службы обладающие секретной информацией, касающейся секретов торговли, управления, стиля работы, данных о персонале какого-либо лица, фирмы, корпорации и т.д., несут ответственность за незаконное разглашение такой информации[1].

Третий уровень – локальные акты, регулирующие вопросы сохранности конфиденциальных информационных ресурсов в рамках того или иного органа, субъекта экономической деятельности, какой-либо организации. Этот уровень предполагает, в первую очередь, заключение различных договоров и соблюдение конфиденциальности полученных сотрудниками этих органов, организаций, предприятий и т.п. сведений ограниченного распространения. К таким конфидентам (лицам, обязанным хранить данные сведения) относятся, в частности, работники субъекта экономической деятельности, состоящие с последним в трудовых отношениях, на которых возлагается обязанность хранить коммерческую тайну этого субъекта. Такие обязательства могут оформляться в рамках самостоятельных соглашений или быть составной частью общего трудового контракта (договора)[2]. Различные обязательства аналогичного характера могут содержаться в правилах трудового распорядка, различных памятках, а также в гражданско-правовых договорах. Примечательно, что и в трудовые договоры, которые заключают государственные служащие, подобные обязанности также могут и должны включаться.

По мере развития информационных отношений по поводу сведений конфиденциального характера правовые меры, как впрочем и меры иного характера,

---

[1] См.: Ответственность за должностные преступления в зарубежных странах / Отв. ред. Ф.М.Решетилов. – М.: Юридическая литература, 1994. – С. 17, 49, 67.

[2] См.: Правовая охрана интеллектуальной собственности: Учебное пособие / Под общ. ред. В.Н.Дементьева. – М.: НИУПРИС, 1995. – С. 114.

должны совершенствоваться и соответствовать степени угрозы конфиденциальным информационным ресурсам со стороны организованной преступности и коррупции.

2.2. Организационные средства защиты

Организационные меры прямо или косвенно связаны с административным управлением предприятия, кредитной организации, государственного органа или любой другой организации, в которой циркулирует конфиденциальная информация. К таким мерам относятся, прежде всего, определение кадровой политики, подбор служащих и их защита, меры по определению и обеспечению конфиденциальности сведений, классификация документов по степени важности и секретности, определение режима их хранения, а также допуска к ним и учета. В рамках организационных мер устанавливается специальный пропускной режим, формируется служба безопасности и охраны, делопроизводство внутри организации, органа, предприятия и т.п. должно отвечать всем требованиям безопасности и на соответствующих документах проставляются специальные грифы (“Конфиденциально”, “Строго конфиденциально”, “Коммерческая тайна”, “Служебная тайна” и т.д.), с персоналом проводится надлежащий инструктаж относительно охраны конфиденциальных сведений[1].

В последнее время в России при приеме на работу в крупные компании или банки проводят тестирование конфидентов на детекторе лжи (полиграфе). Хотя проверять необходимо не только новичков, но и давно работающих сотрудников также. Следует ввести правило (которое в крупных субъектах экономической деятельности уже “взято на вооружение”), согласно которому сотрудники, вовремя сообщившие о попытках завербовать их, должны поощряться.

Говоря о пропускном режиме, необходимо отметить, что зачастую он в различных организациях функционирует неправильно. Перечень лиц, имеющих право

---

[1] См.: Правовая охрана интеллектуальной собственности. – С. 110-113.

на заказ разового пропуска, должен быть ограничен в соответствии с производственной и служебной необходимостью. Получив пропуск, посетитель должен быть встречен охранником на входе, который и отведет гостя к месту встречи, а после ее окончания проводит посетителя к выходу. Это снижает риск проникновения на объект случайных людей и установки специальной прослушивающей техники[1].

Надлежащая организация делопроизводства также является важнейшим условием сохранности конфиденциальных сведений. Нередко в российских коммерческих структурах организации делопроизводства не уделяют должного внимания. Отсутствуют не только инструкции, регламентирующие доступ различных категорий сотрудников к важнейшим документам, но и элементарный учет. Выяснить кто, когда и какой документ получил и как им распорядился подчас просто невозможно. Отсутствие контроля за ксерокопировальной техникой облегчает копирование различных документов, не подлежащих выносу с объекта. Офис следует разделить на режимные зоны. В секторе для приема посетителей нельзя держать важные документы. А наиболее секретная зона, где, как правило, расположены кабинеты высшего руководства, должна быть недоступна не только случайным посетителям, но и большинству рядовых сотрудников. Вход туда может осуществляться лишь по специальному разрешению.

Все конфиденциальные переговоры необходимо вести в специально оборудованном помещении, которое было бы снабжено специальной техникой для подавления радиомикрофонов и диктофонов. Изготовлена эта комната должна быть из прозрачных материалов, чтобы любое подслушивающее устройство можно было обнаружить даже визуально. После проведения переговоров помещение следует

---

[1] См.: Враг подслушивает // Деловые люди. Блокнот делового человека. – 1999. – № 101. – С. 12-13.

опечатать, доступ в него должен охраняться системами видеонаблюдения и входить в него могут только самые высокопоставленные сотрудники[1].

Одним из решающих факторов, влияющих на сохранность конфиденциальной информации, является кадровая политика в соответствующих органах и организациях. Это тем более важно, учитывая активную агентурную и вербовочную работу преступников. В связи с этим служба безопасности должна постоянно вести работу совместно с отделом кадров, направленную на то, чтобы не допустить прием на работу “случайных” людей, лиц с уголовным прошлым и представителей криминальных структур. Подбор кадров – довольно деликатная и сложная проблема. Она включает такие вопросы, как основные принципы кадровой работы с персоналом, задачи и критерии отбора сотрудников, способы и приемы определения мотивации к работе, определение профессиональной пригодности, навыков; методы и процедуры проверки кандидатов на работу, в т.ч. проверка на употребление наркотиков, алкоголя, психотропных препаратов и т.п.[2]

Любые организационные меры защиты конфиденциальной информации должны быть адаптированы к структуре охраняемого объекта, с учетом особенностей управления, стоящих перед персоналом задач, направления деятельности и т.п.

2.3. Технические средства защиты

Технические средства защиты конфиденциальных информационных ресурсов предназначены для предотвращения утечки такой информации по техническим

---

[1] См.: Враг подслушивает. – С. 13.

[2] См.: Ларичев В.Д. Как уберечься от мошенничества в сфере бизнеса. – М.: Юрист, 1996. – С. 82-83.

каналам. Под техническим каналом утечки информации принято понимать систему, в состав которой входят:

1) Объект разведки (помещение, группа помещений, здание, технические каналы, используемые для передачи конфиденциальных сведений).

2) Техническое средство, используемое для несанкционированного получения информации.

3) Физическая среда, в которой распространяется информационный сигнал (строительные конструкции зданий и сооружений, токопроводящие линии, среда распространения акустических, т.е. речевых, сигналов, электромагнитные поля, технические средства обработки информации и т.п.)[1].

Принято выделять следующие основные группы технических каналов утечки информации: а) электромагнитные; б) электрические; в) каналы утечки видовой информации; 2) каналы утечки акустической (речевой) информации (электроакустический, виброакустический, оптико-электронный, проводной, электромагнитный, акустический)[2].

Технические средства защиты включают в себя устройства, предназначенные для защиты от прослушивания: генераторы шума; анализаторы телефонных линий; “подавители” диктофонов, обеспечивающие подавление средств магнитной записи; специальные средства поиска и обнаружения подслушивающих устройств; генераторы радиошума, подавляющие побочные электромагнитные излучения персональных компьютеров и компьютерных сетей; скрэмблеры (маскираторы) для засекречивания речевой информации, передаваемой по телефону или радиоканалу, и т.д.[3]

---

[1] См.: Специальная техника и информационная безопасность: Учебник / Под ред. В.И.Кирина. – Т. 1. – М.: Академия управления МВД России (спонсор издания – компания Моторола), 2000. – С. 397-398.

[2] См.: Специальная техника и информационная безопасность. Т. 1. – С. 400.

[3] См.: Правовая охрана интеллектуальной собственности. – С. 116; Техника специального назначения // Мир безопасности. – 1998. – № 7. – С. 36; Каталог специальной техники // Безопасность нашего дела. – 1997. – № 4. – С. 5-13.

Особое внимание следует уделять безопасности компьютерных систем и сетей. Так, в последнее время широко распространен т.н. электромагнитный перехват. Суть его заключается в приеме паразитирующих радиоизлучений с дисплея компьютера на специальное принимающее устройство, т.е. на экране принимающего устройства отображается все то, что находится в данный момент на дисплее компьютера, за которым шпионят. Радиус действия таких устройств – до 1000 м. Впервые такой перехват был открыто продемонстрирован в Каннах в 1985 г. на международном конгрессе по безопасности ЭВМ. Сотрудник одной голландской телекоммуникационной компании с помощью разработанного им устройства “снял” данные с экрана дисплея персонального компьютера, установленного на восьмом этаже здания, расположенного в ста метрах от автомобиля, из которого действовал перехватчик[1]. Компьютеры должны находиться в специальной комнате, сделанной из материалов, поглощающих паразитирующее электромагнитное излучение. Соответственно в таком помещении должны функционировать генераторы радиошума, подавляющие такое излучение, о чем уже упоминалось.

Перечисленные выше меры правового, организационного и технического характера не являют собой законченный перечень, а знаменуют лишь тенденции в защите информации. Конкретный набор мер защиты зависит от вида конфиденциальной информации, каналов связи, в которых она циркулирует, количества субъектов, обязанных хранить сведения в секрете, технических, правовых, организационных, финансовых и иных возможностей защиты и т.д.

3. ПРОГНОЗИРОВАНИЕ НОВЫХ ВИДОВ ВОЗДЕЙСТВИЯ ОРГАНИЗОВАННОЙ ПРЕСТУПНОСТИ И КОРРУПЦИИ НА КОНФИДЕНЦИАЛЬНЫЕ ИНФОРМАЦИОННЫЕ РЕСУРСЫ

---

[1] См.: Совещание по вопросам компьютерной преступности // Проблемы преступности в капиталистических странах. – М.: ВИНИТИ, 1986. – № 11. – С. 36-40.

Учитывая минимум данных официальной статистики, характеризующих негативное воздействие организованной преступности и коррупции на конфиденциальные информационные ресурсы, мы должны признать, что точного прогнозирования ожидать не стоит. И тем не менее определенные тенденции все же просматриваются.

Так, обращают на себя внимание темпы прироста преступления, предусмотренного ст. 183 УК РФ. В 2000 г. их было зарегистрировано почти в 4,5 раза больше по сравнению с аналогичным периодом предыдущего (1999) года. На наш взгляд, этот прирост вполне объясним, поскольку информация, составляющая коммерческую или банковскую тайну, обладает высокой ценностью, а, следовательно, стремление ОПГ завладеть этой информацией также высоко. Получить эти сведения преступники могут через коррумпированных чиновников, обладающих такими сведениями в силу служебных обязанностей.

Сведения, составляющие коммерческую, банковскую, налоговую тайну, циркулируют, прежде всего, в предпринимательской сфере, которая издавна являлась объектом пристального внимания ОПГ. Такие сведения обращаются в производственном, коммерческом, посредническом, кредитно-финансовом, страховом предпринимательстве. Примечательно, что по мнению респондентов *более всего* преступление, предусмотренное ст. 183, распространено именно в кредитно-банковской сфере (52 % опрошенных).

Обращает на себя внимание также и рост такого преступления, как неправомерный доступ к компьютерной информации (ст. 272). Такой доступ зачастую сопряжен с посягательствами на различные виды тайн. Это неудивительно, поскольку электронный документооборот постепенно вытесняет документооборот бумажный, происходят повсеместная компьютеризация субъектов экономической деятельности, освоение глобальных компьютерных сетей и т.д. Более того, для обмена

конфиденциальной информацией уже создаются специальные компьютерные сети[1]. А поскольку сфера компьютерной информации, в т.ч. и конфиденциального характера, активно подвергается воздействию организованной преступности (о чем уже упоминалось), то эта негативная тенденция будет усиливаться.

Нельзя не сказать о таких объективно влияющих на рассматриваемую проблему факторах, как создание различных государственных органов, представляющих собой гигантский банк данных конфиденциальной информации. Яркий тому пример – появление Комитета по финансовому мониторингу (т.н. финансовой разведки), который является согласно Федеральном закону “О противодействии легализации (отмыванию) доходов, полученных преступным путем” *уполномоченным органом*. В данный орган будет стекаться информация об операциях с денежными средствами или иным имуществом, подлежащих обязательному контролю. Предоставлять эти сведения будут соответствующие организации, такие операции осуществляющие (кредитные организации, страховые и лизинговые компании, ломбарды и др.)[2]. По сообщениям СМИ, заработная плата сотрудников этого уполномоченного органа не будет превышать 500 долларов, а информация, которую они будут обрабатывать, по стоимости будет равна миллионам. Естественно, что повышается риск утечки информации через сотрудников, которые могут не устоять перед искушением поправить свои финансовые дела за счет служебной информации. И эту угрозу предстоит нейтрализовать, в противном случае велик риск перехода сведений, составляющих коммерческую, банковскую, налоговую и иную тайну, “во владение” организованных преступников.

Завершая исследование, необходимо подчеркнуть, что воздействие организованной преступности и коррупции на конфиденциальные информационные

---

[1] См.: Деменков А. Как обмениваться секретами // Экономическая и банковская безопасность. – С. 33-37.

[2] См.: Российская газета. – 9.08.2001.

ресурсы будет усиливаться, и для минимизации угрозы таким ресурсам необходим комплексный подход, включающий различные меры правового, организационного, технического и иного характера. Выработка таких мер должна осуществляться в том числе посредством различных научно-исследовательских изысканий на основе фактических реалий. Скорейшая разработка таких эффективных мер жизненно необходима и является одной из действенных гарантий информационной безопасности России в целом. Бурное развитие новых информационных технологий, появление новых видов связи и способов передачи информации обуславливают и появление новых угроз конфиденциальным информационным ресурсам со стороны организованной преступности и коррупции. И от того, насколько удастся противостоять этим угрозам, во многом зависит будущее России в наступившем тысячелетии.

ЛИТЕРАТУРА

1. Гражданский кодекс РФ I и II части. – М., 2000.

2. Уголовный кодекс РФ. – М., 2000.

3. Закон РФ “О государственной тайне” // Российская газета 21.09.1993; Собрание законодательства РФ. – 1997. – № 41. – Ст. 4673.

4. Федеральный закон “Об информации, информатизации и защите информации” // Собрание законодательства РФ. – 1995. – № 8. – Ст. 609.

5. Федеральный закон “Об оперативно-розыскной деятельности в Российской Федерации” // Собрание законодательства РФ. – 1995. – № 33. – Ст. 3349.

6. Федеральный закон “О противодействии легализации (отмыванию) доходов, полученных преступным путем” // Российская газета. – 9.08.2001.

7. Указ Президента РФ “О Перечне сведений, отнесенных к государственной тайне” // Собрание законодательства РФ. – 1995. – № 49. – Ст. 4775.

8. Указ Президента РФ “Об утверждении перечня сведений конфиденциального характера” // Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

9. Постановление Пленума Верховного Суда РФ “О применении судами законодательства об ответственности за бандитизм” от 17.01.1997 // Сборник постановлений Пленумов Верховных Судов СССР и РСФСР (Российской Федерации) по уголовным делам. – М., 1997.

10. Доктрина информационной безопасности // Российская газета. – 28.09.2000.

11. Агуреев А. Нью-Йорк остается “шпионским гнездом” // Новости разведки и контрразведки. – 1994. – № 21-22.

12. Беловецкий Д. “Слоновая” болезнь // Литературная газета. – 1998. – № 44.

13. Борисов И. Поминальная молитва при свечах. Взяли Яшу Бешеного // Версия. – 1999. – № 27.

14. Бурмистров И.А. Коррупция: ее сущность и меры предупреждения // Коррупция: политические, экономические, организационные и правовые проблемы / Под ред. В.В.Лунеева. – М.: Юрист, 2001.

15. Василенок В.Л., Горшков В.В., Даветов М.Ш., Корешков А.М., Соловьев А.И. Основы безопасности предпринимательства. – СПб., 1998.

16. Воронин Ю. Криминальная революция в государстве: экономические и политические аспекты организованной преступности в России // Российская организованная преступность: новая угроза? / Под ред. Ф.Вильямса; пер. с англ. А.Гостева. – М.: Крон-Пресс, 2000.

17. Враг подслушивает // Деловые люди. Блокнот делового человека. – 1999. – № 101.

18. Геворгян Г. Преступные этнические формирования // Законность. – 1999. – № 9.

19. Гладышев В. “Шпионская техника” доступна не каждому // Все о безопасности. – 1999. – № 1.

20. Глинкина С.П. К вопросу о выборе стратегии экономических реформ и характере российской коррупции // Коррупция: политические, экономические, организационные и правовые проблемы / Под ред. В.В.Лунеева. – М.: Юрист, 2001.

21. Гришина Е. Хакеры воруют миллиардами // Аргументы и факты-Москва. – 1999. – № 20.

22. Гуськова Т. Купите базу данных о себе // Бизнес и безопасность в России. – 2001. – № 2.

23. Данн Г. Основные криминальные группировки современной России // Российская организованная преступность: новая угроза? / Под ред. Ф.Вильямса; пер. с англ. А.Гостева. – М.: Крон-Пресс, 2000.

24. Деменков А. Как обмениваться секретами // Экономическая и банковская безопасность (По материалам журнала “Частный сыск, охрана, безопасность”, с 1997 г. – “Мир безопасности”). – М., 1998.

25. Емельянов Г.В., Стрельцов А.А. Проблемы реализации Доктрины информационной безопасности Российской Федерации // Сборник материалов Всероссийской конференции “Информационная безопасность России в условиях глобального информационного общества” / Под общ. ред. А.В.Жукова. – М.: Бизнес + безопасность, 2001.

26. Загайнов М. Война с преступностью. Вопросов пока больше, чем ответов // Новости разведки и контрразведки. – 1996. – № 5.

27. Игорев А. Предпринимателя взяли за “Флай” // Коммерсантъ. – 14.02.2001.

28. Каталог специальной техники // Безопасность нашего дела. – 1997. – № 4.

29. Кибальник А.Г., Кузьмин С.В., Соломоненко И.Г. Тайна в уголовном праве. – Ставрополь: Ставропольсервисшкола, 2000.

30. Компьютер с “черного хода” // Клиент. – 1999. – № 38.

31. Корольков И. Тень летучей мыши // Московские новости. – 2000. – № 51.

32. Криворучко С. Я знаю о Вас все // Бизнес и безопасность в России. – 1997. – № 1.

33. Криминология: Учебник / Под ред. проф. Н.Ф.Кузнецовой, проф. Г.М.Миньковского. – М.: БЕК, 1998.

34. Куксин И.Н., Смирнов М.П. Проявление организованной преступности в сфере налогообложения и меры борьбы с ней // Организованная преступность–3 / Отв. ред. А.И.Долгова и С.В.Дьяков. – М.: Криминологическая Ассоциация, 1996.

35. Ларичев В.Д. Как уберечься от мошенничества в сфере бизнеса. – М.: Юрист, 1996.

36. Левицкий Ю. “Аргус” не снимает “крыш” // Частный сыск, охрана, безопасность. – 1995. – № 9.

37. Лукашук И.И., Наумов А.В. Международное уголовное право: Учебник. – М.: Спарк, 1999.

38. Лунеев В.В. Преступность XX века. Мировой криминологический анализ. – М.: Норма, 1999.

39. Макиенко А. Служба безопасности банка: информация и анализ // Экономическая и банковская безопасность (По материалам журнала “Частный сыск, охрана, безопасность”, с 1997 г. – “Мир безопасности”). – М., 1998.

40. Матюхин В.Г. // Сборник материалов Всероссийской конференции “Информационная безопасность России в условиях глобального информационного общества” / Под общ. ред. А.В.Жукова. – М.: Бизнес + безопасность, 2001.

41. Мелкобородов В.М. Перспективы изменения структур преступных сообществ и их роль в совершении тяжких преступлений // Насилие: криминальные формы проявления, совершенствование мер борьбы. Ч. II. – Челябинск: Челябинский ЮИ МВД России, 1999.

42. Москвин В. Внутренняя защита банка // Бизнес и банки. – 1996. – № 24.

43. Никифоров А.С. Что нам делать с организованной преступностью? // Изучение организованной преступности: российско-американский диалог. – М., 1997.

44. Нургалиев Б.Н. Организованная преступная деятельность (уголовно-правовые, процессуальные и криминологические аспекты). – Караганда, 1997.

45. Олейников В.В. Делайте бизнес надежным и безопасным. – Рыбинск, 1997.

46. Организация и современные методы защиты информации / Под общ. ред. С.А.Диева, А.Ш.Шаваева. – М., 1998.

47. Организованная преступность–2 / Отв. ред. А.И.Долгова, С.В.Дьяков. – М.: Криминологическая Ассоциация, 1993.

48. Ответственность за должностные преступления в зарубежных странах / Отв. ред. Ф.М.Решетников. – М.: Юридическая литература, 1994.

49. Петрухин И.Л. Личные тайны (Человек и власть). – И.: ИГП РАН, 1998.

50. Подлесских Г., Терешонок А. Воры в законе: бросок к власти. – М., 1994.

51. Политика криминализируется, криминал политизируется (По материалам проекта Центра по международным и стратегическим исследованиям г. Вашингтона “Российская организованная преступность”) // Новости разведки и контрразведки. – 1997. – № 23.

52. Правовая охрана интеллектуальной собственности: Учебное пособие / Под общ. ред. В.Н.Дементьева. – М.: НИУПРИС, 1995.

53. Практика уголовного сыска: Научно-практический сборник / Составитель А.Ваксян; научн. ред. А.И.Алексеев. – М.: Лига Разум, 1999.

54. Пристанская О.В. // Организованная преступность. Проблемы, дискуссии, предложения. “Круглый стол” / Отв. ред. А.И.Долгова, С.В.Дьяков. – М., 1989.

55. Разведчиков заставят курить на благо России // Московский комсомолец. – 2000. – № 48.

56. Совещание по вопросам компьютерной преступности // Проблемы преступности в капиталистических странах – М.: ВИНИТИ, 1986. – № 11.

57. Соколов А.В., Степанюк О.М. Шпионские штучки. Методы информационной защиты объектов и компьютерных сетей. – М., СПб.: Полигон·АСТ, 2000.

58. Специальная техника и информационная безопасность: Учебник / Под ред. В.И.Кирина. Т. 1. – М.: Академия управления МВД России, 2000.

(Спонсор издания – компания Моторола.)

59. Стрельченко Ю.А. Обеспечение информационной безопасности банков. – М., 1994.

60. Техника специального назначения // Мир безопасности. – 1998. – № 7.

61. Углубление социального контроля преступности – одна из предпосылок решения социально-экономических проблем (материалы “круглого стола”). Подготовил В.В.Лунеев // Государство и право. – 1999. – № 9.

62. Федосенко В. “Жучки” от безработного // Российская газета. – 25.05.2000.

63. Хинштейн А. Лицензия на террор // Московский комсомолец. – 03.11.2001.

64. Шахов А.В. Электронные взломщики – преступники под маской романтиков // Защита информации. – 1997. – № 1.

65. Щекочихин Ю. Лев прыгнул в XXI век. Уже в погонах // Новая газета. – 2001. – № 6.

66. Ярочкин В. Организованная преступность. Откуда исходит угроза. – М., 1995.