**Введение**

В настоящее время борьба с преступлениями в сфере информационных технологий является третьим по счету приоритетом в деятельности ФБР США после борьбы с терроризмом и контрразведкой.[[1]](#footnote-1)

В Российской Федерации до недавнего времени считалось, что компьютерная преступность – явление, свойственное только зарубежным странам, и по причине слабой компьютеризации нашего общества, отсутствует вообще. Именно это обстоятельство и привело к отсутствию сколько-нибудь серьезных научных исследований этой проблемы.

Как нередко случалось ранее (например, ситуация с наркоманией или с организованной преступностью), борьба с отдельным видом преступности начиналась лишь после того, как материальные потери от него достигали существенных размеров и начинали резко выделяться на общем фоне потерь от обычных видов общеуголовной преступности.

**Основные причины существования компьютерных преступлений**

Компьютеризация современного российского общества, затрагивающая практически все стороны деятельности людей, предприятий и организаций, государства, породила новую сферу общественных отношений, которая, к сожалению, нередко теперь становится объектом противоправных действий. Стремительное развитие научно-технического прогресса затронуло и Саратовскую область и обусловило необходимость борьбы с преступлениями в сфере компьютерной информации. Если в 2000 году было выявлено только 7 преступлений в сфере компьютерной информации, а в 2001 – 10, то за 2002 было возбуждено 22 уголовных дела, т.е. увеличение за год на 120% (см. Приложение №2: Справку о полученных статистических данных из Информационного Центра при УВД Саратовской области,). Неужели подобная динамика развития уровня преступности в Саратовской области не настораживает? Без эффективного противодействия рост количества преступлений будет продолжаться с новыми силами – в этом и есть специфика киберсферы.

Представители правоохранительных органов признают, что слишком высок уровень латентности данного вида преступности, выявляется только около 10% преступлений. Такова одна из отличительных черт преступлений в сфере компьютерной информации. Это происходит в результате следующих причин:

1. **Транснациональность.** Преступник, как правило, находится на удаленном расстоянии от объекта преступления, даже на территории другого государства. Совершение преступления с территории другого государства вполне оправдано. Преступник может уйти от ответственности из – за разницы (отсутствия) законодательства, регулирующего информационные отношения, из – за отсутствия договоров о сотрудничестве между государствами в данной отрасли, из – за процессуальных и бюрократических проволочек, которые возникнут при обсуждении вопросов, связанных с возбуждением уголовного дела в отношении иностранного гражданина, экстрадиции и другие.

2. Социологическое исследование, проведенное среди сотрудников правоохранительных органов и студентов IV курса СГАП (см. Приложение №1: Справку о результатах анкетирования, проведенного в рамках исследования), показало, что **компьютерным преступлениям свойственна организованность** (82% репондентов), и чаще эти преступления совершаются организованной группой со свойственной иерархией, четким распределением ролей и обязанностей (87,5% респондентов). Действительно, все чаще на лентах интернет – агентств появляются сообщения о хакерских атаках. К примеру, на официальный сайт ФСБ России в 2002 году было совершено около 600 подобных нападений. Эти нападения осуществляются группой хакеров, атака строго синхронизирована во времени, может быть намечена на единственную цель. В группах существует деление на: наблюдателей – имеют законный вход в систему, либо статус рядового пользователя и следят за ходом взлома, закрепляют отклонения в работе системы; бойцов – лиц, взламывающих операционную систему; бойцов – взламывающих программное обеспечение; бойцов – взламывающих системную защиту; запасных – приступают к взлому только в случае обнаружения у атакуемого объекта слабых мест.[[2]](#footnote-2)2

85% респондентов, принявших участие в опросе (см. Приложение №1: Справку о результатах анкетирования, проведенного в рамках исследования), считают, что на организованность компьютерной преступности в Саратове указывает постоянство способов и методов совершения преступлений, сплоченность, устойчивость и межнациональный состав группировок. По данным оперативных сотрудников (см. Приложение №3: Лист интервьюирования №6) хакеры в России объединены в региональные группы. Они издают свои электронные средства массовой информации (к примеру, http://www.xakep.ru). Имеют свой «неформальный кодекс», жаргонный словарь, распространяющийся с помощью компьютерных бюллетеней, в которых имеются все необходимые сведения для повышения мастерства начинающего. Проводят электронные конференции, на которых между собой обмениваются сведениями о создании новых вирусов, способов проникновения в какую-нибудь систему, снятии защиты этой системы или с иного программного продукта. Данные действия можно квалифицировать как соучастие в преступления в виде пособничества, ч. 5 ст. 33 УК РФ – пособником признается лицо, содействовавшее совершению преступления советами, указаниями, представлением информации, средств или орудий совершения преступления. После совершения преступления происходит сокрытие следов. Особенностью подобных атак является то, что участники могут находиться друг от друга за тысячи километров. Этим группировкам не мешает языковой барьер (машинные языки стандартны), государственные границы (в виртуальном мире нет границ).[[3]](#footnote-3)1

В ответе на вопрос: «В чем сложность выявления ОПГ, совершающих компьютерные преступления?» – 77,5% лиц, участвующих в социологическом опросе, указали, что высокая технологичность не позволяет выявить ролевые функции участников преступных структур, а 72,5% ответили, что главная причина в сплоченности и высоком интеллектуальном уровне участников организованных групп, совершающих компьютерные преступления (см. Приложение №1: Справку о результатах анкетирования, проведенного в рамках исследования). На мой взгляд, данные сложности не являются основанием для того, чтобы говорить о невозможности выявления групп преступников, наоборот – данные о способе совершения преступления и личности преступника позволяют сузить круг подозреваемых, которые могут обладать такого уровня специальными познаниями.

3. Малое количество или полное отсутствие следовой информации о совершении преступления. Возможна инсценировка кражи, уничтожение или радикальное изменение программных средств и другие.

4. Трудности в определении времени, места совершения преступления.

Организованная преступность в сфере компьютерной информации существует во всем мире. Какова же картина в Саратовской области? За 2000–2002 годы не выявлено **ни одного** преступления, предусмотренного ст. ст. 272–274 УК РФ, совершенного группой лиц по предварительному сговору (см. Приложение №2: Справку о полученных статистических данных из Информационного Центра при УВД Саратовской области,). Неужели мировые тенденции в развитии криминала не касаются нашей губернии? Почему такие противоречия между официальной статистикой и результатами социологических опросов, проведенных в рамках этого исследования (90% респондентов ответили, что на территории Саратовской обл. компьютерная преступность носит организованный характер)? Можно сделать вывод, что правоохранительные органы просто не готовы к эффективной борьбе с организованной преступностью в высокотехнологичной отрасли.

**Законодательство в борьбе с компьютерными преступлениями**

Глава 28 УК РФ содержит довольно четкие, проработанные составы, но уголовная ответственность за эти преступления слишком низкая, не отвечающая сегодняшним реалиям. В ответе на вопрос: «Достаточна ли законодательная база РФ для эффективного противодействия развитию компьютерной преступности?» – 47,5% респондентов ответили, «нет, слишком слабая ответственность за эти преступления». Ч. 2 ст. 272 УК РФ содержит в диспозиции норму: «То же деяние, совершенное группой лиц по предварительному сговору или организованной группой…» То есть законодатель ужесточил санкцию уголовно – правовой статьи за совершение преступления по предварительному сговору или организованной группой, такие же дополнения необходимо сделать и для ст. ст. 273, 274 УК РФ.

В настоящее время также необходимы технические меры противодействия организованным преступным группам, совершающим компьютерные преступления. Считаю необходимым создавать для пользователей защиту от несанкционированного доступа к компьютерной системе, резервировать важные компьютерные системы, принимать конструкционные меры защиты от хищений и диверсий, обеспечивать резервным электропитанием, разрабатывать и реализовывать специальные программные и аппаратные комплексы безопасности и многое другое.[[4]](#footnote-4)1

Подобные меры необходимо реализовывать как на федеральном, так и на местном уровне. К ведению федеральных органов государственной власти относится доработка гражданского и уголовного законодательства, а также финансирование технических программ, необходимых для противодействия организованным преступным кибергруппировкам. 90% респондентов, участвующих в социологическом опросе, проводимом в рамках данного исследования, высказались, что меры, предпринимаемые федеральными органами государственной власти по борьбе с организованной киберпреступностью (в масштабах Российской Федерации), не эффективны в силу отсутствия законодательной базы.

Законодательная база, регулирующая информационные отношения в РФ, состоит из следующих нормативных актов:

1. Закон РФ от 23 сентября 1992 г. №3523-I «О правовой охране программ для электронных вычислительных машин и баз данных».

2. Закон РФ от 22 октября 1992 г. «О правовой охране топологий интегральных микросхем».

3. Закон РФ от 9 июля 1993 г. №5351-I, с изменениями и дополнениями «Об авторском праве и смежных правах».

4. Закон РФ от 21 июля 1993 г. «О государственной тайне».

5. Федеральный закон от 29 декабря 1994 г. №77-ФЗ «Об обязательном экземпляре документов».

6. Федеральный закон от 16 февраля 1995 г. №15-ФЗ «О связи».

7. Федеральный закон от 20 февраля 1995 г. №24-ФЗ «Об информации, информатизации и защите информации» и другие.

Большинство из этих актов не отвечает современному уровню развития информационных отношений, не смотря на изменения и дополнения они не выстраивают эффективный законодательный барьер для развития преступных кибергруппировок. С точки зрения правоприменительной практики представляется оправданным создание одного специализированного акта, регулирующего юридические, процедурные аспекты по противодействию киберпреступности (к примеру, Закон «РИКО» § 1962 или директивы президента США (PDD-63) об организации работ по защите национальной инфраструктуры в США)[[5]](#footnote-5)1.

Сейчас главным для нас должно являться: создание и совершенствование системы обеспечения информационной безопасности Российской Федерации; устранение внутренних противоречий в федеральном законодательстве; противоречий, связанных с международными соглашениями, к которым присоединилась Российская Федерация, и противоречий между федеральными законодательными актами и законодательными актами субъектов Российской Федерации; а также конкретизация правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности Российской Федерации.

Не произведено законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации.

Имея определенную политическую волю, противодействием, на своем уровне, могли бы заняться власти Саратовской области. На уровне локального нормотворчества можно решить вопросы организационного характера, вопросы по созданию материальной базы для правоохранительных органов. Как положительный пример можно привести Постановление Губернатора Саратовской области от 9 июня 1997 года №470 «О создании в структуре Совета Безопасности Саратовской области отдела по защите информации». Хотя сложно представить себе, как может реально повлиять на ситуацию отдел со штатной численностью в 3 человека. Тем не менее, 77,5% респондентов оценивают предпринимаемые правоохранительными органами, и органами государственной власти Саратовской области меры по борьбе с организованной киберпреступностью как неэффективные из-за отсутствия материально-технической базы. И лишь 62,5% считают, что неспособность противодействовать организованной преступности сложилась из-за отсутствия локального законодательства, регулирующего компьютерную отрасль.

Было бы логичным предположить, что критическая ситуация с ростом компьютерной преступности и особенно её организованным и транснациональным аспектом связана с отсутствием единой политики государства (государств), направленной на борьбу с этим видом преступности. На сегодняшний день в информационной отрасли действует Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. N ПР-1895 (Текст доктрины опубликован в «Российской газете» от 28 сентября 2000 г. №187). Только на 3 месте указывается, что составляющая национальных интересов Российской Федерации в информационной сфере включает в себя развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности.

**Основные направления борьбы**

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности должны являться:

– противодействие развитию преступных транснациональных организованных групп, совершающих компьютерные преступления;

– обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

– предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.

При осуществлении международного сотрудничества Российской Федерации в области обеспечения информационной безопасности особое внимание должно уделяться проблемам взаимодействия с государствами – участниками Содружества Независимых Государств.[[6]](#footnote-6)1

Для осуществления этого сотрудничества по указанным основным направлениям необходимо обеспечить активное участие России во всех международных организациях, осуществляющих деятельность в области борьбы с организованными транснациональными преступными кибергруппировками;

– создание системы сбора и анализа данных об источниках угроз информационной безопасности Российской Федерации, а также о последствиях их осуществления;

– разработку нормативных правовых актов, определяющих организацию следствия и процедуру судебного разбирательства по фактам противоправных действий в сфере компьютерной информации, а также порядок ликвидации последствий этих противоправных действий;

– разработку составов правонарушений с учетом специфики уголовной, гражданской, административной, дисциплинарной ответственности и включение соответствующих правовых норм в уголовный, гражданский, административный и трудовой кодексы, в законодательство Российской Федерации о государственной службе;

– создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем со свободным доступом правоохранительных органов различных государств.

2. Предоставить МВД средства на улучшение материальной базы структур МВД, занимающихся противодействием организованной преступности. Усилить обмен информацией о преступлениях и преступниках с иностранными спецслужбами.

3. Повышение профессионального уровня сотрудников соответствующих силовых структур, привлечение «специалистов», общественности к правоохранительной деятельности.

4. Организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Российской Федерации. Разработка специальных методик, позволяющих выявлять и привлекать к ответственности членов организованных преступных групп, занимающихся преступной деятельностью в сфере компьютерной информации.

5. Разработка федеральной и региональных программ обеспечения противодействия развитию организованных преступных кибергруппировок и координация деятельности по их реализации;

– проведение единой технической политики в области обеспечения информационной безопасности Российской Федерации.

Все вышеизложенные предложения и рекомендации, прежде всего, базируются на соблюдении принципов законности, баланса интересов граждан, общества и государства в информационной сфере.

Соблюдение принципа законности требует от федеральных органов государственной власти и органов государственной власти Саратовской области при выявлении преступных группировок, занимающихся киберпреступлениями неукоснительно руководствоваться законодательными и иными нормативными правовыми актами, регулирующими отношения в этой сфере.

**Заключение**

Соблюдение принципа баланса интересов граждан, общества и государства в киберсфере предполагает законодательное закрепление приоритета этих интересов в различных областях жизнедеятельности общества, а также использование форм общественного контроля деятельности федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации. Реализация гарантий конституционных прав и свобод человека и гражданина, касающихся деятельности в информационной сфере, является важнейшей задачей государства в области информационной безопасности.

Данное исследование имеет своей целью – обращение внимания научной общественности, сотрудников правоохранительных органов на ситуацию, сложившуюся вокруг развития организованных групп, занимающихся преступлениями в сфере компьютерной информации. Анализируя официальную статистику, результаты анкетирования, интервьюирования, можно прийти к выводу, что киберпреступность как разновидность организованной и транснациональной преступности существует на территории Саратовской области. А отсутствие реальных уголовных дел по данной категории является следствием отсутствия государственной политики в этой отрасли, низким уровнем профессиональной подготовки сотрудников правоохранительных органов, отсутствия методик противодействия организованным преступным киберсообществам. Если сейчас не будут приниматься меры, способствующие противодействию развитию данного вида преступности, то в скором времени мы столкнемся с огромным количеством преступлений, вытекающих из этой сферы: вирусным шантажом, компьютерными мошенничествами, кибертерроризмом и другими тяжкими преступлениями.

**Использованная литература**

1. Батурин Ю.М., Жодзинский А.М. Компьютерная преступность и компьютерная безопасность. М.: Юрид. лит., 2006.
2. Быстряков Е.Н., Иванов А.Н., Климов В.А. Расследование компьютерных преступлений. Саратов. 2007.
3. Лысов Н.Н. Содержание характеристики компьютерных преступлений // Проблема криминалистики и методики ее преподавания. М. 2004.
4. Правовая информатика и кибернетика. Учебник / Под ред. Н.С. Полевого. М., 2003.
5. Фигурнов В.Э. IBM PC для пользователя. М.: ИНФРА-М, 2007.
6. Яблоков Н.П. Криминалистическая характеристика финансовых преступлений // «Вестник Московского университета», Серия 11, Право, 2004. №6
7. Яковлев А.Н. Возможности компьютерно-технической экспертизы // Вопросы квалификации и расследования преступлений в сфере экономики. Саратов, 2004.
1. http://www.fbi.gov/priorities/priorities.htm [↑](#footnote-ref-1)
2. 2 Быстряков Е.Н., Иванов А.Н., Климов В.А. Расследование компьютерных преступлений, Саратов, 2001, с. 26 [↑](#footnote-ref-2)
3. 1 http://www.crime-research.org/library/Abstract\_Zvit.htm [↑](#footnote-ref-3)
4. 1 См. подробнее на http://www.crime-research.org/library/Steganos.htm [↑](#footnote-ref-4)
5. 1 www. legis.state. [↑](#footnote-ref-5)
6. 1 ст. 10 Доктрины информационной безопасности Российской Федерации от 9 сентября 2000 г. N ПР-1895 [↑](#footnote-ref-6)