# ПОДГОТОВКА СПЕЦИАЛИСТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ВАЖНЕЙШЕЕ НАПРАВЛЕНИЕ В СИСТЕМЕ ПРОФЕССИОНАЛЬНОГО ОБУЧЕНИЯ СОТРУДНИКОВ ПОЛИЦИИ

**А.А. Несмеянов,**
доцент кафедры автотехнической экспертизы и автоподготовки ФГОУ ВПО ВСИ МВД России, кандидат физико-математических наук

**А.Г. Подопригора,**
заместитель начальника кафедры автотехнической экспертизы и автоподготовки ФГОУ ВПО ВСИ МВД России кандидат технических наук, доцент

*В статье рассматриваются основные технические и правовые аспекты борьбы с преступлениями в области высоких технологий и кибертерроризмом и поднимается проблема подготовки квалифицированных профессиональных кадров для работы в этом направлении.*

*This paper deals with the basic technical and legal aspects of crime prevention in the spheres of high technology and cyber-terrorism. The problem of personnel training in this field is raised*[*].

В результате стремительного развития компьютерных технологий и их применения в различных сферах нашей жизни человечество вошло в новую эру информатизации, когда компьютер является необходимым инструментом в самых различных сферах жизнедеятельности человека. Углубляется зависимость человека и общества в целом, от компьютерных и информационных систем. Однако преступления, тем или иным образом связанные с компьютером, ущемление интересов пользователей и распространение заведомо ложной и другой опасной информации создают серьезную угрозу безопасности информационной системы, а также интересам государства, правам и свободам гражданина. Таким образом, проблема правовой защиты компьютерной и информационной систем, профилактика и противодействие компьютерным преступлениям становится актуальной для общества и государства.

[*] Nesmeyanov A.A., Podoprigora A.G. Information Security Training as an Important Component of the Police Officer Training System.

В настоящее время хорошо налаженная распределенная сеть информационно-вычислительных комплексов способна сыграть такую же роль в общественной жизни, какую в свое время сыграли электрификация, телефонизация, радио и телевидение вместе взятые. Ярким примером этому стало развитие глобальной сети Internet. Уже принято говорить о новом витке в развитии общественной формации - информационном обществе.

Любая экономическая и политическая деятельность тесно связана с получением, накоплением, хранением, обработкой и использованием разнообразных информационных потоков. Целостность современного мира как сообщества обеспечивается, в основном, за счет интенсивного информационного обмена. Приостановка глобальных информационных потоков даже на короткое время способна привести к не меньшему кризису, чем разрыв межгосударственных экономических отношений.

Конечно внедрение в управленческий процесс и другие сферы жизни общества электронно-вычислительной техники, без которой хранение, обработка и использование огромного количества самой разнообразной информации было бы невозможным, принесло неоценимую пользу в развитие науки, техники и других отраслей знаний. Однако выгоды, которые можно получить благодаря использованию этой техники, стали использоваться и в преступных целях. Так, появился новый вид преступной деятельности – компьютерные преступления, общественно–опасные последствия, от совершения которых не шли в сравнение с ущербом от других преступлений. По оценкам экспертов правоохранительных органов стран Центральной и Восточной Европы по вопросам борьбы с компьютерной преступностью, прибыли преступников от преступлений в сфере использования электронно-вычислительных машин занимают третье место после доходов наркоторговцев и от продажи оружия, а нанесенный ущерб уже сейчас оценивается миллиардами долларов. Только в США ежегодно экономические убытки от такого рода преступлений составляют около ста миллиардов долларов. К середине восьмидесятых годов прошлого столетия в Великобритании убытки от компьютерных преступлений составляли 750 миллионов фунтов стерлингов [1]. В настоящее время они возросли вдвое.

Таким образом, изучение проблем предотвращения и расследования преступлений в сфере компьютерной информации выступает одной из острейших проблем современной криминалистической науки. Остановимся на некоторых аспектах этой проблемы более подробно. Под компьютерным преступлением (интеллектуальной преступностью) подразумеваются несанкционированный доступ к компьютерным системам и базам данных и причинение ущерба, а также совершение уголовно наказуемого преступления посредством компьютера. Характерные черты подобного рода преступлений - его закрытость, интеллектуальность, многообразие, продолжительность и серьезная опасность, которую они представляют для общества. Английский ученый Н. Батлей выделил два вида компьютерных преступлений: при первом компьютер рассматривается как объект преступления, а при втором

— как инструмент преступления. В первом случае — это хищение компьютера и его комплектующих, хакерная атака и различного рода вредительство, распространение компьютерных вирусов и т.д.; во втором случае — это реализация порнографической продукции и пиратских компьютерных программ, мошенничество в Интернете с целью присвоения чужого имущества, а также и отмывание денег [2].

Объективную сторону рассматриваемых преступлений составляет неправомерный доступ к охраняемой законом компьютерной информации, который всегда связан с совершением определенных действий и может выражаться в проникновении в компьютерную систему путем [3]:

- использования специальных технических или программных средств, позволяющих преодолеть установленные системы защиты;
- незаконного использования действующих паролей или кодов для проникновения в компьютер либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя;
- хищения носителей информации, при условии, что были приняты меры к их охране, если это деяние повлекло уничтожение или блокирование информации.

Вышеперечисленные действия могут привести к целому ряду последствий, таких как

- уничтожение информации - удаление информации или изменение ее параметров, повлекшее за собой невозможность использования данной информации, вне зависимости от возможности ее восстановления;
- блокирование информации - совершение действий, приводящих к ограничению или закрытию доступа к компьютерной системе и предоставляемым ею информационным ресурсам;
- модификация информации - внесение изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе;
- копирование информации - перенос информации на другой материальный носитель, при сохранении неизмененной первоначальной информации;
- нарушение работы ЭВМ, системы ЭВМ или их сети - нарушение работы как отдельных программ, баз данных, выдача искаженной информации, так и при нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети.

С субъективной стороны рассматриваемое преступление может быть совершено только умышленно. Совершая неправомерный доступ к компьютерной информации, виновный осознает неправомерность своих действий, предвидит, что в результате его действий могут наступить приведенные ранее последствия, и желало либо сознательно допускало возможность их наступления. Совершение действий по неправомерному доступу к компьютерной информации предполагает наличие специальных знаний и опыта по работе с компьютерами, а сами современные

компьютерные системы имеют достаточно высокий уровень программной защиты от случайных ошибок.

Наиболее важным аспектом рассматриваемой проблемы является то, что сегодня преступные группы и сообщества для достижения корыстных целей все чаще применяют системный подход при планировании своих действий, разрабатывают оптимальные варианты проведения и обеспечения криминальных «операций», создают системы конспирации и скрытой связи, принимают дополнительные меры по оказанию эффективного противодействия сотрудникам правоохранительных органов, используя современные технологии и специальную технику, в том числе и всевозможные компьютерные устройства и новые информационно-обрабатывающие технологии [4].

Еще в 1987 г. Ю.М. Батурин писал, что «…мафия нуждается в компьютерах по трем причинам. Во-первых, мафия включена в крупномасштабный бизнес, где без компьютеров сегодня нечего делать. Во-вторых, из организаций, использующих компьютеры, удобнее вытягивать деньги тоже с помощью компьютеров. Наконец, в-третьих, силы безопасности и полиция используют такой мощный инструмент, как компьютер» [5]. Его предположения подтвердились. Уже в 1996 году 62 % преступников совершали такие преступления в составе преступных групп [6]. Отечественные криминалисты тогда пришли к выводу, что преступления в области компьютерной информации в России наиболее часто встречаются в области экономики и совершаются организованными преступными группами.

Сейчас, становится очевидным, что информационная компьютерная преступность перерастает в сферу профессиональную. Анализ, проведенный Академией ФСБ, показывает, что в настоящее время происходит формирование неформальных групп компьютерных «взломщиков» в некоторых учебных заведениях. Имеются сведения о привлечении организованными преступными группами хакеров к подготовке преступлений в кредитно-банковской сфере, на фондовом рынке. С их же помощью ведется контроль информации, накапливаемой в информационно-справочных и учетных компьютерных системах правоохранительных органов.

Сегодня, полиция по всему миру имеет подразделения по борьбе с компьютерными преступлениями, создаются специальные центры по обучению специалистов в этой области, ежегодно проводится целый ряд международных конференций и семинаров, посвященных данной проблематике. Например, в США существует «Национальное товарищество по обучению борьбе с киберпреступностью» (National Cybercrime Training Partnership – NCTP), которое охватывает местные, на уровне штатов и федеральные правоохранительные органы Соединенных Штатов, международная ассоциация руководителей полиции (International Association of Chiefs of Police – IACP) выступает в качестве принимающей стороны на Ежегодной конференции правоохранительных органов по информационному

управлению, темой которой являются IT-безопасность и киберпреступность. Европейский Союз создал орган под названием «Форум по киберпреступности». Множество стран подписало Конвенцию Совета Европы по киберпреступности, которая пытается стандартизировать европейские законы, касающиеся преступности в Интернете [7].

Таким образом, очевидно, что сегодня одной из важнейших проблем является потребность подразделений полиции МВД России грамотными компьютерными специалистами. Сотрудник полиции, работающий в областях связанных с защитой секретной служебной информации, расследованием компьютерных преступлений и т.п. конечно должен обладать всеми необходимыми навыками. Однако сейчас, очень часто, в этих областях работают люди, пришедшие после окончания гражданских ВУЗов, поэтому одним из приоритетных направлений развития образования в МВД является обучения именно специалистов в компьютерной сфере.

Конечно, за последние годы, был уже сделан целый ряд шагов в этой области. Так в московском университете МВД России существует факультет подготовки специалистов в области информационной безопасности, обеспечивающий реализацию образовательных программ с целью подготовки специалистов по защите информации высшей квалификации для подразделений органов внутренних дел, который готовит высококвалифицированных специалистов по комплексной защите информации, профессионально владеющих всеми методами и средствами защиты информации. Ежегодно проводятся научно-практические конференции по технологиям информационной безопасности в деятельности органов внутренних дел, с привлечением курсантов и слушателей факультета, профессорско-преподава-тельского состава профильных кафедр и сторонних вузов, на которых представляются результаты научных разработок по целому набору тематик - от развития представлений о технических каналах утечки информации, электромагнитного экранирования служебных кабинетов, использования генераторов акустического шума, применения тепловизоров до космических навигационных технологий, технологий радиочастотной идентификации, использования компьютерной стеганографии, а также технологий безопасного электронного документооборота, повышения качества подготовки специалистов, криминогенного потенциала ресурсов Интернета и информационного противоборства [8]. В Санкт-Петербургском университете МВД России существуют специальности «Организация и технология защиты информации», «Информационные системы и технологии», в Воронежском институте МВД России - специальность «Информационная безопасность телекоммуникационных систем». Изучаются отдельные предметы, такие как «Информационная безопасность и применение информационных технологий в борьбе с преступностью», «Информационная безопасность и применение информационных технологий в юриспруденции», «Защита информации» в Воронежском и Ростовском институтах МВД России, Омской академии МВД России, нашем институте. Тем не менее, из приведенных фактов видно, что

на территории Восточной Сибири и Дальнего Востока подготовка специалистов необходимого профиля практически не ведется, хотя потребность в них достаточно велика. Таким образом, открытие новой специальности в этом направлении в целом, или по крайней мере введение дополнительных профильных специальных дисциплин в частности отвечает требованиям текущего момента и является очень актуальным на сегодняшний день.

## ПРИМЕЧАНИЯ


1. Широков В.А., Беспалова Е.В. Компьютерные преступления: основные тенденции развития / В.А. Широков, Е.В. Беспалова // Юрист. – 2006. №10. – С. 18 – 21.

2. Хуэй Шэнь Ву, Фань Ин. Компьютерная преступность и правовое обеспечение информационной безопасности // Центр исследования компьютерной преступности (http://www.crime-research.org), 2009.

3. Егорышев А.С. Безопасность компьютерной информации в XXI веке. / А.С. Егорышев // Общество, государство и право России на пороге XXI века: теория, история. Межвузовский сборник научных трудов. / Уфа: УЮИ МВД России, 2000.

4. Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. Спб.: Арлит, 2002.

5. Батурин Ю.М. Право и политика в компьютерном круге. М.. 1987.

6. Крылов В.В. Расследование преступлений в сфере информации. М., 1998.

7. Компьютерная преступность - перед лицом проблемы / Д.Л. Шиндер // Центр исследования компьютерной преступности, 2010.

8. Материалы официального сайта Московского университета МВД России (http://91.192.71.100/).