Агентство финансовой полиции Республики Казахстан
Академия финансовой полиции

НАУЧНЫЕ ТРУДЫ АКАДЕМИИ ФИНАНСОВОЙ ПОЛИЦИИ

ВЫПУСК 4

Астана
2003

ББК 67. 402
Н 34

Редакционная коллегия:

Айкимбаев А.К. – ответственный редактор, кандидат юридических наук;
Сандрачук М.В. – кандидат экономических наук;
Омарова Ш.А. – кандидат экономических наук;
Рубенкова Н.Б. – кандидат экономических наук;
Сарыкулов К.Р. – кандидат юридических наук;
Смагулов А.А. – кандидат юридических наук;
Казина Р.А. – кандидат педагогических наук;
Кожетаева К.К. – ответственный секретарь.

Н 34 Научные труды Академии финансовой полиции. Выпуск 4 / Колл. авторов. – Астана: "Издательство "Парасат Әлемі", 2003. – 320 с.

ISBN 9965 - 9357 - 1 - 8

Академия финансовой полиции Агентства финансовой полиции Республики Казахстан с 2000 года ежегодно издает Научные труды.

В четвертый выпуск вошли научные статьи, посвященные актуальным проблемам обеспечения экономической безопасности государства.

Наряду с известными учеными Республики Казахстан и Республики Узбекистан в сборнике выступают молодые ученые, призванные внести свой вклад в дело построения правового государства.

Научные труды предназначены для практических работников органов финансовой полиции, других правоохранительных органов, занимающихся повышением своей профессиональной квалификации, преподавателей, научных сотрудников, слушателей и студентов вузов юридического и экономического профиля.

Н $\frac{1203020300}{00\ (05) - 04}$ **ББК 67. 402**

© Коллектив авторов, 2003
© Академия финансовой полиции АФП РК, 2003
© Общественный фонд "Достижения молодых", 2003
© "Издательство "Парасат Әлемі", 2003

ISBN 9965 - 9357 - 1 - 8

АВТОРСКИЙ КОЛЛЕКТИВ

Абдумажидов Г.М., директор Центра по правовой пропаганде Министерства юстиции Республики Узбекистан, доктор юридических наук, профессор, заслуженный деятель науки Республики Узбекистан;

Абдурасулова К., доцент кафедры уголовного права Ташкентского государственного юридического института Министерства юстиции Республики Узбекистан, кандидат юридических наук, доцент;

Абылкасимов К.Ж., старший преподаватель кафедры военной, физической и специальной подготовки Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, майор финансовой полиции;

Айтжанов А.Т., и.о. начальника научно-исследовательского центра Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат экономических наук;

Акбергенова Д.А., аспирант кафедры международных экономических отношений экономического факультета Российского университета дружбы народов, магистр экономических наук;

Алимкулов Р.С., консультант Конституционного Совета Республики Казахстан, кандидат юридических наук;

Асильбаева А.И., преподаватель кафедры таможенного дела Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, лейтенант финансовой полиции;

Арыстамбаева С.А., старший преподаватель кафедры социально-экономических дисциплин Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, капитан финансовой полиции;

Аубакирова А.Б., начальник учебно-методического кабинета кафедры специальных экономико-правовых дисциплин Академии финансовой полиции Агентства финансовой полиции Республики Казахстан;

Бауман Е.В., старший преподаватель кафедры уголовного права и криминологии Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, подполковник финансовой полиции;

Бектурганов О.Е., доцент кафедры военной, физической и специальной подготовки Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат педагогических наук, доцент, майор финансовой полиции;

Булгакбаев Б.А., Председатель Агентства финансовой полиции Республики Казахстан;

Есимбекова А.К., преподаватель кафедры государственно-правовых дисциплин Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, лейтенант финансовой полиции;

Ефимчук Н.Н., начальник отдела Департамента по борьбе с преступлениями и правонарушениями в сфере таможенного дела Агентства таможенного контроля Республики Казахстан;

Зуфаров Р.А., проректор по учебной работе Ташкентского государственного юридического института, кандидат юридических наук, доцент;

Кабжанов А.Т., старший преподаватель кафедры уголовного права и процесса Юридической академии "Фемида";

Казина Р.А., начальник кафедры языков Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат педагогических наук, доцент, майор финансовой полиции;

Казыбаев Е.С., доцент кафедры языков Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, капитан финансовой полиции;

Керимова К.К., преподаватель Института национального права и государственной службы Казахского гуманитарно-юридического университета;

Ким А.Г., доцент кафедры таможенного дела Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат технических наук, доцент;

Когамов М.Ч., первый проректор Казахского гуманитарно-юридического университета, доктор юридических наук, профессор, академик АЕН Республики Казахстан;

Крутько О.Г., преподаватель кафедры уголовного права Ташкентского государственного юридического института;

Куштарова Г.А., преподаватель кафедры уголовного процесса Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, старший лейтенант финансовой полиции;

Мурзахметов Б.Ш., старший преподаватель кафедры социально-экономических дисциплин Академии финансовой полиции Республики Казахстан, капитан финансовой полиции;

Омарова Ш.А., начальник кафедры специальных экономико-правовых дисциплин Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат экономических наук, доцент, подполковник финансовой полиции;

Оскеева Б.Р., старший преподаватель кафедры таможенного дела Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, старший лейтенант финансовой полиции;

Пак В.В., научный сотрудник научно-исследовательского центра Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, старший лейтенант финансовой полиции;

Примашев Н.М., старший преподаватель кафедры конституционного права и государственного управления Казахского гуманитарно-юридического университета, кандидат юридических наук;

Рубенкова Н.Б., начальник кафедры таможенного дела Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат экономических наук, доцент, майор финансовой полиции;

Салкебаев Т.С., преподаватель кафедры уголовного права и криминологии Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, старший лейтенант финансовой полиции;

Сарыкулов К.Р., начальник кафедры государственно-правовых дисциплин Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат юридических наук, доцент, майор финансовой полиции;

Смагулов А.А., начальник кафедры уголовного права и криминологии Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат юридических наук, доцент, майор финансовой полиции;

Сандрачук М.В., начальник кафедры социально-экономических дисциплин Академии финансовой полиции Агентства финансовой полиции Республики Казахстан, кандидат экономических наук, подполковник финансовой полиции;

теоретики и практики управления все чаще склоняются к той точке зрения, что некоторые конфликты даже в самой эффективной организации при самых лучших взаимоотношениях не только возможны, но и желательны.

Түйін

Дау туралы ойлағанда, жағымсыз әсерлер: қатер, қастандық, түсінбеушілік, өзінің адал екендігінді дәлелдей алмайтын әрекеттер еске түседі.

Нәтижесінде дау – барлық жағдайда, біздің әрбіреумізге,әсіресе басқаларға қарағанда даулармен жие кездесетін болғандықтан бастықтар мен менеджерлерге де қажетсіз, теріс екендігі туралы пікір қалаптасқан. Даулардан мүмкіндігінме алшақ болған абзал. Қазіргі кезде басқару теоретиктері мен практиктері кейбір даулардың ең жақсы қарым-қатынастарды нәтижелі ұйымдастар мүмкін емес, тіпті қажет екеніне бейім.

Abstract

The memoirs on the conflicts as a rule cause unpleasant associations: threats, animosities, misunderstanding, attempt, at times hopeless to prove the correctness, insult…

In result there was an opinion, that the conflict – always phenomenon negative, undesirable to each of us, and in particular for the chiefs, managers, as they should collide with the conflicts more often others. The conflicts are considered, as something such, that whenever possible is necessary to avoid. Presently theorists and practice of management are even more often declined to that point of view, that some conflicts even in the most effective organization at the best mutual relation not only are possible, but also are desirable.

Пак В.В.

ИНТЕРНЕТ КАК СРЕДА И ОРУДИЕ СОВЕРШЕНИЯ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

Современные информационные технологии стали важным фактором жизни общества и средством повышения эффективности управления всеми сферами общественной деятельности. Уровень информатизации становится одним из существенных факторов успешного экономического развития государства.

Сфера информатизации Казахстана, в силу действия объективных факторов, перехода от индустриального общества к обществу информационному, непрерывно расширяется. Казахстанский рынок информационных технологий, продуктов и услуг развивается достаточно динамично. Быстро развивается казахстанский сегмент сети интернет.

В странах, где уровень компьютеризации достаточно высок, проблема борьбы с компьютерной преступностью уже довольно давно стала одной из первостепенных. И это не удивительно. Так, в США ущерб от компьютерных преступлений составляет ежегодно около 5 млрд. долларов, во Франции эти потери доходят до 1 млрд. долларов в год, а в Германии при помощи компьютеров преступники каждый год ухитряются похищать около 2 млрд. долларов. И число подобных преступлений увеличивается ежегодно на 30–40 %.[1]

С развитием компьютерных и информационных технологий в Республике Казахстан проблема преступлений в данной сфере становится особо актуальной. Это обстоятельство вызвало необходимость разработки соответствующей законодательной базы. В новый Уголовный кодекс Республики Казахстан, введенный в действие с 1 января 1998 года, включена ст. 227 "Неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ", которая предусматривает наказание за неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы или ее сети.[2]

Следует сказать, что наличие законодательства, регламентирующего ответственность за компьютерные преступления, само по себе не является показателем степени серьезности отношения общества к таким преступлениям. К примеру, в Англии полное отсутствие специальных законов, предусматривающих наказание за компьютерные преступления, на протяжении многих лет отнюдь не мешает английской полиции эффективно расследовать дела такого рода. И действительно, все эти деяния можно успешно квалифицировать по действующему законодательству, исходя из конечного результата преступной деятельности (хищение, вымогательство, мошенничество или хулиганство). Ответственность за них предусмотрена уголовным кодексом.[3]

Как показывает практика, доля компьютерных преступлений составляет около 0,05 % от общего числа преступлений. Однако к этой статистике следует относиться осторожно. Дело в том, что долгое время в правоохранительных органах не было полной ясности относительно параметров и критериев, по которым следовало фиксировать совершенные компьютерные преступления, а также попытки их совершить. Можно предположить, что данные, учтенные официальной статистикой, составляют лишь вершину айсберга, подводная часть которого представляет существенную угрозу обществу. И для этого имеются серьезные основания. Правоохранительным органам становится известна лишь незначительная часть совершенных компьютерных преступлений. Их раскрываемость тоже невелика. Это связано с тем, что хищение информации долгое время может оставаться незамеченным, поскольку зачастую данные просто копируются. Жертвы компьютерной преступности проявляют нежелание контактировать с правоохранительными органами, опасаясь распространения среди своих настоящих и потенциальных партнеров сведений о собственной халатности и ненадежной работе своей фирмы, что может инициировать отток капитала и последующее банкротство.

Анонимность, которую предоставляет своим пользователям сеть интернет, возможность охвата большой аудитории, высокая скорость и гораздо более низкая стоимость распространения информации по сравнению с традиционными средствами делают интернет наиболее удобным инструментом для совершения преступлений.

Рассмотрим наиболее распространенные способы совершения преступлений с использованием компьютерных технологий.

Создание программ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации

Компьютерные вирусы в последнее время представляют собой настоящую эпидемию в глобальной сети. Так, компьютерный червь (разновидность вируса) "Welchia" поразил базу данных Государственного департамента США, содержащую данные о лицах, имеющих связи с террористами (свыше 13 миллионов). В результате был закрыл доступ к части сети, используемой для проверки информации о подавших заявление на получение визы.

К этой же группе можно отнести и такой вид преступления, как незаконное копирование и использование баз данных служебного

характера, результатом чего является возникновение нелегальных рынков сбыта конфиденциальной информации. Например, в сети на интернет-форумах, посвященных сотовой связи, появились сообщения о продаже базы данных абонентов сотового оператора. Объем базы – около 3 млн. абонентов, и содержит она такие сведения об абоненте, как его фамилия, имя и отчество, домашний и юридический адрес, паспортные данные, индивидуальный номер налогоплательщика (ИНН), дата подписания контракта с компанией и даже прошедшие платежи.

Несанкционированный доступ к информации

Жертвой хакеров может оказаться каждый. Так, летом 2000 года в Лондоне были арестованы двое граждан Казахстана, обвиненные во взломе компьютерной системы Агентства финансовой информации Bloomberg и вымогательстве у ее основателя и владельца Майкла Блумберга 200 тыс. долларов. Позднее с одного из них были сняты обвинения. 24 марта 2000 года Блумберг получил послание, в котором некий Алекс сообщал о том, что нашел доступ к информационной сети агентства. После того, как в подтверждение своих слов он прислал факс с личным компьютерным паролем и номером кредитной карты Блумберга и пригрозил разослать конфиденциальную информацию всем клиентам агентства, к расследованию было подключено ФБР. Предполагалось, что злоумышленник получил доступ к системе, работая в одной из крупных инвестиционных компаний Казахстана (Kazkommerts Securities), которая была клиентом агентства. Нью-йоркский суд признал автора послания виновным в вымогательстве и приговорил к 20 годам лишения свободы.

Блумберг не первая жертва "электронных шантажистов". В марте 2000 года полиция арестовала 18-летнего хакера из Уэльса (Великобритания), укравшего номер кредитной карты основателя корпорации Microsoft Билла Гейтса, а также получившего 26 тысяч номеров других кредитных карточек. Жертвой другого преступления стала туристическая компания Expedia – 22-летний выходец из России, живущий в США, нанес компании ущерб в размере 6 млн. долларов, пользуясь краденными номерами кредитных карт для заказов туристических услуг с сайта компании.

Многие компании предпочитают заплатить хакерам, нежели предавать дело огласке, подвергая сомнению свою репутацию.

Еще один пример использования информации, полученной незаконным путем, – это нелегальное получение товаров или услуг.

Так, в ноябре 2003 года в России впервые прошла операция по задержанию хакеров, сбывавших фальшивые номера карточек оплаты доступа в интернет. Два мошенника пытались поставить на поток продажу номеров карточек компании по предоставлению интернет услуг. В ходе следствия выяснилось, что злоумышленники взломали корпоративный сервер компании и получили доступ к программе, генерирующей номера платежных карт, в результате использования которой нанесли ущерб на сумму 150 тыс. рублей.

Сетевое мошенничество

Наряду с нелегальным получением товаров и услуг интерес для преступных группировок представляют такие сферы деятельности, как азартные игры (казино, лотереи и тотализаторы), организация финансовых пирамид, фиктивных брачных контор и фирм по оказанию мифических услуг. Во всех случаях оперативность взаимодействия с жертвами мошенничества, а также анонимность самого мошенника весьма привлекательны при совершении компьютерных преступлений в сети интернет.

В исследованиях Центра по борьбе с экономическими преступлениями и преступлениями в сфере высоких технологий (NW3C – National White Collar Crime Center) говорится, что наибольший риск представляют мошеннические интернет-аукционы (64 % от общего числа интернет-преступлений) и интернет-магазины (22 %), бесследно исчезающие после получения денег с доверчивых пользователей сети. Как показывает практика, именно эти способы нечестного заработка лидируют среди всех сетевых преступлений. Также интересно, что на пресловутые кражи номеров кредитных карт, которых больше всего боятся пользователи сети, приходится всего 5 % онлайновых мошенничеств.[4]

Эксперты Юридического Центра Общества Потребителей США (National Consumer Law Center) считают, что действия мошенников особо не отличаются разнообразием, и используют они лишь несколько широко известных приемов. Однако эти методы работают, несмотря на то, что об опасности подобных действий хорошо известно. Часть из них основана на доверии потенциальной жертвы – торговля фантастическим медицинским препаратом, часть – на безвыходном положении жертвы ("чистка" кредитной истории от негативной информации), часть – на стремлении человека помочь ближнему своему (уже в первые часы после трагических событий 11-го сентября в сети начали появляться сайты и рассылки от якобы пострадавших в террористических актах с просьбой пожертвовать

скромную сумму). Общаясь с потенциальными жертвами, мошенники обычно подчеркивают, что их деятельность абсолютно законна.

Но больше всего махинаций построено на эксплуатации человеческой жажды к лёгким деньгам. Это и вариации на тему всем известной пирамиды, и схемы с привлечением ценных бумаг, в которых для того, чтобы временно поднять цену на акции той или иной компании, используются миллионные спам-рассылки или фиктивные новости.

Интернет предоставляет уникальные возможности по вложению своих денег для разумных инвесторов, но не меньшие – и по их потере, ведь за считанные часы можно охватить многомиллионную аудиторию. Отчасти поэтому строгого определения интернет-мошенничества до сих пор нет: эксперты предпочитают причислять к этой категории любые аферы, в которых так или иначе используются ресурсы сети.

Каждый год появляются все новые схемы мошенничества. Так, совсем недавно был отмечен всплеск совершенно уникального вида махинации – кража личности (Identity Theft), в которой не требуется прямое участие жертвы. Суть схемы заключается в том, что мошенник тщательно собирает всю персональную информацию о потенциальной жертве (имя, адрес, паспортные данные, номер кредитной карты и т.д.), после чего с успехом выдаёт себя за него. В отличие от множества прочих схем, здесь максимально использует потенциал цифровой эпохи. А для того, чтобы найти такую информацию, вовсе не обязательно быть великим хакером, достаточно умело сыграть на психологии человека. Согласно данным eMarketer, 75 % детей выдадут незнакомцу в сети любую информацию, касающуюся членов семьи, в обмен на доступ к заинтересовавшему их веб-сервису.[5]

По данным Бюро Юридической Статистики (Bureau of Justice Statistics), в 2002 году жертвой мошенников стал каждый десятый американец. Эти данные были получены на основе опроса и не в полной мере отражают реальное положение дел. Этот же опрос показал, что в 2002 году о случаях мошенничества в полицию сообщали 49 % пострадавших.

В результате развития телекоммуникаций все больше мошенников начинает оперировать в виртуальном пространстве, в 2001 году впервые ущерб от мошенничеств, совершенных с помощью сети интернет и электронной почты, превысил ущерб, нанесенный

"традиционными" мошенниками. По данным Центра анализа интернет-мошенничества (Internet Fraud Complaint Center), среднестатистическая жертва интернет-преступления в 2002 году потеряла $845, жертва "традиционных" мошенников – $840.[6]

Экономические преступления в сети

Интернет – удобный инструмент для отмывания денег, то есть сокрытия нелегального источника их получения и превращения в законные вложения. Отследить и поймать преступников теперь сложнее, чем когда бы то ни было, в сети можно добиться практически полной анонимности.

"Потенциальный риск существует на всех стадиях общения нового клиента и финансового учреждения", – отмечается в отчете Международной организации по борьбе с отмыванием грязных денег (Financial Action Task Force on Money Laundering (FATF)), основанной странами Большой семерки. Но проблема "становится более серьезной, если процедура открытия счетов не предусматривает обязательной личной встречи". FATF также отмечает, что возможность доступа в интернет из любой точки земного шара еще более затрудняет обнаружение преступников. Не всегда сразу понятно, из какой страны осуществляется доступ к счету, а у обслуживающего персонала не хватает времени на проверку действий каждого пользователя.

В виртуальных казино деньги отследить еще сложнее. Игровые регистрационные записи хранятся на сайтах, часто расположенных в оффшорных зонах, в результате чего сильно затрудняется сбор доказательств преступной деятельности.

FATF предлагает ряд мер, которые могут помочь государствам в борьбе с отмыванием денег. Среди них:

- требование от интернет-провайдеров точной информации о своих клиентах;
- требование сохранения логов (отчетов) с параметрами доступа и телефонными номерами;
- обеспечение международной доступности подобной информации.

Однако наибольший интерес сеть интернет представляет именно как орудие для совершения преступлений в банковской сфере.

Одной из предпосылок повышенного интереса преступников к сети является то, что с развитием компьютерных сетей информация становится все более ценным товаром. Особенно это касается информации, имеющей отношение к сфере банков, – данные о вкладах

и вкладчиках, финансовом положении банка и клиентов, кредитной и инвестиционной политике банка, а также о направлениях его развития. Поскольку в современных условиях субъекты финансово-кредитной системы не могут существовать без взаимного информационного обмена, а также без общения со своими территориально удаленными филиалами и подразделениями, то часто для этих целей используется интернет. Это означает, что у преступников появляется возможность получить доступ к сугубо секретной информации о потенциальных объектах своей преступной деятельности. Даже одна угроза ее уничтожения может сама по себе послужить эффективным средством воздействия на руководство банка с целью вымогательства или шантажа.

Кибертерроризм

Следует также отметить такую особенность сети интернет, которая привлекает преступников, как возможность осуществлять в глобальных масштабах информационно-психологическое воздействие на людей. Преступное сообщество весьма заинтересовано в распространении своих доктрин и учений, в формировании общественного мнения, благоприятного для укрепления позиций представителей преступного мира, и в дискредитации правоохранительных органов. Экстремистские группировки, сепаратистские силы, проповедники идей, противоречащих общечеловеческим ценностям, интенсивно используют современные технологии для пропаганды своей идеологии и ведения информационных войн. Террористические акции в киберпространстве могут совершаться не только отдельными лицами или террористическими группами, но и одним государством против другого. В этом кибертерроризм ничем не отличается от любого другого вида терроризма.

Распространение порнографии

Немаловажной на сегодня проблемой является распространение порнографии. По данным Harding Institute, ежедневно в сети появляется 266 новых порносайтов, всего же их число превышает 70 тысяч.[7] Согласно результатам исследования, проведённого фирмой N2H2 Internet Content Filtering, на конец 2003 года число страниц, входящих в состав коммерческих порносайтов, превысило 260 млн. (для сравнения, в 1998 году специалисты N2H2 насчитали 14 млн. страниц). Результаты, приводимые N2H2, лишний раз доказывают: "запретные" виды бизнеса и в сети являются самыми доходными. Суммарный годовой доход преступником в этой сфере превышает 10 млрд. долларов.[8]

Мировое сообщество в полной мере осознало уровень возможных последствий от угрозы киберпреступности, так, в ноябре 2001 года государства-члены Совет Европы подписали Международную конвенцию об онлайновой преступности (киберпреступности). Совет, в состав которого входит 43 государства, ввел в текст конвенции дополнения, которые призваны гарантировать безопасность частной информации при расследованиях киберпреступлений, включая распространение компьютерных вирусов и использование краденых номеров кредитных карт. В ответ на критику со стороны Европейского Союза, в конвенции была изменена норма, предусматривающая, что страны-члены конвенции должны обеспечить все условия, чтобы их местное законодательство не противоречило постановлениям международных организаций о защите частной жизни. Кроме того, государства должны представить свое законодательство для независимого контроля. В то же время разработчики конвенции не пошли навстречу провайдерам интернет услуг, которые требовали смягчить существующие правила по хранению данных об их пользователях как минимум в течение 60 дней в случае, если они понадобятся для расследования.

Конвенция наделяет широкими полномочиями правоохранительные органы. По словам наблюдателей, эти полномочия иногда идут вразрез с законодательством некоторых стран, которые должны будут подписать конвенцию. В число таких стран входят США, Канада и Япония. Эта тема, а точнее, проблема соблюдения права невмешательства в частную жизнь, уже обсуждалась в США после того, как в прошлом году стало известно о намерении ФБР внедрить мощную систему "Карнивор", выборочно анализирующую электронную переписку с целью выявления террористов.

Таким образом, уникальность сети интернет, с одной стороны, заключается в том, что она не находится во владении какого-то физического лица, частной компании, государственного ведомства или отдельной страны, поэтому практически во всех ее сегментах отсутствует централизованное регулирование, цензура и другие методы контроля информации, благодаря этому открываются практически неограниченные возможности ее использования. С другой стороны, сеть интернет следует рассматривать не только как инструмент совершения компьютерных преступлений, но и как среду для ведения разнообразной преступной деятельности.

1. *Анин Б.Ю.* Защита компьютерной информации. – СПб.: БХВ-Петербург, 2000. – 384 с.

2. Комментарий к Уголовному кодексу Республики Казахстан / Отв. ред. д-р юрид. наук, проф. И.Ш. Борчашвили; канд. юрид. наук, доцент Г.К. Рахимжанова. – Караганда: РГК ПО "Полиграфия", 1999. – 960 с.

3. *Волокитин А.В., Манюшкин А.П., Курносов И.Н. и др.* Практические аспекты информатизации. Стандартизация, сертификация и лицензирование. Справочная книга руководителя / Под общ. ред. Л.Д. Реймана. – М.: ФИОРД-ИНФО, 2000. – 270 с.

4. NW3C – National White Collar Crime Center. http://www.nw3c.org/

5. eMarketer Internet, Business & Ecommerce Statistics Email Marketing & Online Market Research. http://www.emarketer.com/

6. Internet Fraud Complaint Center. http://www.ifccfbi.gov/

7. Harding Institute. http://www.harding.edu/

8. N2H2 Internet Content Filtering. http://www.n2h2.com/

Резюме

В статье дается характеристика преступлений, совершаемых с использованием возможностей сети интернет.

Түйін

Мақалада интернет желісін қолдану мүмкіндігімен жасалынған қылмыстарға мінездемелер беріледі.

Abstract

In this article are given the characteristic features of crimes committed through the Internet.

Асильбаева А.И.

ИНТЕГРАЦИЯ: ПЛАНЫ И ПЕРСПЕКТИВЫ (ЕВРАЗИЙСКИЙ ЭКОНОМИЧЕСКИЙ СОЮЗ)

Подавление путча 19–21 августа 19991 года привело к уходу КПСС с политической арены. С этого времени начался отсчет новой посткоммунистической эпохи.

Глубокий кризис и крах партийно-советской системы способствовали выходу союзных республик на самостоятельный путь развития. Главным мировым событием стал распад СССР. Перед новыми независимыми странами появились фундаментальные