Содержание:

ВВЕДЕНИЕ

В настоящее время, в России, так и за рубежом идет бурное процветания компьютеризации во всех деятельностях человека. Вычислительная техника широко используется во всех сферах жизнедеятельности людей. Персональные компьютеры, являются не только хранителями большой и важной информации, которая необходима для принятия важных решений, но и жизненно необходимом средством для облегчения и убыстрения всех человеческих процессов.

В современном мире, преступные группировки начинают активно пользоваться новой техникой и достижениями науки. Преступники для достижения своих корыстных мыслей и обеспечения преступной деятельности используют технические достижения, в том числе всевозможные устройства для компьютеризации.

Из вышесказанного можно понять, что в своей работе я расскажу подробно о компьютерных преступлениях, которые происходят с использованием средств компьютерной техники и информационно-обрабатывающей технологии. Также расскажу о причинах и методах совершения преступлений в сети Internet.

Глава 1. Понятие компьютерных преступлений

В нашей общественной жизни, компьютерная преступность, уже не ново, особенно в социально - экономических условиях.

Компьютерная преступность - это компьютерное преступление, где хранящийся в памяти компьютера информация выступает главным предметом преступных посягательств, а также нарушение закона, которые совершаются с помощью опасных деяний, предметом которых является хранящийся информация. В современном мире эти деяния являются одним из наиболее вредоносных и опасных явлений, которые посягают на безопасность сферы информации хранящийся в памяти вычислительной технике.

В уголовном законодательстве Российской Федерации предусмотрена специальная глава 28 «Преступления в сфере компьютерной информации». В этой главе рассматриваются на сегодняшний день всего три статьи:

- Статья 272. Неправомерный доступ к компьютерной информации.

Это деяние, когда за собой повлекло устранение, блокирование, трансформацию или копирование компьютерной информации.

- Статья 273. Создание, использование и распространение вредоносных компьютерных программ.

Создание, распространение или же внедрение компьютерных программ или другой компьютерной информации, заранее специализированных для несанкционированного удаление, блокирования, трансформации, копирования компьютерной информации или же нейтрализации средств обороны компьютерной информации.

- Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Несоблюдение правил эксплуатации средств сбережения, обработки или же передачи охраняемой компьютерной информации или информационно-телекоммуникационных сетей и оконечного оснащения, а еще правил доступа к информационно-телекоммуникационным сетям, повлекшее удаление, блокирование, трансформации или копирование компьютерной информации.

Ключевая индивидуальность компьютерных злодеяний – это сложность в установлении состава правонарушения и заключении вопроса о возбуждении уголовного дела. Компьютерная информация способна довольно проворно менять собственную форму, копироваться и пересылаться на всевозможные расстояния. Следствием сего считаются проблемы с определением первоисточника и субъекта совершения правонарушения.

Что такое компьютерное правонарушение и в чем оно состоит?

На данный вопрос не так уж и просто ответить, так как грани подобной работы никем еще однозначно не определены, нет абсолютной ясности в определении критериев и характеристик, по которым следует определять и закреплять компьютерные правонарушения и поползновение их совершения. Несомненно,

возможно считать, собственно, что компьютерное преступление, это каждое противозаконное воздействие, объектом которого считается информация, обрабатываемая в компьютерной системе, а орудием служит компьютер. Другими словами, компьютерные преступления, предполагает те же облики злодеяний, но производимые новыми орудиями и в новой сфере.

Компьютерные правонарушения считаются очень опасными. Это вызвано следующими основаниями:

- Правонарушения, производимые в компьютерной сфере недостаточно обширны, популярны и исследованы, так как обратили на себя интерес лишь только в 90-х годах.
- Причиной также считается их выявление, потому что современные способы их обнаружения малоэффективны.
- Предотвращение таких преступлений проблематично, так как способы и методы защиты постоянно отстают от средств и методов нападения.
- Такие правонарушение происходят в массовом масштабе, злоумышленники действуют на большом удалении, проследить их крайне непросто, потому что они затирают следы собственного присутствия.
- Компьютерная преступность повсеместно принимает организованный характер.
- Наказать обнаруженного правонарушителя не всегда представляется возможным: пользуясь несогласованностью правовых баз всевозможных государств, законопреступник может совершать «взломы» из страны, где аналогичная деятельность не является противозаконной.
- Нейтрализовать результаты компьютерных преступлений чрезвычайно сложно.

На сегодняшний день наиболее распространённым преступлением в компьютерной сфере считается компьютерное пиратство. Пиратство представляет собой нелегальное копирование и распространение программ для ЭВМ и БД. Угроза, таких поступков заключается в несоблюдение авторских прав и внедрение программ для ЭВМ и БД. Не считая того, компьютерное пиратство наносит значительный финансовый ущерб.

Изготовители компьютерного обеспечения, установила, что рынок на 94% удовлетворен контрафактной продукцией. Услугами и контрафактной продукцией пользуются не только граждане, но и государственные учреждения.

Основные облики компьютерных преступлений

Виды преступлений, связанных с вмешательством в работу компьютеров:

1. ***Несанкционированный доступ к информации, хранящейся в компьютере.***

Несанкционированный доступ осуществляется, как правило, с использованием чужого имени, измененного программного обеспечения, модифицированного IP – адреса, хищения информации и установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакер - лицо, совершающее доступы в компьютерные системы и сети с целью утехи, афер или же нанесения вреда. С одной стороны «хакер», это человек, великолепный техник – программист понимающий компьютер от «А» до «Я», а с иной – преступник, незаконно проникающий в компьютерные системы с целью получения информации.

Хакеры подразделяются на хороших и плохих, так как в переводе с английского с одной стороны, это «взломщик», а с другой «мастер».

«Хорошие хакеры» двигают технический прогресс и используют собственные познания и умения на благо населения земли. Ими созданно большое количество новых технических и программных систем.

Им, как водится, противостоят «плохие» - они читают чужие послания, крадут чужие программы и всеми доступными методами вредят современному населению земли.

1. ***Ввод в программное обеспечение «логических бомб».***

«Логическая бомба» – это программное обеспечение, которое включается при выполнение определенных критерий, и отчасти или же всецело уничтожает компьютерную систему.

“Временная бомба” – это одна из разновидность «логической бомбы», которая включается по достижении определенного момента времени.

Способ «троянский конь» состоит в тайном внедрение в чужую программу новых команд, которые дают возможность осуществлять в тайне новые программные функции, но при этом при всем сохранять прежнюю функциональность. С помощью

«троянского коня» злоумышленники, например, отчисляют на личный счет определенную сумму с каждой операции.

1. ***Разработка и распространение компьютерных вирусов.***

Компьютерный вирус - это вид вредоносного программного обеспечения, способного делать копии самого себя и внедряться в код иных программ, системные области памяти, загрузочные секторы, а еще распространять собственные копии по различным каналам связи. Процесс внедрения вирусом собственной копии в другую программу, именуется ***заражением***, а программа или другой объект, содержащий вирус - ***зараженным***.

Глава 2. Компьютерная безопасность, мировой опыт, мировые проблемы

Прошлый год был отмечен серьезным ростом сообщений о компьютерных преступлениях. Благодаря опросу организаций, у которых сумма утрат составляет в валютном эквивалентне, были выделены следующие опасности:

- кража денежных данных и подделка финансовых документов сотрудниками;
- кража критичной информации уволенными сотрудниками;
- саботаж сотрудников, извещенных о грядущим увольнении;
- кражи переносных компьютеров и их компонентов.

Тема хищения баз данных, содержащих «важную» информацию, вовсе не нова. Несложно догадаться, для какой работы предназначается данная информация адептам санкционированной преступности, различным махинаторам.

Составление аналогичных баз данных занимается достаточно большое количество государственных ведомств и ряд коммерческих структур. Главная сложность состоит в невозможности предоставить конкретный ответ на вопрос о происхождении данных. У всех баз, как правило, изменена оболочка, внесено что-нибудь свое, тем самым информация лишена собственных персональных признаков и спрятаны концы, по которым можно было бы установить ее источник.

Есть еще одна неувязка, с которой приходится сталкиваться следствию, - отсутствие заинтересованности со стороны потерпевших компаний к сотрудничеству с правоохранительными органами. Коммерческие структуры боятся

широкой огласки происшедшего по причине страха, лишится существующих и потенциальных клиентов. Аналогичная обстановка уже довольно давно стала свойственной для кредитно-финансовой сферы на Западе, когда банку выгоднее смириться с малозначительными потерями от тех или иных махинаций с электронной наличностью, чем разрешить случится оттоку части собственной клиентуры, усомнившейся в его абсолютной надежности.

С иной стороны, шила в мешке не утаишь, и жертвам все же стоит подумать о том, что наведение порядка в собственном жилище принципиально в первую очередь для них самих, потому что в конечном результате это лишь только укрепит их позиции на рынке. А пока следствие вынуждено находить нетрадиционные пути решения данной проблемы, обращаясь к гражданам через телевидение с призывом заявлять о понесенном ими вреде, потому что формальные владельцы украденных баз данных этого делать не спешат.

Необходимом нюансом проблемы распространения баз данных считается то, что часть из них относится к уровню сведений, представляющих коммерческую тайну. Это разрешает следствию инкриминировать обвиняемым ст. 183, ч. 2 Уголовного Кодекса РФ, которая предусматривает ответственность «за нелегальный сбор, разглашение и внедрение сведений, составляющих коммерческую тайну, без согласия обладателя из алчной или же другой личной заинтересованности».

Статья 11 Закона РФ «Об информации, информатизации и защите информации» относит индивидуальные данные к категории конфиденциальной информации и воспрещает сбор, хранение, внедрение информации о личной жизни, а также информации, нарушающей собственную тайну. Пункт 4 этой статьи, несомненно, указывает на то, что «подлежит обязательному лицензированию деятельность негосударственных организаций и частных лиц, связанная с обработкой и предоставлением пользователям персональных данных».

Если коммерческие структуры имеют разрешение на разработку и реализацию программного обеспечения, но фактически промышляют сбором и коммерческим распространением информационных баз, содержащих индивидуальные данные – налицо признаки преступления, предусмотренного ст. 171, ч. 2 Уголовного Кодекса РФ, «нарушение условий лицензирования с причинением крупного ущерба и с извлечением дохода в особо крупных размерах».

Раскрытие компьютерных преступлений – нестандартная, тяжелая и иногда дискуссионная проблема – как по основанию трудности самого факта доказывания,

так и в силу несовершенства действующего законодательства, которое разрешает обвиняемым «маневрировать» в оценке собственного деяния.

Каковы же перспективы? Они довольно туманны, и, прежде всего, потому, что наши силовые ведомства в данных случаях пристрастились идти по накатанной схеме: оперативная разработка – задержание – арест – следствие – суд. В приведенной цепочке любая служба постановляет свои личные задачи, нередко деятельность идет «от преступления» – есть сам факт, и надо найти правонарушителя. В сфере компьютерных преступлений эта методика неприемлема. Компьютерный законопреступник высокоинтеллектуален, в классическом осознание безусловно законопослушен, нередко одержим собственными мыслями. Вследствие этого для удачного противостояние с ними работники МВД, ФСБ, прокуратуры, судов обязаны владеть надлежащими познаниями и подготовкой. Потребуется создание предназначенных отрядов, которые вели бы постоянный мониторинг компьютерных сетей, периодической специализированной печати и других источников преступной и в пределах криминальной информации, воплощали ее быстрый анализ, оперативную помощь и реализацию, возбуждение уголовного дела (естественно, при наличии состава преступления). Соединенные Штаты уже пошли по данному пути. В каждом филиале ФБР созданы особые отделы по борьбе с компьютерными преступлениями, и все говорит за то, что было бы сносно последовать их примеру.

Глава 3. Методы взлома

В общем случае программное обеспечение любой универсальной компьютерной системы состоит из трех основных компонентов: операционной системы, сетевого программного обеспечения (СПО) и системы управления базами данных (СУБД). Вследствие этого все попытки взлома защиты компьютерных систем, возможно, разделить на три группы:

- атаки на уровне операционной системы;
- атаки на уровне сетевого программного обеспечения;
- атаки на уровне систем управления базами данных.

Атаки на уровне операционной системы

Защищать операционную систему, гораздо труднее, чем базы данных.

Более сложной задачей в соблюдении адекватной политики безопасности в современных операционных системах усложняется внутренний структурой, так как чрезвычайна сложна. Не правда, что атаки на операционные системы имеют все шансы быть организованы лишь только с поддержкой сложнейших средств, основанных на самых последних достижениях науки и техники, а хакер должен быть программистом высочайшей квалификации.

Никто не спорит с тем, что юзеру следует быть в курсе всех релизов в области компьютерной техники. Да и высочайшая квалификация - совсем не лишнее. Впрочем, искусство хакера состоит отнюдь не в том, чтобы взламывать любую самую "крутую" компьютерную защиту. Нужно элементарно суметь найти слабое место в конкретной системе защиты. При этом простейшие методы взлома оказываются ничуть не хуже самых изощренных, потому что чем легче метод атаки, тем больше вероятность ее окончание без ошибок и сбоев, особенно если возможности предварительного тестирования этого алгоритма в условиях, приближенных к "боевым", весьма ограничены.

Триумф реализации того или же другого алгоритма хакерской атаки на практике в значительной степени зависит от архитектуры и конфигурации определенной операционной системы, являющейся объектом данной атаки. Однако имеются атаки, которым может быть подвергнута практически каждая операционная система:

- кража пароля;
- подглядывание за юзером, когда тот вводит пароль, дающий право на работу с операционной системой;
- получение пароля из файла, в котором данный пароль был сохранен юзером, не желающим затруднять себя вводом пароля при подключении к сети;
- поиск пароля, который юзер, дабы не забыть, записывают па календарях, в записных книгах или на оборотной стороне компьютерных клавиатур;
- кража внешнего носителя парольной информации;
- полный перебор всех вероятных разновидностей пароля;
- подбор пароля;
- сканирование жестких дисков;
- сборка "мусора";
- превышение полномочий;
- запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы;

- модификация кода или же данных подсистемы защиты самой операционной системы;
- отказ в обслуживании;
- захват ресурсов;
- бомбардировка запросами;
- использование ошибок в программном обеспечении или же администрировании.

В случаи если в ПО компьютерной системы нет ошибок, и администратор соблюдает все правила политики безопасности, то хакерские атаки на операционную систему малоэффективны. Тем не менее, приходится признавать, что при всех соблюдений правил политики безопасности и от предпринятых мер всецело хакерские угрозы компьютерной системы на уровне операционной системы устранить невозможно.

Атаки на уровне сетевого программного обеспечения

Сетевое программное обеспечение, более уязвим, потому что канал связи, по которому передаются сообщения, не защищен, и кто имеет доступ к данному каналу, имеет возможность перехватывать и отправлять свою собственную информацию. Выделяются следующие хакерские атаки:

- прослушивание сегмента локальной сети;
- перехват сообщений на маршрутизаторе;
- создание неверного маршрутизатора;
- навязывание;
- отказ в обслуживании.

Для затруднения обмена информацией на уровне СПО, для незаконных юзеров сети, выделяются некоторые критерии безопасности:

- уменьшение объемов компьютерной сети;
- изоляция сети от внешнего мира;
- шифрование сетевых сообщений;
- электронная цифровая подпись сетевых сообщений;
- использование брандмауэров.

Атаки на уровне систем управления базами данных

Защита СУБД считается одной из самых несложных задач, так как имеет строго определенную структуру, и довольно элементарные действия (поиск, вставка, удаление и замена элемента). Иные операции считаются вспомогательными и использование у них довольно редкое. Благодаря наличию строгой структуру конкретных операций упрощает решение задачи защиты СУБД. Если СУБД использует ненадежные механизмы защиты, плохо проводилось тестирование версии, или содержит ошибки, то хакер с легкостью преодолеет защиту СУБД.

Глава 4. Контроль над компьютерной преступностью в России

К правовым мерам оотносятся разработка общепринятых норм, устанавливающих ответственность за совершение компьютерных правонарушений, защита авторских прав разработчиков, а также вопросы контроля за разработчиками компьютерных систем и использование интернациональных соглашений об их ограничениях. Меры контроля над компьютерной преступностью разделяются на правовые, организационно-тактические и программно-технические.

К организационно-тактическим мерам относятся хороший подбор персонала, исключения ведения важных работ, только одним человеком, охрана электронно вычислительных центров и т.п.

К программно-техническим мерам можно отнести применение мер защит от хищений, диверсий, взрывов, профилактику от компьютерных вирусов, установка сигнализации, установка биометрической системы защиты, защиту от несанкционированного доступа к системе и другое.

На сегодня ключевой целью государственной политики по выявлению и подавлению компьютерных преступлений, считается создание эффективной государственной системы борьбы с правонарушениями в сфере компьютерной информации.

Создаваемая система обязана быть снабжена высококвалифицированными кадрами. Создание целостной системы изучения, подготовки и переподготовки специалистов по борьбе с компьютерными преступлениями станет одной из основных задач.

В рамках ООН периодически ведутся симпозиумы по профилактике и подавлению компьютерной преступности, целью которых является поиск адекватных стезей противодействия на интернациональном уровне. Не считая того, создаются контрмеры против этого нового вида преступлений и универсально применимые стандарты и нормы, гарантирующие надежное использование компьютерных систем и средств телекоммуникаций.

Признано, собственно то, что для выработки всесторонней методики по профилактике и борьбе с компьютерной преступностью необходим единый согласованный план действий, включающий:

- неправительственные события, под которыми имеется в виду программа инициатив по внедрению основ ответственности в экономике и промышленности, стандартов профессиональной квалификации, технических и процедурных норм, а еще этических установок и кодексов поведения;
- правительственные меры, то есть воздействие правительства на национальном уровне, нацеленные на улучшение национального уголовного законодательства, а там, где это нужно, и промышленного изготовления средств противодействия компьютерным преступлениям;
- межправительственные меры и интернациональное сотрудничество, нацеленные на унификацию законодательных актов;
- международных стандартов и координацию действий органов уголовной юстиции.

ЗАКЛЮЧЕНИЕ

Компьютерные правонарушения - это особая плата за прогресс в технической сфере. С подъемом совершенства компьютерной техники растет изощренный характер компьютерной преступности. В соответствие с этим обязаны, стремится к совершенству способы борьбы с этим видом преступлений. Данные методы должны присваивать системный характер и принимать во внимание наряду с другими и общественные нюансы.

В науке уголовного права есть большое количество трактовок понятия компьютерное преступление. Под компьютерным правонарушением понимается противоправное общественно небезопасное деяние, причиняющие урон, или опасность причинения вреда публичным отношениям использования компьютерной информации.

В Уголовном Кодексе Российской Федерации интегрированны только три состава компьютерных правонарушений — неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

На данный момент хакерство и компьютерная преступность в РФ лишь только развивается и набирает обороты. Хакерству немало содействует сеть Internet с поддержкой, которой возможно не только обмениваться информацией, но и отыскивать нужные для законопреступников программы. К данному следует добавить собственно и то, что основная масса компьютерных взломов протекает без конкретного контакта с компьютером потерпевшего, и любой компьютер подключенный к сети Интернет находиться под опасностью конкретного взлома и кражи личной информации.

В связи с появление большого числа вирусов и вредоносных программ, стартовал подъем продаж антивирусной продукции. Это говорит нам собственно о том, что данная область стала прибыльной не только для преступников и хакеров, но и для тех кто борется с этой проблемой.

БИБЛИОГРАФИЯ

Нормативно-правовые акты:

1. Уголовный Кодекс Российской Федерации. - М.: ТК Велби, Изд - во Проспект, 2007. - 192 с.

2. Федеральный закон от 27.07.06 №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Справочная информационно-правовая система Консультант-Плюс

3. Федеральный закон от 9 июля 1993 года №5351-1 «Об авторском и смежных правах» (в ред. Федеральных законов от 19.07.1995 №110-ФЗ, от 20.07.2004 №72-ФЗ) // Справочная информационно-правовая система Консультант-Плюс

Специальная литература:

4. Комментарий к Уголовному кодексу Российской Федерации (под ред. Лебедева В.М.) - М.: Юрайт - М, 2002

5. Абызов К.Р., Гриб В.Г., Ильин И.С. Криминология: курс лекций / под ред. В.Г. Гриба. - М.: Маркет ДС, 2008. - 352 с.

6. Криминология: учеб. для студентов вузов, обучающихся по специальности «Юриспруденция» (Гуров А.И. и др.); научные редакторы - Н.Ф. Кузнецова, В.В. Лунеев. - М.: Вольтере Клувер, 2005. - 640 с.

7. Криминология: учеб. пособие / Г.И. Бауш и др.; под ред. Н.Ф. Кузнецовой. - М.: ТК Велби, Изд - во Проспект, 2007. - 328 с.

8. Криминология: Учебник / Под ред. В.Н. Кудрявцева и В.Е. Эминова - 3 - е изд., перераб. и доп. - М.: Юристъ, 2006 - 734 с.

9. Криминология: Учебник для вузов / под ред. д. ю. н. В.Н. Бурлакова, д. ю. н. Н.М. Кропачева - СПб.: Санкт - Петербургский государственный университет, Питер, 2004. - 427 с. - (Серия «Учебники для вузов»).

10. Криминология: Учебник для вузов / Под общ. ред. д. ю. н., проф. А.И. Долговой. - 3 - е изд., перераб. и доп. - М.: Норма, 2007. - 912 с.

11. Криминология: Учебник для вузов / под ред. проф. В.Д. Малкова - 2 - е изд., перераб. и доп. - М.: ЗАО «Юстицинформ», 2006. - 528 с.

12. Криминология: учеб. пособие / И.А. Моисеева, Г.Г. Шиханцов. - Минск: Амалфея, 2008. - 204 с.

Материалы периодической печати:

13. Копырюлин А. Квалификация преступлений в сфере компьютерной информации / А. Копырюлин // Законность. - 2007. - №6. - С. 40 - 42.

14. Степанов В. - Егиянц. Ответственность за компьютерные преступления / В. Степанов - Егиянц // Законность. - 2005. - №7. - С. 49 - 51.

15. Талимончик В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности / В.П. Талимончик // Правоведение. - 2008. - №2. - С. 103 - 110.

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

17. Доктрина информационной безопасности Российской Федерации: от 09.10.2000 № Пр-1895: (утвержден В.В. Путиным). - Электрон. Дан. - Режим доступа: http://www.agentura.ru/library/doctrina/

18. Уголовный Кодекс Российской Федерации: от 13.06.1996 N 63-ФЗ: (прият ГД ФС РФ 24.05.1996). - Электрон. Дан. - № 28. - Ст. 273. - Режим доступа: http://www.consultant.ru/popular/ukrf/ Литература

19. Кловский Д.Д. Теория передачи сигналов. - М.: Связь, 1984.

20. Рябков Б.Я., Фионов А.Н. Эффективный метод адаптивного арифметического кодирования для источников с большими алфавитами // проблемы передачи информации. - 1999. - Т.35.

21. Колесник В.Д., Полтырев Г.Ш. Курс теории информации. М.: Наука, 2006.

22. Акулов О.А., Медведев Н.В. Информатика базовый курс. М.: Омега-Л, 2005.

23. Успенский В. А. Машина Поста. М.: Наука, 1988. Ресурсы Интернет

24. Wikipedia.ru. [Электронный ресурс]: Свободная энциклопедия. - Электро. дан. - М., Режим доступа: http://ru.wikipedia.org

25. Федоров В. Компьютерные преступления: выявление, расследование и профилактика // Законность, 1994. № 6. С.44-47.

26. Формальный язык интерактивного общения (FLINT). М.: “ТАИС”, 1993. С. 205.

27. Хананашвили М.М. Информационные неврозы. М.: Медицина, 1986. С. 290.

28. Цуприков С. Новый этап автоматизации банков Московского региона // ComputerWorld, М., 1993. № 28.

29. Черкасов В.Н. Отметим, что теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. М., 1994.

30. Черкасов В.Н. О понятии “компьютерная преступность” // Проблемы компьютерной преступности. Минск: НИИПКК СЭ, 1992. С. 26-34.

31. Чугуев А.Д., Захарин С.И. Вирусный бизнес криминальной среды как социальная база для развития преступной деятельности по созданию вирусов // В сб.:

Подготовка специалистов в условиях изменяющейся структуры преступности и обновляющегося законодательства России. Волгоград: ВСШ МВД РФ, 1994. С.169-171.

32. Шальнев А. Наша мафия — самая компьютеризированная в мире // Известия, 1995. 15 фев.

33. Шаповалов А. ФБР вызывали? // Рос. газета, 1995. 29 апр.

34. Шрейдер Ю.А. Социальные аспекты информатики // НТИ, сер. 2. М.: Наука, 1989. № 1. С. 3-14.

35. Экономическая преступность в ФРГ и Швейцарии // Проблемы преступности в капиталистических странах. М.: ВИНИТИ, 1987. № 4. С. 3-10.

36. Яблоков Н.П., Колдин В.Я. Криминалистика: Учебник. М.: МГУ, 1990,