УДК 343.985.7
ББК 67.523.12 DOI 10.25724/VAMVD.BDEF

С. Г. Еремин, С. С. Домовец

СПОСОБЫ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ДИСТАНЦИОННО-БАНКОВСКОГО ОБСЛУЖИВАНИЯ И СЛЕДЫ-ПРИЗНАКИ ИХ ОБРАЗОВАНИЯ

В статье отмечается, что стремительное и глобальное развитие компьютерных информационных технологий существенно повлияло на организацию всех сфер жизнедеятельности общества, в том числе бизнеса. Так, стали очевидными автоматизированные функциональные процессы, в которых современные информационные технологии устранили расстояния, увеличили количество различного рода хозяйственно-финансовых операций. За последние годы системы дистанционного банковского обслуживания (ДБО) стали неотъемлемой частью взаимодействия коммерческих и иных организаций с банковской системой. Однако инновационные технологии в сфере компьютеризации, ее программного обеспечения привели к совершению преступлений, характеризующихся многообразием способов и профессиональных навыков определенных категорий преступников. В статье авторы рассматривают реальные проблемы, связанные с угрозой вмешательства киберпреступников в работу финансовых компаний и их клиентов. Оперативные сотрудники, следователи, эксперты все чаще сталкиваются с различными преступлениями, затрагивающими интересы финансовых организаций и граждан. Это DDos-атаки (распределенные атаки на отказ в обслуживании), подрыв репутации путем размещения в Интернете клеветы, оскорблений, а также мошенничество в системах дистанционного банковского обслуживания, взлом серверов и хищение конфиденциальной информации и денежных средств. Каждое из этих незаконных действий пагубно отражается на хозяйственно-финансовой и иной деятельности пострадавших компаний и граждан, но наибольший финансовый ущерб наносит мошенничество в системах интернет-банкинга: клиент-банк, интернет-клиент. Первая система направлена на обслуживание банком юридических лиц, вторая — физических лиц. В целях повышения эффективности раскрытия и расследования преступлений в сфере ДБО авторы изложили некоторые важные элементы криминалистической характеристики, содержащие специфическую информацию, способствующую выдвижению версий, проведению следственных действий для получения доказательств преступления данного вида, установлению лиц, его совершивших.

Ключевые слова: криминалистическая характеристика, компьютерная информация, доказательства преступления, интернет-банкинг, юридические лица, физические лица, способы преступления, следы-признаки преступления, следственные версии, дистанционно-банковское обслуживание.

S. G. Eremin, S. S. Domovets

MODI OPERANDI OF CRIMES COMMITTED IN THE SPHERE OF REMOTE BANKING SERVICE AND TRACES-ELEMENTS OF THEIR FORMATION

It is stated in the article that rapid and global computer information technologies development has considerably influenced the overall life organization, which includes business all over the world. So, some automated functional processes have become evident, in which modern information technologies have smoothen distances, have increased the number of different kind of business and financial operations. Over the last years, the systems of remote banking service (RBS) have become an essential part of commercial and other organizations cooperation with the banking sector. In the article we touch upon real issues, related to the thread of cybercriminals intervention into financial companies' and their clients' work. Operatives, investigators and experts increasingly deal with different crimes that affect interests of financial organizations and people. They are DDos-attacks (distributed denial-of-service based attacks), reputation damage by means of libel and

obscenities online publishing as well as remote banking service systems fraud, hacking servers, embezzlement and sensible information pilfering. Each of these illegal acts affects detrimentally business and other kind of companies and people's activity, but maximum financial loss might be caused by fraud in the internet-banking systems: online baking, internet client. The first system is designed for wholesale banking; the second — for personal banking. In order to enhance DBS related crimes detection, the authors have stated some of the important elements of forensic characteristics, which contain specific information, promoting leads suggestion and investigative measures in order to receive evidence of this kind of crime and identify perpetrators.

Key words: forensic characteristic, computing information, evidence of a crime, internet-banking, juridical entities, physical entities, modi operandi of crimes, traces-elements of crimes, investigative leads, remote banking service.

Быстрое и глобальное развитие компьютерных информационных технологий существенно повлияло на организацию бизнеса во всем мире: стали очевидными автоматизированные функциональные процессы, устранилась проблема расстояния, увеличилось количество различного рода хозяйственно-финансовых операций. В частности, сегодня можно хранить корпоративные данные на сервере в Малайзии, а осуществлять платежи в другом государстве, или, находясь в Волгограде, оказывать услуги иранским партнерам и т. д. Глобальность позволяет совершать хищения компьютерной информации и предоставляет заинтересованным лицам неправомерный доступ к содержанию этой информации [1].

В толковом словаре русского языка С. И. Ожегова обозначены два определения термина «информация». Первое сводится к тому, что это «…сведения об окружающем мире и протекающих в нем процессах, воспринимаемые человеком или специальным устройством». Второе, что это «…сообщения, осведомляющие о положении дел, о состоянии чего-нибудь (научно-техническая и газетная информация, средства массовой информации — печать, радио, телевидение, кино)» [2].

К. К. Колин пишет: «Информация — это не плод нашего воображения, не продукт деятельности сознания, а реальный физический феномен, характеризующий состояние и движение материи или энергии» [3]. Вместе с тем М. С. Цветкова и Л. С. Великович отмечают: «Сведения — это знания, выраженные в сигналах, сообщениях, известиях, уведомлениях и т. д.» [4].

За последние годы системы дистанционного банковского обслуживания стали неотъемлемой частью взаимодействия коммерческих и иных организаций с банковской системой. Все чаще финансовые операции совершаются с помощью сети Интернет, а возможность удаленного доступа к банковским услугам в режиме реального времени важна в решении различного рода вопросов современного бизнеса. Удобство применения таких систем позволяет снизить издержки и повысить оперативность проведения финансовых операций.

Дистанционное банковское обслуживание — это комплекс сервисов удаленного доступа клиентов к банковским услугам. При этом клиент удаленно (без визита в банк) передает необходимые распоряжения, используя информационные технологии. Существует большое количество терминов, используемых в качестве синонимов для описания услуг дистанционного банковского обслуживания через Интернет: клиент-банк, банк-клиент, электронный банкинг и пр. Встречаются и англоязычные варианты обозначений (online-banking, remote banking, e-banking, home banking, internet banking и т. д.).

Однако, несмотря на разное количество терминов, связанных с наиболее распространенным видом ДБО, системы электронного банкинга сводятся к двум основным типам систем, в которых и совершается большая часть преступлений: клиент-банк, интернет-клиент.

Первая направлена на обслуживание банком юридических лиц, вторая — физических лиц. Обе системы объединяет то, что доступ к ним осуществляется через персональный компьютер, а для соединения с банком используется Интернет. Принципиальное отличие состоит в том, что для системы «Клиент-банк» на компьютере устанавливается специальная программа, а для системы «Интернет-клиент» достаточно обычного браузера (рис. 1).

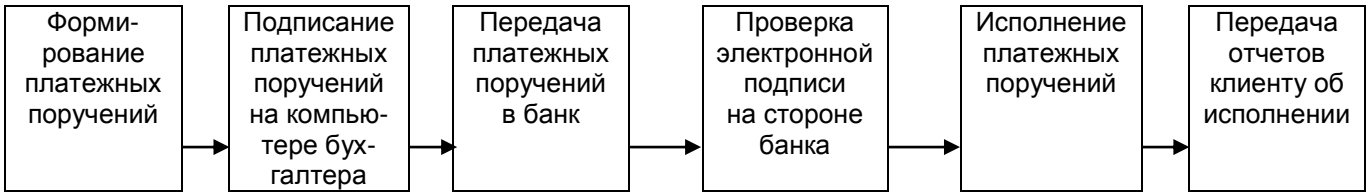

Рис. 1. Схема дистанционного банковского обслуживания

На схеме видно, что дистанционное банковское обслуживание — это вполне приемлемая, удобная, доступная и оперативная форма обоюдного взаимодействия банка и клиента, несущая выгоды обеим сторонам.

Однако кроме преимуществ применение информационных технологий ДБО обозначило новые, ранее не известные и даже не предполагаемые проблемы для добросовестных пользователей. Одна из них — угроза вмешательства киберпреступников в работу финансовых компаний и их клиентов. Оперативные сотрудники, следователи, эксперты стали сталкиваться с различными преступлениями, затрагивающими интересы финансовых организаций и граждан. Это DDos-атаки, подрыв репутации путем размещения в Интернете клеветы, оскорблений, а также мошенничество в системах дистанционного банковского обслуживания, взлом серверов и хищение конфиденциальной информации и денежных средств. Каждое из этих незаконных действий пагубно отражается на хозяйственно-финансовой и иной деятельности пострадавших компаний и граждан, но наибольший финансовый ущерб наносит мошенничество в системах интернет-банкинга. В связи с этим представляется важным рассмотреть содержание отдельных элементов криминалистической характеристики преступлений, совершаемых в сфере дистанционного банковского обслуживания. В криминалистической литературе традиционно выделяют такие элементы криминалистической характеристики, как: 1) способ подготовки, совершения и сокрытия преступления; 2) личность преступника; 3) механизм следообразования; 4) предмет преступного посягательства; 5) обстановка совершения преступления (место, время) и др. Рассмотрим наиболее значимые из них применительно к преступлениям в сфере ДБО.

Под способом совершения преступления принято понимать детерминированный целым рядом субъективных и объективных факторов комплекс действий субъекта (субъектов) по подготовке, совершению и сокрытию преступного деяния [5]. В частности, Я. П. Яблоков указывает на «…очевидное проявление закономерных связей между способом совершения преступления и формой его отражения в окружающей среде…» [6].

Следует иметь в виду, что необязательно, чтобы способ преступления включал все названные элементы, поскольку существуют преступления, где злоумышленник может не осуществлять никаких действий по сокрытию или не может их осуществить (например, в силу своего болезненного состояния), что бывает редко. Все же преступник при совершении преступлений, требующих интеллектуального подхода, стремится уничтожить оставленные следы, фальсифицировать обстановку происшествия либо непосредственно самих следов. Цель этих действий предполагает, с одной стороны, воспрепятствование своевременному обнаружению преступления, с другой — сокрытие возможности установления личности преступника. Многие ученые-криминалисты считают способ совершения преступления центральным звеном криминалистической характеристики, а другие ее элементы, связанные с ним, хотя и имеющие самостоятельное значение, признают второстепенными. В то же время бесспорно установлено наличие корреляционной зависимости между способом преступления и личностью преступника, обстановкой (временем и местом) совершения преступления и личностью преступника, механизмом следообразования и другими структурными элементами криминалистической характеристики.

Н. И. Шумилов обозначает три группы «информационных» способов совершения преступлений, где объектом посягательства является информация, содержащаяся на машинных носителях:

1) незаконное изъятие носителей информации;

2) несанкционированное получение информации;

3) неправомерное манипулирование информацией [7].

В целом мы признаем эту классификацию удачной. Однако в ней есть некоторые недостатки: в частности, незаконное изъятие носителей информации может восприниматься как хищение компонентов техники, содержащей такую информацию, т. е. квалифицироваться как кража собственности.

Ю. Ляпунов и В. Максимов полагают, что предметом рассматриваемых видов преступлений выступает компьютерная информация либо информационные ресурсы машинных носителей в системе ЭВМ или их сети [8]. На этом основании, на наш взгляд, действия преступников, похитивших компьютер, надлежит квалифицировать по совокупности преступлений против: а) собственности; б) компьютерной информации (в случае, когда установлен неправомерный доступ к охраняемой законом информации).

Справедливой представляется позиция В. Б. Вехова, полагающего, что «…способы совершения рассматриваемых видов преступлений делятся в зависимости от их вида: во-первых, когда компьютерная техника выступает в роли объекта посягательства; во-вторых, когда она же выступает в роли орудия и средства совершения преступления». В первом случае, по мнению ученого, объектом преступного посягательства является информация, находящаяся в компьютере, несанкционированный доступ и манипулирование ею возможно с использованием средств компьютерной техники. В. Б. Вехов не отрицает, что такие же действия могут быть совершены и без нее (физическое уничтожение жесткого диска компьютера с находящейся на нем информацией). Вместе с тем автор, считая, что в качестве орудия преступления выступает компьютерная техника, подразумевает ее использование как для получения несанкционированного доступа, прослушивания и перехвата сообщений, так и для хранения информации (например, баз данных номеров украденных автомобилей) [9]. В результате очевидно отсутствие границ отнесения того или иного способа совершения рассматриваемых видов преступлений к какой-либо группе способов по причине взаимной интеграции содержания понятий. С учетом сказанного предлагаем из существующих оснований классификации видов преступлений и, соответственно, способов их совершения, выделить те, в которых:

а) информация в устройствах компьютерного типа выступает в роли объекта посягательства;

б) компьютерная техника и средства коммуникации выступают в роли орудия и средств совершения преступления;

в) к информации, находящейся на машинных носителях, возможны неправомерный доступ, а также манипулирование ею в преступных целях только при использовании аппаратных и программных средств компьютерной и иной техники (смешанную группу способов), т. е. частные виды первых двух групп способов совершения рассматриваемых преступлений нужно объединить в третью группу. Итак, способы совершения преступлений в сфере высоких информационных технологий, включая ДБО, мы делим на следующие три группы способов, в которых:

1) объектом посягательства является информация, находящаяся на машинных носителях (компьютерах, мобильных телефонах, электронных записных книжках и т. д.);

б) компьютерная техника, средства коммуникации и т. д. выступают в виде орудий и средств совершения и сокрытия преступления;

в) применяются высокотехнологичные устройства и их использование направлено на получение незаконного доступа к информации, ее модификации или блокирования и оперирования ею в преступных целях.

Как представляется, перечисленные группы объединяют большое количество способов совершения преступлений в сфере высоких информационных технологий. Однако каждый конкретный способ может быть отнесен к той или иной группе по классификационным основаниям, под которыми подразумеваются приемы совершения определенных действий в преступных целях. Для отнесения того или иного способа к конкретной группе способов совершения преступлений в сфере высоких информационных технологий, где объектом посягательства становится информация, находящаяся на машинных носителях, классификационным основанием является метод блокирования, т. е. выполнение преступником действий, физически приводящих к блокировке или уничтожению информации на машинных носителях (разукомплектованию устройств, использованию физических и химических методов воздействия на них, ограничению к ним доступа в виде организации завалов в ходе взрыва и др. в целях временного затруднения доступа либо полного уничтожения). Подобная ситуация будет очевидна при краже.

Так, в США преступники похитили компьютеры с важной информацией стоимостью полмиллиарда долларов, что рассматривалось как промышленный шпионаж против Interactive Television Technologies Inc. Похищенная информация являлась секретным коммерческим проектом по превращению каждого телевизионного приемника в устройство доступа к сети Интернет [10].

Рассмотрим наиболее распространенный способ мошенничества в системах интернет-банкинга, который состоит из трех основных этапов:

1. Получение информации для осуществления неправомерного доступа в систему «Клиент-банк».

2. Проведение мошеннической операции.

3. Обналичивание денег.

В первом случае для хищения авторизационных данных пользователя системы ДБО (логина, пароля и ключей электронной цифровой подписи) преступники используют специальное вредоносное программное обеспечение (ПО). Чаще всего это модификации известных банковских троянов: Zeus, SpyEye, Carberp — с дополнительным функционалом. Схема работы таких вирусов следующая: сотрудник компании (гражданин) посещает зараженный веб-сайт, с которого на его компьютер, используя ту или иную уязвимость, загружается вредоносная программа, обходящая антивирусную и другие виды защит. Попадая на компьютер, такая программа определяет, с какими приложениями работает пользователь. При обнаружении следов работы с системами дистанционного банковского обслуживания или системами электронных денег на компьютер дозагружаются вредоносные модули, предназначенные для хищения авторизационных данных пользователя. Все эти данные вместе с сопутствующей информацией, например, о количестве денежных средств на банковских счетах, попадают в руки преступников. Современные банковские вирусы, например, трояны имеют широкий функционал и способны работать одновременно с несколькими компьютерными системами дистанционного банковского обслуживания, обеспечивая киберпреступникам возможность удаленного доступа и сокрытия следов преступлений.

Во втором случае при получении данных от вируса трояна мошенники проверяют полученные сведения и определяют возможности для совершения преступления. Важную роль на данном этапе совершения преступления играют средства защиты ЭВМ, применяемые банком и его клиентом (рис. 2).

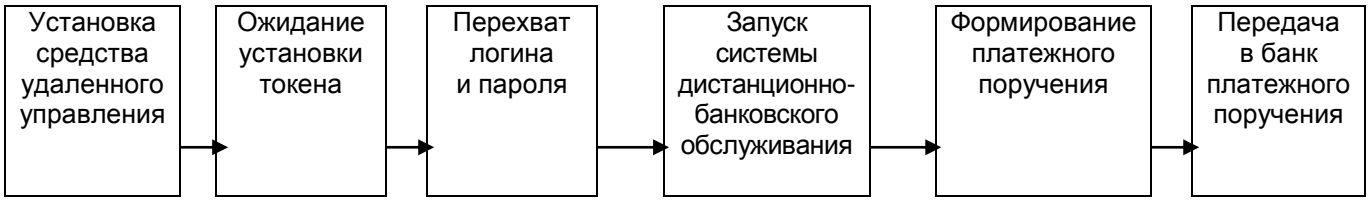

Рис. 2. Схема мошеннической финансовой операции

Для отправки подложного платежного поручения мошенники могут использовать различные возможности вредоносных программ, например, отправить платежное поручение непосредственно с компьютера клиента банка с использованием средств удаленного управления или автоматически формировать мошенническое платежное поручение вирусом и подменить вредоносной программой реквизиты легитимного платежного поручения за мгновение до его подписания и передачи в банк.

После отправки платежного поручения в банк основная задача преступников сводится к ограничению доступа легитимного пользователя к системе «Клиент-банк». Для этого применяют различные способы (смену пароля от системы интернет-банкинга, вывод из строя компьютера пользователя, DDos-атака на сервер банка). Конечно же, преступники стремятся повредить файловую систему жесткого диска пользователя или удалить один из компонентов операционной системы. Пока клиент банка занят восстановлением работоспособности компьютера, денежные средства покидают его счет и попадают в руки преступников.

В третьем случае обналичивание денежных средств обычно осуществляют специализированные группы лиц, связанные с организованными группами. Схема обналичивания продумывается при подготовке к хищению денежных средств, предполагаемых к выведению. При небольших суммах, например до двух млн руб., часто используют банковские пластиковые карты физических лиц (предпочтительны с большими лимитами по выдаче наличных средств в банкоматах). Если же предполагается вывести значительные суммы денежных средств, преступники используют цепочку счетов подставных компаний и физических лиц с разделением средств на мелкие для снятия денег через банкомат (рис. 3).

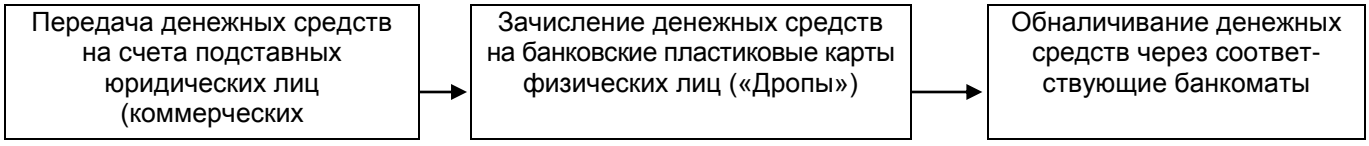

Рис. 3. Схема обналичивания похищенных денежных средств

Рассмотренные нами примеры представляют собой лишь некую общую схему, часто используемую мошенниками в качестве основы с добавлением в нее различных промежуточных этапов.

В целом сценариев совершения мошенничества в системах интернет-банкинга по хищению и легализации (обналичиванию) денежных средств может быть множество. Они зависят от профессиональных навыков преступников.

Следует отметить, что общим для всех способов совершения преступлений в сфере высоких информационных технологий является единый механизм следообразования, под которым понимается специфическая конкретная форма протекания процесса. Его конечная фаза — образование следа.

В отличие от традиционно рассматриваемого в криминалистике физического следообразующего воздействия (механического или теплового) здесь будет иметь место другой механизм следообразования (физико-химическое воздействие, сопряженное с механическим). Так, механическое движение нажатия пальцем руки на какую-либо клавишу клавиатуры компьютера вызовет изменение напряжения и силы тока в электрической цепи, что может повлечь изменение магнитного поля носителя информации (при ее сохранении или копировании) либо передачу этого электрического импульса по каналам коммуникаций к другому компьютеру (при обмене информацией) или может быть вновь преобразовано в механическое движение головки принтера (при распечатывании информации).

Механизм следообразования, характерный для определенного вида или группы преступных посягательств, предполагает содержание сведений о локализации следов, их признаках, видах, сохранности и других криминалистически значимых данных, способствующих эффективному поиску и работе с ними. Обнаружение, фиксация, изъятие и исследование следов-признаков преступления является неотъемлемым компонентом предварительного расследования, на котором при дальнейшем исследовании формируются криминалистические версии. Полагаем, прав Б. Анин, который отмечает, что предлагаемая учеными-криминалистами Г. Л. Грановским, А. Я. Гинзбургом, Г. И. Поврезнюком, А. В Калининым и другими традиционная классификация следов-признаков совершения тех или иных преступлений не охватывает виды новых преступлений, в том числе в сфере высоких информационных технологий [11].

Полагаем, что для следообразующего воздействия в сфере высоких информационных технологий очевидны следующие виды следов, указывающих на признаки преступлений:

а) программы и текстовые файлы и (или) их части, не входящие в стандартный состав системы, функционирующей в данном устройстве ранее, до совершения преступления;

б) наборы команд, отдельных знаков, символов и т. д., содержащихся в программах системы, текстовых и иных документах, которые были умышленно внесены преступником в систему для изменения ее свойств, возможностей, содержания и т. п.;

в) записи в учетных файлах системы, так называемые log-файлы, в которых содержится информация о пользователях (не только о преступниках), когда-либо использовавших данное устройство, регистрирующих особенности работы пользователя в системе, время его работы и т. д., причем количество регистрируемых служебных параметров зависит как от функционирующей в данном устройстве системы, так и от проводимой на нем политики безопасности.

Естественно, перечисленные следы-признаки не являются традиционными, исчерпывающими и не могут быть отнесены ни к одной существующей в криминалистике группе следов.

1. Рабовский С. В., Маевский Л. С. Основы информационной безопасности: содержание и правовое обеспечение. М., 2002.

2. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. 22-е изд., стер. М., 1990.

3. Колин К. К. Эволюция информатики // Информационные технологии. 2005. № 1. С. 2—16.

4. Цветкова М. С., Великович Л. С. Информатика и ИКТ. 3-е изд., стер. М., 2012. С. 21.

5. Криминалистика: учебник / под ред. И. Ф. Герасимова, Л. Я. Драпкина. М.: Высшая школа, 1999. С. 331.

6. Яблоков Я. П. Криминалистическая характеристика преступлений как составная часть общей криминалистической теории // Вестник МГУ. Сер. Право. 2000. № 2. С. 3.

7. Шумилов Н. И. Криминалистические аспекты информационной безопасности: дис. … канд. юрид. наук. СПб., 1997.

8. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1.

9. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / под ред. акад. Б. П. Смагоринского. М., 1996.

10. Kabay M. E. The Information Security Year in Review. National Computer Security Association (NCSA) News, 1997.

11. Анин Б. Защита компьютерной информации. СПб., 2000. С. 18.

1. Rabovsky S. V., Maevsky L. S. Fundamentals of information security: contents and legal coverage. M., 2002.

2. Ozhegov S. I., Shvedova N. U. Definition dictionary of Russian language. 22nd edition, stereotype M., 1990.

3. Kolin K. K. Information science evolution // Information technologies. 2005. No. 1. Pp. 2—16.

4. Tsvetkova M. S., Velikovich L. S. Information science and ICT. 3rd edition stereotype. M., 2012. P. 21.

5. Criminalistics: College textbook / under the editorship of I. F. Gerasimov, L. Y. Drapkina. M.: Vysshaya shkola, 1999. P. 331.

6. Yablokov Ya. P. Forensic characteristic of crimes as an aspect of general forensic theory // Annals of MSU. Series Pravo. 2000. No. 2. P. 3.

7. Shumilov N. I. Forensic aspects of information security: thesis for a Candidate degree in Law sciences. St. Petersburg, 1997.

8. Lyapunov U., Maksimov V. Liability for computer related crimes // Legality. 1997. No. 1.

9. Vekhov V. B. Computer related crimes: modi operandi and detection / under the editorship of academic B. P. Smagorinsky. M., 1996.

10. Kabay M. E. The Information Security Year in Review. National Computer Security Association (NCSA) News, 1997.

11. Anin B. Computer information protection. St. Petersburg, 2000. P. 18.