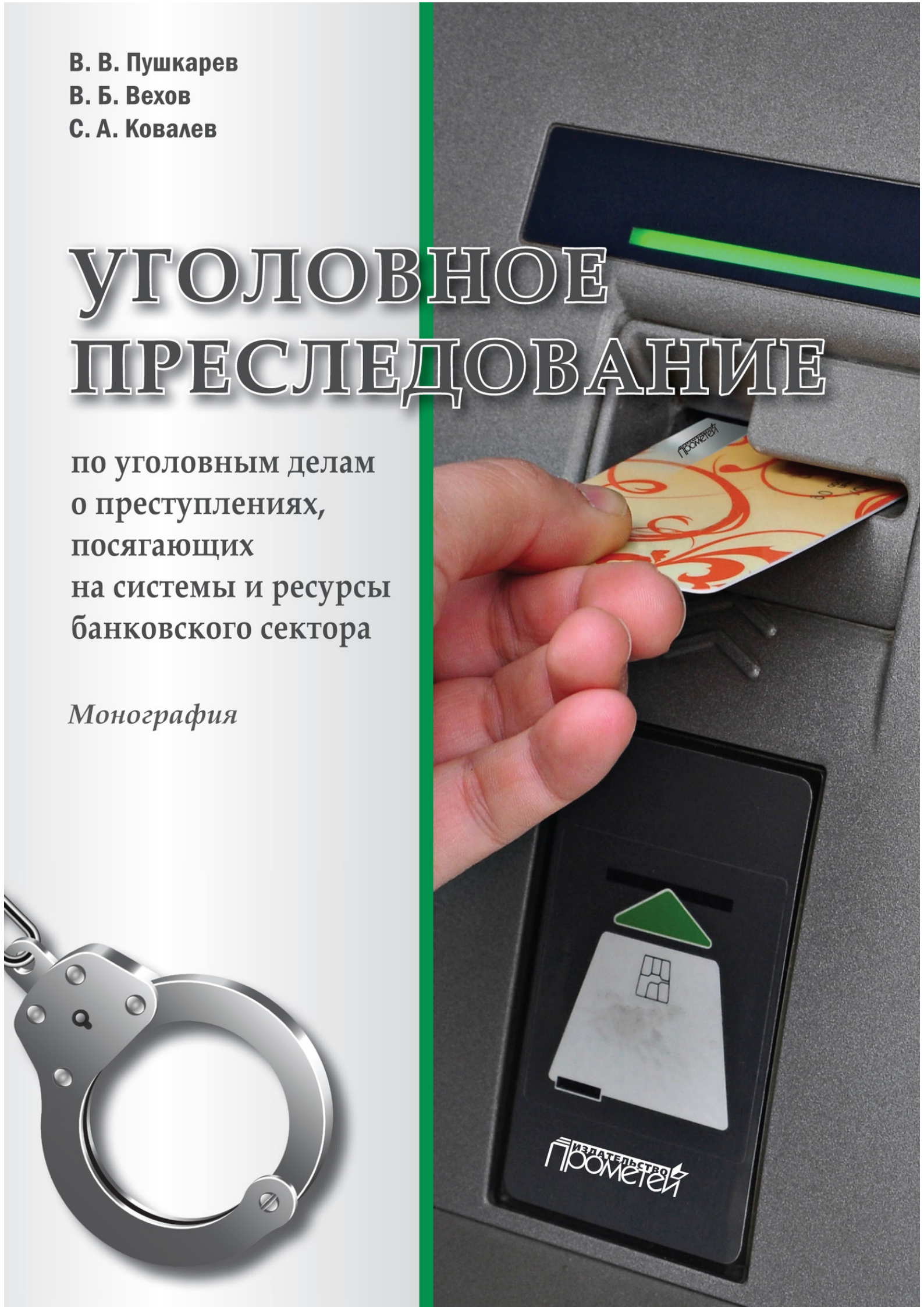
В. В. Пушкарев
В. Б. Вехов
С. А. Ковалев

УГОЛОВНОЕ ПРЕСЛЕДОВАНИЕ

по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора

Монография



Сергей Ковалёв

Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора

«Прометей»
2019

УДК 343.13
ББК 67.410.2

Ковалёв С. А.

Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора / С. А. Ковалёв — «Прометей», 2019

ISBN 978-5-907100-79-4

В монографии рассмотрены преступления, посягающие на системы и ресурсы банковского сектора. Большое внимание уделено кардингу, как цементирующему основанию системы преступлений экономической направленности. Проблемы осуществления уголовного преследования рассматриваются на основе анализа глубокой эмпирической базы, что позволяет не только раскрыть значимые аспекты и направления генезиса механизма подобных преступлений, но и предложить актуальные приемы и способы расследования преступлений, посягающих на системы и ресурсы банковского сектора. Настоящая монография также фокусирует внимание читателя на особенностях применения специальных знаний для выявления способов совершения исследуемых преступлений и их познания при производстве по уголовному делу. В формате a4.pdf сохранен издательский макет.

УДК 343.13
ББК 67.410.2

ISBN 978-5-907100-79-4

Содержание

Виктор Викторович Пушкарев,
Виталий Борисович Вехов,
Сергей Александрович Ковалев
Уголовное преследование по уголовным делам о преступлениях, посягающих на системы и ресурсы банковского сектора

Предисловие

Рациональная организация системы безналичных расчетов позволяет обеспечить нормализацию денежного обращения, снизить издержки субъектов платежного оборота, создать благоприятные условия для экономического развития государства. Внедрение банковских пластиковых карт в платежную систему страны позволяет снизить объем налично-денежной массы, упрощает расчеты с населением, делает прозрачным торговый оборот для государства, что, в свою очередь, повышает эффективность функционирования экономики.

При этом стремительное развитие науки и техники способствует не только проникновению его результатов в банковскую сферу, но и появлению новых видов хищений, приспособлению известных российской уголовной практике способов совершения преступлений к новым условиям. Поэтому ситуация в сфере выпуска и обращения банковских карт характеризуется и рядом негативных признаков.

Наряду с развитием системы карточных расчетов наблюдается возрастание интереса к сфере обращения банковских карт со стороны криминальных кругов. По мере увеличения в обращении количества карт эти платежные средства становятся предметом разного рода преступлений, выступая как в качестве предмета преступления в уголовно-правовом значении, так и в качестве средства совершения преступлений против собственности. Анализ криминогенной ситуации в кредитно-финансовой сфере показывает, что преступность в этой области растет параллельно с развитием банковских систем.

Несомненно, что в названных условиях сотрудники правоприменительных органов должны обладать необходимыми современными знаниями и практическим инструментарием, которые бы совокупно позволили им своевременно выявлять, раскрывать, расследовать и пресекать подобные деяния.

Представляется, что помимо специалистов в области уголовно-процессуального права, криминалистики и оперативно-розыскной деятельности и тех, кто на практике осуществляет уголовное преследование по делам о преступлениях, посягающих на системы и ресурсы банковского сектора, данное пособие будет интересно широкому кругу читателей.

Глава 1
Современное состояние уголовного преследования по делам о преступлениях, посягающих на системы и ресурсы банковского сектора

§ 1. Факторы, обусловливающие необходимость уголовного преследования

Анализ статистических и иных данных свидетельствует о том, что ресурсы банковской системы Российской Федерации являются весьма привлекательными для совершения преступлений, в силу их сверхприбыльности, поэтому ежегодно увеличивается число преступных атак на системы и ресурсы банковского сектора, что сопряжено с увеличением количества лиц, вовлекаемых в их совершение, возрастанием уровня их преступного профессионализма и общественной опасности, появлением новых и модернизацией имеющихся способов совершения преступлений, созданием преступной инфраструктуры, которая не только повышает уровень криминализации данной сферы экономической деятельности, но и создает предпосылки формирования преступных сообществ нового типа – экстерриториальных, основанных на принципах анонимности, действующих дистанционно, в киберсреде.

В первую очередь активность преступников направлена на рынок платежных карт, который продолжает бурно развиваться в России и во всем мире. Параллельно увеличивается количество преступлений, совершенных с использованием платежных карт. По данным МВД России, за последние 10 лет очевиден прирост преступлений, предусмотренных ст. 159.3, ст. 187 УК РФ, – почти в восемь раз[1], но регистрируется лишь около 10 % таких деяний и в абсолютном большинстве случаев личность преступника остается неустановленной.

Только из банкоматов на территории России в 2017 году было украдено 5 млрд рублей, вдвое больше, чем в 2016 году. Число попыток завладения денежными средствами по сравнению с 2016 годом увеличилось на 25 %. В странах Европейского

Союза общее число преступных атак на банкоматы в разы больше: 26620 по сравнению с 5000, а суммарная потеря 414,64 млн долларов, при этом количество атак выросло на 30 %.

В то же время преступлений, совершенных с использованием платежных карт, гораздо больше, и их составы раскрываются в ст. ст. 158, 159, 159.1–159.6, 183, 272, 173, 174, 174[1] и др. Уголовного кодекса Российской Федерации. В этой связи, во-первых, совершенно справедливо употребление обобщающего термина «кардинг», который используется и в иностранной, и в отечественной юридической литературе.

15 декабря 2017 года в России впервые в результате кибератаки на SWIFT (систему межбанковских переводов), до этого считавшуюся неуязвимой, были выведены денежные средства одного из отечественных банков.

Что касается создания инфраструктурных преступных проектов, о которых было упомянуто ранее, то они направлены на популяризацию, вовлечение и обучение методам такого криминального воздействия на системы и банковского сектора. Примером является преступная деятельность Селезнева и его сообщников, которые взломали тысячи компьютеров по всему миру, в том числе системы многочисленных малых субъектов предпринимательской деятель-

[1] См.: Анализ статистических данных, представленных на официальном сайте МВД России. URL: https://мвд. рф/Deljatelnost/statistics (дата обращения: 23.03.2017).

ности в Западном округе Вашингтона (США), в результате чего были скомпрометированы миллионы платежных карт, которые были реализованы через два специально созданных ими автоматизированных пункта продажи реквизитов кредиток, по сути онлайн-рынок – сайт POS Dumps, на котором тысячи новых преступников не только приобретали эти данные, но и знакомились с азами их использования в мошеннических целях. Только известные убытки, связанные с преступлениями Селезнева, приблизительно равны 170 млн долларов. В числе его жертв – 3700 различных финансовых учреждений, более 500 компаний по всему миру и миллионы владельцев платежных карт[2].

Различные посягательства на системы банковского сектора обусловлены особенностями функционирования экономической системы современных государств, когда большинство финансовых операций осуществляются через них, при этом они выступают в роли «кровеносной системы» всего экономического организма.

При этом необходимо учитывать, что:

1) процессы подготовки, совершения и сокрытия кардинга во многом происходят в киберпространстве, поэтому проистекают максимально незаметно;

2) доказательства, особенно цифровые, могут быть собраны в течение кратчайшего срока после совершения преступления;

3) сами преступления экстерриториальны.

Во-вторых, можно констатировать, что кардинг становится системообразующим фактором экономической преступности, хотя бы по тому основанию, что дроп-проекты становятся обязательным элементом любого киберпреступления, связанного с финансами[3].

В-третьих, приведенный перечень преступлений предполагает разрозненность аналитических данных и отсутствие, к сожалению, единого учета их в ведомственной статистике, что существенным образом усложняет сбор сведений для объективных научных исследований в данной области. Однако аргументируем актуальность темы исследования данными о размере причиненного такими преступлениями имущественного вреда.

Так, в конце 2015 года сотрудники МВД России пресекли деятельность международной преступной группы, ущерб от деятельности которой исчислялся сотнями миллионов рублей, а на сумму более 1,5 млрд рублей были предотвращены аналогичные хищения[4].

Следственным департаментом МВД России закончено производство по уголовному делу, общий ущерб составил 1,7 млрд рублей[5].

В настоящее время в Мещанском районном суде г. Москвы идет процесс по делу Юрия Лысенко и соучастников, ущерб от деятельности которых составил более 1 млрд руб.

Ошеломляющие цифры не являются конечными. Так, анализ данных ведущей компании в области интернет-безопасности Groop-IB, выявившей лидеров преступной группы А. и Н. Покорских, создавших одну из крупнейших в мире бот-сетей по использованию вредоносной программы Carberp (самый распространенный банковский троян), и материалов уголовного дела 1–504/13 по их обвинению устанавливает, что ущерб от преступной деятельности Покорских составил более 250 млн долларов[6], а вменен (по обвинительному приговору суда) только

---

[2] *Козловский В.* Дело Селезнева: нечистосердечное признание осужденного в США русского хакера // Русская служба Би-би-си. Нью-Йорк, 2017. URL: http://www.bbc.com/russian/features-39676891 (дата обращения: 23.03.2017).

[3] Дропы, то есть лица – держатели платежных карт, очевидно используемые для совершения противоправных действий в качестве подставных, например, для обналичивания скомпрометированных платежных карт в банкомате, либо перевода похищенных средств на другой счет, либо для доставки на их адрес приобретенных в интернет-магазинах с помощью данных карт товаров. Известны, например, случаи оформления в крупных банках зарплатных проектов по специально созданным для совершения хищений юридическим лицам.

[4] *Юрьев И.* Кибербанда угрожала разорить все банки // UTRO.RU. 2016. URL: https://www.utro.ru/articles/2016/02/04/1269788.shtml (дата обращения: 23.03.2017).

[5] Данные из личного архива автора.

[6] Group-IB: [сайт]. URL: http://www.group-ib.ru/investigation.html (дата обращения: 03.03.2017)

на 150 млн руб., поскольку не все пострадавшие обращались с заявлением в полицию, а в некоторых случаях причастность этой группы к совершению иных преступлений не удалось доказать.

Приведенные данные не только не позволяют рассчитывать на уменьшение числа атак на системы и ресурсы банковского сектора в целом по стране, в том числе с учетом сверхприбыльности таких преступлений, но и обнажают целый ряд взаимосвязанных и взаимообусловленных проблем:

1) предполагается постоянное совершенствование имеющихся и разработка новых способов совершения рассматриваемых преступлений;

2) наличествует серьезный недостаток специальных знаний у субъектов выявления, расследования и разрешения дела по существу, объективно затрудняющий перечисленные процессы.

§ 2. Предмет преступного посягательства

Очевидно, что в условиях создания цифровой экономики Российской Федерации электронные средства платежа, в том числе платежные карты и содержащаяся в их памяти охраняемая законом компьютерная информация[7], все чаще становятся предметом и средством совершения преступлений.

Электронное средство платежа – это средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств[8].

Платежная карта – это документ, выполненный на основе металла, бумаги или полимерного (синтетического) материала – пластика стандартной прямоугольной формы, хотя бы один из реквизитов которого представлен в электронной форме, доступной восприятию средствами электронно-вычислительной техники и электросвязи, и предназначенный для использования в качестве электронного средства платежа. *Общим классифицирующим основанием данной группы криминалистически значимых предметов будет являться наличие у них совокупности следующих признаков:*

1) машинописного документа – письменного документа, при создании которого знак письма наносят техническими средствами;

2) документа на машинном носителе – документа, созданного с использованием носителей и способов записи, обеспечивающих обработку его информации ЭВМ и иным компьютерным устройством.

Следовательно, любая платежная карта и техническое устройство, предназначенное для считывания с нее информации или ввода в нее реквизитов карты, как предмет или средство совершения преступления обязательно должно содержать какую-либо компьютерную информацию и иметь в своем конструктивном исполнении ее электронный носитель. Их виды, размеры, места расположения в документе, способы записи на них и кодирования компьютерной информации, а также иные физические характеристики определяются соответствующими международными и государственными стандартами.

В зависимости от вида материального носителя, технологии записи и кодирования компьютерной информации платежные карты подразделяются на следующие категории[9].

1. *Штрих-кодовые*. Компьютерная информация в этих картах представлена в виде параллельных черно-белых штриховых линий одинаковой высоты, но разной ширины либо квадратного QR-кода (от англ. Quick Response Code – код быстрого реагирования). Их наносят на подложку документа печатающими компьютерными устройствами – принтерами либо специальными электронными маркираторами. В качестве азбуки используется универсальный торговый код. Документы рассматриваемого вида относительно популярны в связи с низкой себестоимостью и дешевизной считывающего компьютерного оборудования: ручного или стационарного сканера с инфракрасной лампой.

---

[7] Сведения (сообщения, данные), представленные в форме электрических сигналов и отнесенные к банковской, коммерческой, служебной тайне или персональным данным соответствующими федеральными законами.

[8] О национальной платежной системе: федер. закон Рос. Федерации от 27 июня 2011 № 161-ФЗ: принят Гос. Думой Федер. Собр. Рос. Федерации 14 июня 2011 г.: одобр. Советом Федерации Федер. Собр. Рос. Федерации 22 июня 2011 г. Ст. 3. П. 19.

[9] Подробнее об этом см.: Вехов В. Б. Особенности расследования преступлений, совершенных с использованием пластиковых карт и их реквизитов: Монография. Волгоград: ВА МВД РФ, 2005. Гл.1. П. 2.2.

В целях повышения уровня защищенности закодированной информации:

– штрих-код покрывают слоем специальной флуоресцентной краски, которая визуально непрозрачна при обычном (дневном или искусственном) освещении, но способна светиться (становиться видимой) в инфракрасных (ИК) или ультрафиолетовых (УФ) лучах [10];

– штрих-код наносят двумя специальными ферромагнитными красками одинакового цветового тона, но с разными магнитными свойствами, создающими дискретное распределение полос штрих-кода;

– используется трехмерный голографический штрих-код, когда штрихи оптически имеют ширину, высоту и глубину[11].

2. *Оптические.* К этой группе относятся документы, имеющие электронные реквизиты, в которых компьютерная информация зафиксирована с помощью оптических методов записи. Мы выделяем следующие их разновидности.

2.1. *Оптические кодовые*. При их создании используется технология чередования прозрачных и непрозрачных зон в виде точек и штрихов или кружков и прямоугольничков. В считывающем устройстве с одной стороны установлен источник УФ и/или ИК света, а с другой – его приемник – электронные фотоэлементы (фотодиоды, фототранзисторы или полупроводниковый прибор с зарядовой связью – ПЗС матрица)[12]. Свет, проходя через оптически прозрачные зоны, расположенные в определенном порядке на подложке документа, воспринимается приемником, трансформируется в электромагнитные сигналы, которые усиливаются и передаются в микро-ЭВМ для обработки. Такие документы в форме карт используются в охранных системах для разграничения доступа.

2.2. *Карты с оптической памятью*. Основаны на использовании лазерной (оптической) технологии записи информации. Карта рассматриваемого вида была изобретена в 1981 г. Джоном Дрекслером[13]. В настоящее время эти карты изготавливают в соответствии с техническими требованиями, изложенными в ГОСТ Р ИСО/МЭК 11693–2004 «Карты идентификационные. Карты с оптической памятью. Общие характеристики».

Запись информации производится с помощью сфокусированного оптического луча (лазера) в порядке, установленном ГОСТ Р ИСО/МЭК 11694–1–2003 «Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Физические характеристики». Луч оставляет на специальном информационном (термоперезаписываемом) слое многослойного пластика дорожку термических следов («ямок»), имеющих различные оптические свойства и характеристики: оптический контраст между следом и следовоспринимающим слоем; коэффициент отражения света от следа. Эти физические параметры должны соответствовать ГОСТ Р ИСО/МЭК 11694–3–2003 «Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Оптические свойства и характеристики».

Оптический реквизит карт рассматриваемого вида занимает значительную часть площади ее оборотной стороны. Размеры и место размещения реквизита на карте определяются ГОСТ Р ИСО/МЭК 11694–2–2003 «Карты идентификационные. Карты с оптической памятью. Метод линейной записи данных. Размеры и расположение оптической зоны».

3. *Карты с магнитной полосой или проволокой*. Это наиболее распространенная категория документов-следов. Как правило, они существуют в форме карт (magnetic stripe card). Метод записи компьютерной информации основывается на общеизвестном физическом явлении, называемом остаточный магнетизм, т. е. способность отдельных (ферромагнитных) мате-

---

[10] Пластиковые карты. 4-е изд. перераб. и доп. М.: БДЦ-ПРЕСС, 2002. С. 14.

[11] Об этом подробнее см.: *Григорович В. Л., Федоров Г. В.* Голография в криминалистике / Под ред. Г.В. Федорова. Минск, 2003. Гл. 1, 2.

[12] О понятии и принципе действия ПЗС-матрицы см.: *Кузнецов Ю. А., Шилин В. А.* Микросхемотехника БИС на приборах с зарядовой связью. М.: Радио и связь, 1988.

[13] Пластиковые карточки в России / Сост. А.А. Андреев, А.Г. Морозов и др. М.: Банкцентр, 1995. С. 29.

риалов приобретать и сохранять намагниченность под воздействием внешнего электромагнитного поля. Принцип кодирования данных заключается в создании на магнитной проволоке[14] или полосе участков – магнитных доменов с различной степенью напряженности магнитного поля или противоположными направлениями магнитной ориентации.

После рассмотрения общих криминалистических признаков электромагнитных карт исследуем их частные признаки. В этих целях сгруппируем их с учетом различных критериев.

3.1. *По стойкости к размагничиванию.* Важной характеристикой магнитной полосы является напряженность размагничивания, которая называется коэрцитивность – сопротивление ферромагнетика к размагничиванию. Иными словами, речь идет о силе магнитного поля, необходимой для записи или стирания компьютерной информации. По этому основанию мы выделили некоторые виды карт.

3.1.1. *Карты с низкой степенью коэрцитивности*. Их технические характеристики определяются ГОСТ Р ИСО/МЭК 7811–2–2002 «Карты идентификационные. Способ записи. Магнитная полоса малой коэрцитивной силы» (так называемая Lo-co). При изготовлении магнитной полосы используется оксид железа Fe_2O_3, который является магнитомягким материалом. Визуально такие карты можно отличить от других по коричневому цвету магнитной полосы: чем он светлее, тем меньше коэрцитивная сила. Эти карты имеют самую низкую степень защиты от подделки (по сравнению с другими картами рассматриваемого вида) и поэтому используются в качестве одноразовых проездных документов или пропусков.

3.1.2. *Карты с высокой степенью коэрцитивности* производят из магнитотвердых материалов – оксида хрома или феррита бария. Магнитная полоса данных карт имеет насыщенный черный или серый со стальным оттенком цвета. Чем цвет насыщенней, тем выше коэрцитивность карты, а следовательно, и ее защита от подделки. Эти карты изготавливают по требованиям ГОСТ Р ИСО/МЭК 7811–6–2003 «Карты идентификационные. Способ записи. Магнитная полоса большой коэрцитивной силы» (так называемая Hi-co).

3.2. *По ширине магнитной полосы*. По этому признаку также выделяются определенные группы карт.

3.2.1. *Карты с узкой магнитной полосой* производятся в соответствии с ГОСТ Р ИСО/МЭК 7811–2–2002 «Карты идентификационные. Способ записи. Магнитная полоса малой коэрцитивной силы». Это самая незащищенная от подделки категория электромагнитных карт. На территории Российской Федерации такие карты в основном используются для оплаты услуг электросвязи, в качестве проездных документов на городском транспорте (трамвай, троллейбус, автобус, метро), а также пропусков на охраняемые объекты.

Информация на эти карты кодируется в виде магнитных штрихов. В зависимости от целей использования рассматриваемого реквизита карты применяют два способа электромагнитного штрих-кодирования информации, а именно:

– для защиты документа от подделки на магнитную полосу наносят штрихи, имеющие одинаковую ширину и высоту, но разное расстояние друг от друга. Такое кодирование не предусматривает перемагничивания записанной информации, которая остается неизменной до окончания срока службы или цикла использования карты;

– для многоразовой оплаты услуги или фиксации частоты доступа на охраняемый объект на магнитную полосу наносят магнитные штрихи, имеющие одинаковые ширину, высоту и расстояние друг от друга. Каждый магнитный штрих соответствует одной условной единице, например одной минуте телефонного разговора по таксофону или одному проходу через автоматизированный турникет контрольно-пропускного пункта. Каждый раз при этом один магнитный штрих размагничивается (стирается) головкой считывающего устройства. Этот про-

[14] Изготавливается из бериллиево-медного сплава. Сверху покрыта магнитным слоем (ферромагнетиком). См.: *Першиков В. И., Савинков В. М.* Толковый словарь по информатике. М.: Финансы и статистика, 1991. С. 256.

цесс продолжается до тех пор, пока на магнитной полосе не останется ни одного магнитного штриха. После этого карта перемагничивается (перезаписывается) или выбрасывается за ненадобностью. Данным обстоятельством активно пользуются преступники.

3.2.2. *Карты с широкой магнитной полосой.* В отличие от предыдущих карт, они имеют высокую степень защиты компьютерной информации. Это достигается за счет: изготовления полосы из магнитных материалов, имеющих среднюю и высокую коэрцитивность; различного формата записи информации на трех дорожках; использования персонального идентификационного номера (ПИН-кода).

Ширина магнитной полосы составляет 12,7 мм, что соответствует аналогичному размеру стандартной магнитной ленты, используемой при производстве видеокассет (ГОСТ 20958–80).

В зависимости от типа магнитной полосы и применяемого формата записи компьютерной информации количество дорожек данного электронного реквизита варьируется от одной до четырех. Например, в соответствии с отечественным ГОСТ Р 50809 «Нумерация и метрологическое обеспечение идентификационных карт для финансовых расчетов» все банковские карты должны иметь: *ширину* – 85,595 ± 0,125 мм; *высоту* – 53,975 ± 0,055 мм; толщину – 0,76 ± 0,08 мм; радиус окружности в углах – 3,18 ± 0,125 мм[15]. На их магнитной полосе находится три дорожки[16]. Первые две предназначены для идентификационных целей и технологически работают в режиме «только считывание информации». По завершении цикла использования карты информация на магнитных дорожках перезаписывается, например, записываются персональные данные нового клиента, чтобы он смог воспользоваться картой для совершения платежно-расчетных операций.

3.2.3. *Карты с нестандартной магнитной полосой*. К этой категории относятся документы, имеющие нестандартные размеры бумажной подложки и магнитной полосы. Ширина бумажной подложки этих карт составляет 8,5 см, длина – 20,3 см; ширина магнитной полосы, содержащей 4 дорожки, – 1,5–1,7 см, а ее длина – 20,3 см. Карты имеют локальное использование в рамках одного национального эмитента и поэтому подробно не рассматриваются в настоящей работе.

4. *Карты на интегральных микросхемах с контактами:* ГОСТ Р ИСО/МЭК 7816-1-2002 «Карты идентификационные. Карты на интегральных схемах с контактами. Физические характеристики»; ГОСТ Р ИСО/МЭК 7816-2-2002 «Информационная технология. Карты идентификационные. Карты на интегральных схемах с контактами. Размеры и расположение контактов»; ГОСТ Р ИСО/МЭК 7816-6-2003 «Карты идентификационные. Карты на интегральных схемах с контактами. Элементы данных для межотраслевого обмена»; ГОСТ Р ИСО/МЭК 7816-10-2004 «Карты идентификационные. Карты на интегральных схемах с контактами. Электронные сигналы и ответ на восстановление у синхронных карт».

В настоящее время эти карты широко используются для идентификации абонентов сетей электросвязи – сотовой радиотелефонной, спутникового телевещания, стационарной телефонной («таксофонной»), мобильного интернета (с помощью USB-модема).

[15] Пластиковые карты. 4-е изд. перераб. и доп. М.: БДЦ-ПРЕСС, 2002. С. 46.

[16] Гелль П. Магнитные карты и ПК / Пер. с фр. М.: ДМК Пресс, 2001. С. 16, 27–49.

Конец ознакомительного фрагмента.