https://doi.org/10.30764/1819-2785-2025-2-6-21

Криптография в криминалистике и судебной экспертизе: история и современное состояние

Ш.Н. Хазиев[1,2], А.Н. Штохов[2]

[1] Федеральное бюджетное учреждение Российский федеральный центр судебной экспертизы имени профессора А.Р. Шляхова при Министерстве юстиции Российской Федерации, Москва 101000, Россия

[2] Акционерное общество «Научно-производственная компания "Криптонит"», Москва 115114, Россия

Аннотация. В настоящей статье предпринята попытка отдать должное вкладу криминалистов в теорию и практику использования криптографии. Рассмотрены публикации основоположников криминалистической науки – Антонио Коспи, Ганса Гросса, Эдмона Локара, ряда отечественных криминалистов, посвященные вопросам криптографии. Показано значение этих публикаций для развития криминалистики и судебно-экспертной деятельности, а также представлена взаимосвязь криминалистики и судебной экспертизы с криптографией в современных условиях.

Ключевые слова: *Ганс Гросс, Антонио Мария Коспи, Эдмон Локар, Иван Якимов, Сергей Трегубов, история криминалистики, криптография, судебная компьютерно-техническая экспертиза, цифровая криминалистика*

Для цитирования: Хазиев Ш.Н., Штохов А.Н. Криптография в криминалистике и судебной экспертизе: история и современное состояние // Теория и практика судебной экспертизы. 2025. Т. 20. № 2. С. 6–21. https://doi.org/10.30764/1819-2785-2025-2-6-21

Cryptography in Forensic Science and Forensic Examination: History and Current State

Shamil N. Khaziev[1,2], Aleksander N. Shtokhov[2]

[1] The Russian Federal Centre of Forensic Science named after professor A.R. Shlyakhov of the Ministry of Justice of the Russian Federation, Moscow 101000, Russia

[2] Joint Stock Company "Research and Production Company "Kryptonite", Moscow 115114, Russia

Abstract. This article makes an attempt to pay tribute to the contribution of forensic scientists to the theory and practice of using cryptography. It considers publications on cryptography issues of the founders of forensic science – Antonio Cospi, Hans Gross, Edmond Locard and a number of domestic forensic scientists. The importance of these publications for the development of forensic science and forensic activities is shown as well as the interrelation of forensic science and examination with cryptography under present-day conditions.

Keywords: *Hans Gross, Antonio Maria Cospi, Edmond Locard, Ivan Yakimov, Sergey Tregubov, history of forensic science, cryptography, forensic computer-technical examination, digital forensics*

For citation: Khaziev Sh.N., Shtokhov A.N. Cryptography in Forensic Science and Forensic Examination: History and Current State. *Theory and Practice of Forensic Science.* 2025. Vol. 20. No. 2. P. 6–21. (In Russ.). https://doi.org/10.30764/1819-2785-2025-2-6-21

Введение

История криптографии тесно связана с государственной службой, дипломатией, военным делом, деятельностью правоохранительных и разведывательных органов. Правоохранительным органам, в частности, приходится обращаться к криптографии как для защиты служебной информации, так и для расшифровки коммуникаций участников преступной деятельности.

Зарубежные и отечественные исследователи посвятили немало научных и научно-популярных работ истории криптографии. В них в основном рассматривались различные этапы ее возникновения в далеком прошлом и последующее развитие в рамках политической борьбы, дипломатии, военных сообщений, шифрованной переписки революционеров. При этом вопросы применения криптографии в раскрытии и расследовании преступлений почти не были освещены. Не уделялось должного внимания в этих изданиях и публикациям основоположников криминалистики. В связи с этим представляется целесообразным привести некоторые сведения о криптографических изысканиях таких известных криминалистов, как Антонио Мария Коспи, Ганс Гросс, Эдмон Локар, Сергей Николаевич Трегубов, Иван Николаевич Якимов.

История становления криминалистики в определенной степени была связана с криптографией. Одна из причин проявления интереса основоположников научной криминалистики к криптографии – стремление преступников маскировать свою противоправную деятельность и способы передачи информации между сообщниками, а также между арестованными или осужденными и их «товарищами», находящимися на свободе.

Первым криминалистом-практиком, написавшим фундаментальное руководство для судебных следователей и судей по уголовным делам «Судья-криминалист» и обратившимся к вопросам криптографии, был флорентийский следственный судья Антонио Мария Коспи.

Антонио Мария Коспи

Как в зарубежной, так и в отечественной криминалистике многие годы единственным и главным основоположником криминалистической науки и инициатором введения в научный оборот термина «криминалистика» было принято считать австрийского судебного следователя, а впоследствии профессора Ганса Гросса. Однако первой фундаментальной публикацией, содержавшей основы криминалистики и сам термин «криминалист», была 610-страничная книга флорентийского следственного судьи Антонио Марии Коспи «Судья-криминалист» (Il' Giudice Criminalista) [1]. Таким образом, ее автора можно считать предшественником не только Ганса Гросса, но и всей современной криминалистики [2].

Антонио Мария Коспи (Antonio Maria Cospi, 1560–1635) к моменту завершения работы над книгой для следственных судей был секретарем Великого герцога Тосканы Фердинанда II Медичи[1] и жил во Флоренции. Работая в должности судьи по уголовным делам, он накопил богатый опыт в области их расследования и судебного разбирательства. В рукописи книги он изложил полученные знания и научно-методические обобщения, однако опубликовать ее не успел. Книга «Судья-криминалист» типографским способом была издана посмертно его племянником доктором Оттавиано Карло Коспи в 1643 году, в 1681 году ее переиздали в Венеции.

Помимо первого публичного печатного употребления слова «криминалист», автор установил некоторые руководящие принципы и рекомендации по расследованию преступлений, детально описал способы совершения основных видов преступлений, правила осмотра места происшествия, поиска и описания следов, проведения судебно-следственного эксперимента, использования помощи специалистов при осмотре места происшествия, поиска тайников и ряд других технических, методических и судебно-медицинских рекомендаций и приемов.

Еще задолго до Г. Гросса, посвятившего криптографии отдельную главу в своем руководстве, А.М. Коспи написал отдельный труд под названием «Интерпретация шифров. Правила хорошего и легкого понимания любых простых шифров» [3]. Книга была издана также после смерти автора его племянником в 1639 году. Два года спустя данный труд был переведен с итальянского на французский (рис. 1, слева) известным французским математиком, монахом Фран-

[1] Фердинанд II Медичи занимал пост Великого герцога Тосканы в 1628–1670 гг. Отмечен в истории покровительством науке и искусствам, в частности активно защищал Галилея во время церковного суда над ним.

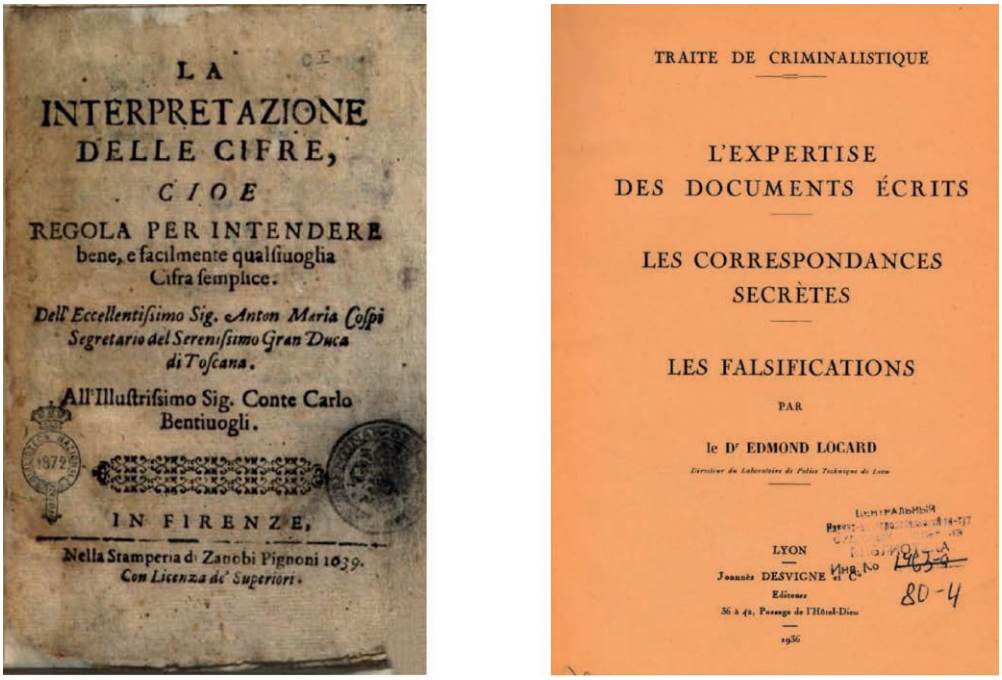
LA
INTERPRETAZIONE
DELLE CIFRE,
CIOE
REGOLA PER INTENDERE
bene, e facilmente qualsiuoglia
Cifra semplice.
Dell' Eccellentissimo Sig. Anton Maria Cospi
Segretario del Serenissimo Gran Duca
di Toscana.
All'Illustrissimo Sig. Conte Carlo
Bentiuogli.
IN FIRENZE,
Nella Stamperia di Zanobi Pignoni 1639.
Con Licenza de' Superiori.
TRAITE DE CRIMINALISTIQUE
L'EXPERTISE
DES DOCUMENTS ÉCRITS
LES CORRESPONDANCES
SECRÈTES
LES FALSIFICATIONS
PAR
le Dr EDMOND LOCARD
LYON
Joannès DESVIGNE et Cie
Editeurs
36 à 42, Passage de l'Hôtel-Dieu
1936

Рис. 1. Титульные страницы книги А.М. Коспи «La Interpretazione delle Cifre, Cioe Regola per Intendere Bene, e Facilmente Qualsiuoglia Cifra Semplice» и шестого тома «Руководства по криминалистике»[2] Эдмона Локара

Fig. 1. *The title pages of the book by A.M. Cospi "La Interpretazione delle Cifre, Cioe Regola per Intendere Bene, e Facilmente Qualsiuoglia Cifra Semplice" (left) and the sixth volume of the "Manual on Criminology" by Edmond Locard (right)*

суа-Жаном Нисероном и напечатан в Париже в 1641 году [4].

Книга представляет собой справочник, объясняющий методы шифрования и взлома шифров. При этом автор ограничился простыми одноалфавитными шифрами и явно не хотел иметь дело с омофоническими системами[3], которые он и его современники называли «шифрованием сочинения». Коспи открыто признавал, что разгадать этот тип шифрования практически невозможно, а затем описал одноалфавитные шифры, представил способы нахождения гласных в слогах и предложил таблицы, содержащие частотные слоги во французском, латинском и испанском языках. К сожалению, каких-либо указаний на конкретные случаи применения криптографии для расследования преступлений А.М. Коспи не привел. Неизвестно также, что послужило причиной написания книги о шифрах – криминалистическая практика или политическая деятельность Коспи на посту секретаря Великого герцога, предполагавшая необходимость ведения тайной переписки.

Ганс Гросс

Вторым по хронологии криминалистом-практиком и ученым, обратившимся к криптографии и ее применению при расследовании уголовных дел, был австрийский судебный следователь, а впоследствии профессор университетов в Черновцах, Праге и Граце Ганс Густав Адольф Гросс (Hans Gustav Adolf Groß, 1847–1915), опубликовавший в 1893 году фундаментальный труд «Руководство для судебных следователей, чинов жандармерии и полиции». Данную публикацию долгое время было принято считать первой систематизированной книгой о технике, тактике и методике раскрытия и расследования преступлений. Ее третье издание вышло в 1898 году под названием «Руководство для судебных следователей как система криминалистики» (далее – Руководство), в связи с чем Ганс Гросс долгое

[2] Хранится в библиотеке ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России, имеет оттиск штампа ЦНИИ судебных экспертиз.

[3] Омофоническая система шифрования (омофоническая замена) – шифр подстановки, при котором каждый символ открытого текста заменяется на один из нескольких символов шифра алфавита, причем количество заменяющих символов для одной буквы пропорционально частоте этой буквы. Это позволяет скрыть настоящую частоту появления данной буквы в зашифрованном тексте. Шифрование методом омофонической замены известно с 15 века.

время считался автором и самого термина «криминалистика», который, как было указано выше, на деле впервые использовал Антонио Мария Коспи.

Глава пятнадцатая Руководства была посвящена криптографии и называлась «Наука дешифровки» (Dechiffrierkunde). В русском переводе 1908 года она имела название «О чтении шифрованных писем».

Глава состояла из следующих пунктов и подпунктов.

1. Общие замечания.

2. Различные системы тайнописи:

1) шифры цифровые;

2) шифры буквенные;

3) шифры из слогов и целых слов;

4) шифры с перемещениями при помощи патронов и сеток;

5) шифры других видов:

а) тайнопись со знаками каменщиков или с изображением углов;

б) тайнопись с помощью ниток;

в) тайнопись при помощи масштаба;

г) тайнопись посредством пунктирования по способу Шотти [5];

д) тайнопись при помощи игральных карт;

е) способ секретной полицейской переписи по системе графа Вержена;

ж) древняя тайнопись.

3. О прочтении шифров.

Ганс Гросс описал основные методы шифрования, используемые преступниками, и способы их дешифровки. Он считал, что судебные следователи должны уметь расшифровывать сообщения криминального характера, созданные с использованием относительно несложных и распространенных шифров. Помимо способов дешифровки Гросс привел ряд, на наш взгляд, полезных и важных рекомендаций криминалистического характера, направленных на установление факта и вида шифрованной связи преступников, а также поиск ключей шифрования при проведении следственных действий. В этом заслуга Ганса Гросса несомненна.

Кроме того, основываясь на многочисленных источниках по криптографии европейского происхождения, автор изложил основы шифрования и криптоанализа и постарался представить материал данной главы доступным для правоприменителей (следователей, судей) языком. При этом он приводил подробные библиографические ссылки на наиболее, по его мнению, основательные труды по криптографии.

Эдмон Локар

Всемирно известный французский криминалист Эдмон Локар (Edmond Locard, 1877–1966), в 1910 году создавший и впоследствии 40 лет возглавлявший полицейскую криминалистическую лабораторию в Лионе, также внес большой вклад в разработку и внедрение методов криптографии в криминалистическую науку и практику. Он был, пожалуй, единственным в истории мировой криминалистики ученым и практиком, профессионально и на высоком уровне владевшим основными методами военной и криминалистической криптографии.

Эдмон Локар родился 13 декабря 1877 года во Франции в Сен-Шамоне в обеспеченной семье. Учился в пансионе Бланшу, после чего перешел в Доминиканский колледж Сен-Тома д'Акен в Уллене, где проходил обучение на отделении древних языков. В 17 лет он уже был бакалавром, специализировался на литературе и науках и говорил на 11 языках.

Затем Э. Локар принялся за изучение права и медицины в университете Лиона, стал учеником профессора кафедры судебной медицины Александра Лакассаня. Будучи его секретарем и помощником, он сотрудничал с другими выдающимися деятелями криминалистики, в том числе с Рудольфом Арчибальдом Рейссом из Лозаннского университета [6]. В 1902 году он защитил диссертацию по теме «Судебно-медицинская практика в XVII веке» и стал доктором медицины.

В 1905 году Локар завершил свое второе, юридическое образование. Через два года он стал выступать в качестве эксперта в суде. В 1908 году Локар отправился в путешествие по миру. Будучи обеспеченным человеком, он смог посетить многие европейские города – Париж, Лозанну, Рим, Берлин, Брюссель, а также Нью-Йорк и Чикаго в США, где знакомился с работой криминалистических лабораторий.

Локар оставался помощником профессора Александра Лакассаня вплоть до 1910 года, после чего основал собственную криминалистическую лабораторию, которая помещалась на чердаке Дворца правосудия в Лионе. Двумя годами позднее его лаборатория стала официально принадлежать полиции, хотя основные расходы по ее уком-

плектованию и содержанию лежали на Локаре.

В 1912 году отдельным изданием вышла брошюра Локара «Криптография в полицейской технике: исследование использования шифров преступниками» [7]. Этот труд первоначально был опубликован в виде статьи в журнале «Бюллетень Антропологического общества Лиона» (Bulletin de la Soci t d'anthropologie de Lyon).

В том же году в журнале «Архив криминальной антропологии, судебной медицины, нормальной и патологической психологии» было опубликовано сообщение о выходе этой брошюры Локара со ссылкой на Бюллетень Антропологического общества Лиона:

«Шифрованные письма до сих пор изучались только с дипломатической и военной точки зрения. Однако они часто используются в криминальной среде, как между заключенными, так и между их сообщниками, оставшимися на свободе. Здесь автор излагает методы, которым необходимо следовать для надежной расшифровки зашифрованных текстов: процессы чтения основаны на применении теорем, которые, очевидно, не очень просты, но приводят к надежной расшифровке, за исключением случаев, когда записи очень кратки. Системы, используемые преступниками, весьма разнообразны: некоторые из них наиболее сложны и хитры (многоалфавитная инверсия, квадратная таблица Виженера и т. д.). Интерес к этой брошюре обусловлен главным образом тем, что приведенные в ней примеры не являются воображаемыми; все они имели место в полицейской лаборатории Лиона в рамках уголовных дел о кражах или мошенничествах. Это первая опубликованная работа, посвященная этому важному и сложному вопросу полицейской техники» [8, с. 555].

Локар также вел рубрику «Критический обзор. Латинская хроника» в данном журнале. В своих обзорах латиноамериканской криминалистической литературы он неоднократно приводил данные об использовании в работе полиции методов дешифровки криминальных криптограмм. Так, в 1913 году при описании изданного в Рио-де-Жанейро курса криминалистики, подготовленного профессором Элизио де Карвальо, Локар особо отметил раздел под названием «Криптография в полицейской технике, язык шифров» [9, с. 442].

Во время Первой мировой войны Локар, по одним данным, служил в Секретной службе Франции (1914–1918)[4] и занимался судебно-медицинской идентификацией, а также исследованием пятен и грязи на солдатской униформе. По другим сведениям, в 1914 году с началом войны тридцатисемилетний Эдмон Локар был мобилизован в армию и направлен в Париж для прохождения службы в дешифровальном подразделении. В его задачу входила дешифровка сообщений противника. Будучи изобретательным и очень увлеченным ученым и практикующим экспертом, Локар разрабатывал эффективные методы расшифровки в зависимости от способа написания криптограммы: метод простой замены букв алфавита соответствующими буквами других алфавитов; метод транспозиции, «где порядок букв зашифрован и определяется с помощью сетки»; или словарный метод, «где каждый корреспондент имеет словарь, в котором слова заменяются числами». В начале конфликта Германия, ранее использовавшая метод словаря, удивила своих врагов, отдав предпочтение методу транспозиции. Однако Эдмону Локару очень быстро удалось наладить процесс расшифровки немецких сообщений, за что после войны он получил Орден Почетного легиона.

В 1919 году Локар начал активно публиковать свои научные труды.

В 1920 году вышла его книга «Уголовный розыск и его научные методы» [11, с. 205–235]. Глава VI этой книги посвящена расшифровке тайных писем и содержит три параграфа: язык преступников, симпатические чернила, криптография.

В книге Локар справедливо отмечал, что лучшие криптологи находятся на военной или дипломатической службе, поскольку в полицейской практике приходится иметь дело с «менее опытными в шифровании субъектами». Однако при расследовании преступлений необходимо стремиться расшифровывать криптограммы в кратчайшие сроки, чтобы успеть предотвратить преступление или помешать скрыть его следы. Кроме того, криминальные криптограммы в большинстве случаев достаточно кратки, что также усложняет их расшифровку. На основании этих соображений Локар предлагал организовать проведение криптогра-

[4] По данным французского историка Мюриэль Салле, Локар демобилизовался в 1920 году [10, с. 18].

фических исследований в полицейских криминалистических лабораториях в крупных городах [11, с. 213].

В 1923 году Локар приступил к написанию главного труда своей жизни, посвященного криминалистике. Он подготовил и издал семитомное фундаментальное «Руководство по криминалистике» (Traite de Criminalistique) общим объемом более трех тысяч страниц. Над ним он работал вплоть до 1931 года, однако по мере подготовки к изданию каждого очередного тома и до выхода завершающего тома в 1940 году Локар вносил соответствующие дополнения и уточнения. Вопросы криптографии он детально осветил в шестом томе – «Экспертиза письменных документов (вторая часть). Секретная переписка. Фальсификации», вышедшем в 1937 году [12], где криптографии была отведена третья глава. Особо следует отметить обширный список литературы по криптографии, начиная с 16 века, насчитывающий 353 источника, из них 226 работ полностью посвящены криптографии и 127 – частично (рис. 1, справа).

В 1931 году Э. Локар опубликовал статью памяти известного французского специалиста по криптографии Этьена Базери (1846–1931), которого считал своим другом. В теорию шифрования Базери особого вклада не внес, но практическое искусство дешифрования он, по мнению Локара, поднял на большую высоту [13].

Во время Второй мировой войны Локар продолжал работать в созданной им полицейской лаборатории Лиона, несмотря на то что власть в городе находилась в руках профашистского режима Виши. В мемуарах некоторых участников Французского Сопротивления встречаются упоминания о неком высокопоставленном полицейском деятеле в Лионе, оказывавшем тайное содействие антифашистам [14]. Можно предположить, что этим деятелем был именно Локар, о чем свидетельствуют и воспоминания племянницы Альфонса Бертильона – Сюзанны Бертильон [15].

К вопросам криптографии Локар вернулся уже будучи на пенсии, в 1959 году. В книге «Судебная экспертиза фальшивых писем» криптографии наряду со стеганографией был отведен один из ее разделов [16].

В литературе, посвященной научной биографии Э. Локара, упоминается ряд рукописей, хранящихся в малоисследованном муниципальном архиве города Лион, в их числе рукопись 1946 года «Важность криптографии», машинописная статья «Криптография в уголовных делах» [17], рукописные черновики 1926 года: «Тайное письмо, тайнопись», «Контрразведка и криптография», «Криптография и война»[5] и несколько заметок о методах дешифрования [18]. В них автор описал некоторые показательные случаи дешифровки сообщений преступников из своей практики.

Эдмон Локар не занимался разработкой шифров и не сделал каких-либо значимых открытий в области криптографии, его заслугой является то, что он доказал важность криптографии для криминалистики, описал и классифицировал применяемые преступниками наиболее распространенные способы шифрования, доступным для полицейских криминалистов языком изложил основные методы дешифровки, привел тактические рекомендации по работе с криминальными криптограммами при проведении различных следственных действий.

Также ученый внес большой вклад в дактилоскопию, судебное почерковедение и автороведение, судебную баллистику, судебную медицину, теорию идентификации и криминалистику. Он руководил лионской криминалистической лабораторией до 1950 года, затем ушел на пенсию и организовал частную консультационную фирму, в которой вместе со своей второй женой Дениз занимался в основном проведением в частном порядке почерковедческих и автороведческих экспертиз.

После ухода на пенсию Эдмона Локара лабораторию возглавил его сын Жак Локар (Jacques Locard, 1914–1952), профессор Национальной полицейской школы. В 1951 году он издал книгу «Курс полицейской науки», где также уделил внимание вопросам криптографии, описав основные приемы шифрования, применяемые преступниками: методы замены, транспозиции, словаря [19, с. 35–39].

Умер Э. Локар 4 мая 1966 года в Лионе в возрасте 88 лет.

Криптография в деятельности правоохранительных органов царской России

Во время работы над статьей не удалось обнаружить какие-либо оригинальные научные публикации отечественных криминалистов времен царской России по вопросам

[5] Статья была опубликована в журнале «Les Alpes Militaires» в 1923 году.

применения криптографии при расследовании общеуголовных преступлений. Элементарные сведения о шифрованных письмах имелись лишь в главе о тайных сношениях преступников в практическом руководстве для судебных деятелей «Основы уголовной техники», составленном С.Н. Трегубовым на основе конспектов лекций Р.А. Рейсса [20; 21, с. 274–276].

При этом криптография активно использовалась в деятельности политических подразделений Департамента полиции, Отдельного корпуса жандармов, охранных отделений, что было обусловлено важностью противодействия терроризму и экстремизму, революционному движению. Члены различных революционных, террористических и экстремистских организаций активно использовали методы шифрования для обмена информацией как внутри страны, так и при контактах с находящимися за рубежом единомышленниками. Примечательным является издание членами этих революционных организаций книг, посвященных криптографии и ее использованию. Так, в 1902 году в Женеве на русском языке вышла книга известного революционного деятеля В.П. Махновца под псевдонимом "В. Бахарев" «О шифрах» [22]. В ней были описаны основные виды простых шифров: шифр «по слову», шифр «по книжке», шифр «по таблице Пифагора» и «Гамбетовский шифр». В последней главе приводилось описание правил перестукивания в тюрьме (рис. 2, слева).

Там же через два года была опубликована книга «Шифрованное письмо: критика употребляемых у нас систем шифра», изданная Всеобщим еврейским рабочим Союзом в Литве, Польше и России (Бунд) (рис. 2, справа) [23].

В историю отечественной криптографии вошли такие талантливые и высокообразованные специалисты по криптоанализу, как Владимир Иванович Кривош (1865–1942) и Иван Александрович Зыбин (1865 – после 1919), служившие в правоохранительных органах царской России [24]. Их деятельность и яркая биография подробно описаны в публикациях по истории отечественной криптографии. Однако ни научных статей по методам дешифрования, ни своих мемуаров эти выдающиеся криптологи-практики, к сожалению, не опубликовали [25, 26].

Шифрованные тексты нередко поступали и в созданные в 1912–1914 гг. Кабинеты научно-судебной экспертизы при прокурорах Судебных палат в Санкт-Петербурге, Москве, Киеве и Одессе, но специалистов по криптографии в данных судебно-экспертных учреждениях не имелось. В июле 1915 года на съезде руководителей Кабинетов была поднята проблема дешифровки поступающих документов, поскольку в отсутствии специальной литературы и соответствующего руководства сотрудники Кабинетов были вынуждены сами искать способы и приемы дешифровки. Съезд принял решение временно командировать чины кабинетов в Департамент полиции, Министерство иностранных дел и Военное министерство для ознакомления с существующими приемами дешифровки, принимая во внимание, что в перечисленных ведомствах уже накоплен большой опыт по данному вопросу.

Однако само Министерство юстиции не спешило выполнять решения съезда. Лишь через год, в июле 1916 года, начальнику Особого отдела Департамента полиции Е.К. Климовичу было направлено письмо с просьбой допустить помощника управляющего Московским кабинетом Владимира Львовича Русецкого на стажировку в Департамент полиции и ознакомить его с наиболее распространенными видами шифров и приемами их разбора. Такое разрешение было дано [27, с. 66]. Однако каких-либо сведений о проведении криптографических исследований В.Л. Русецким или иными лицами в Кабинетах научно-судебной экспертизы при прокурорах Судебных палат в царской России обнаружить пока не удалось[6].

Криптография в криминалистической литературе советского периода

В первые годы Советской власти возникла необходимость достаточно быстро обеспечить недавно созданную службу уголовного розыска учебной литературой по криминалистике и оперативно-розыскной деятельности. Это осложнялось эмиграцией большинства опытных криминалистов и судебных экспертов или их гибелью в 1917–1922 годах. Отечественные криминалисты «старой школы», перешедшие на сторону

[6] Русецкий Владимир Львович (1880–1925) – российский и советский криминалист, после революции работал в Высшем Институте фотографии и фототехники, где занимался вопросами судебной фотографии, затем с 1920 года был начальником научно-технического отдела Управления уголовного розыска НКВД РСФСР. В 1923 году ушел на пенсию.

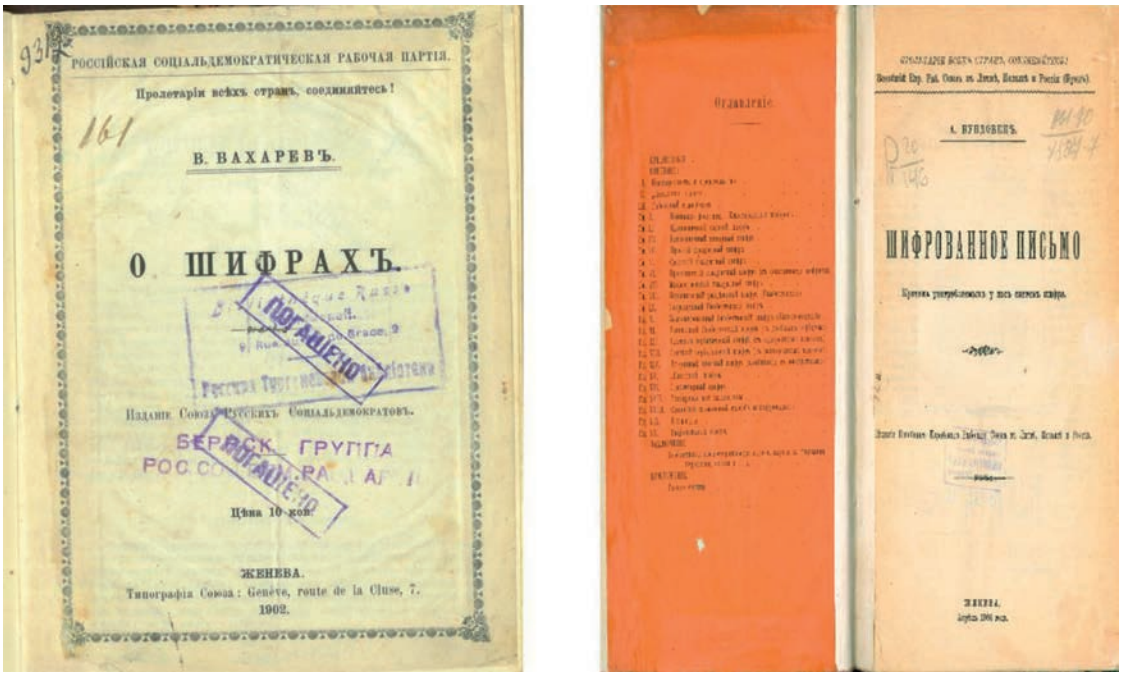
РОССІЙСКАЯ СОЦІАЛЬДЕМОКРАТИЧЕСКАЯ РАБОЧАЯ ПАРТІЯ.
Пролетаріи всѣхъ странъ, соединяйтесь!
В. ВАХАРЕВЪ.
О ШИФРАХЪ.
ПОГАШЕНО
Изданіе Союза Русскихъ Соціалъ-Демократовъ.
ПОГАШЕНО
Цѣна 10 коп.
ЖЕНЕВА.
Типографія Союза: Genève, route de la Cluse, 7.
1902.
Оглавленіе.
А. ВУЛЫОВЕЦЪ.
ШИФРОВАННОЕ ПИСЬМО

Рис. 2. Титульные листы книг В. Бахарева «О шифрах» (слева) и В.П. Махновца «Шифрованное письмо» (справа)
Fig. 2. *The title pages of the books by V. Bakharev "On Ciphers" (left) and V.P. Makhnovetz "Encrypted Letter" (right)*

советской власти, подготовили и издали несколько переводов монографий известных немецких криминалистов – Альберта Гельвига [28], Ганса Шнейкерта [29] и др. В этих изданиях наряду с традиционными методами криминалистики рассматривались и вопросы криптографии применительно к дешифровке коммуникаций преступников. Содержание разделов этих изданий практически повторяло рекомендации по расшифровке криминальных криптограмм, опубликованные в книгах Г. Гросса и Э. Локара.

Из первых советских изданий по криминалистике только в книге «Криминалистика. Руководство по уголовной технике и тактике», написанной выдающимся отечественным криминалистом Иваном Николаевичем Якимовым[7] и изданной в 1925 году (рис. 3, справа), имелась глава с описанием методов шифрования и дешифрования. В данной главе «Тайные способы общения у преступников» Якимов детально рассмотрел способы звуковых (акустических) и письменных сношений преступников. В числе письменных способов скрытых коммуникаций преступников он представил способы шифрованной переписки по книге, переписки при помощи «криптографа», решетки (шаблона), буквенных и цифровых шифров [30, с. 238–252].

Начиная с 1925 года, в научных и учебно-методических изданиях по криминалистике уже не имелось не только описаний шифров и методов их прочтения, но и упоминаний о криминальных криптограммах. Это было обусловлено следующими обстоятельствами:

– в СССР было провозглашено, что профессиональной организованной преступности больше нет и, соответственно, в орбиту следствия перестали попадать образцы зашифрованной коммуникации участников организованных преступных сообществ;

– случаи обнаружения и изъятия криминальных криптограмм в местах лишения свободы стали крайне редки;

– каких-либо законспирированных антисоветских организаций, нуждающихся в шифрованной переписке, не осталось;

– широкое распространение получила телефонная связь, в том числе междугородняя и международная, что существенно повлияло на снижение актуальности шифрованной бумажной или телеграфной переписки.

[7] Якимов Иван Николаевич (1884–1954) – советский ученый-криминалист и практик. С 1924 по 1933 гг. работал сначала в Московском уголовном розыске, а затем в Центральном управлении уголовного розыска НКВД.

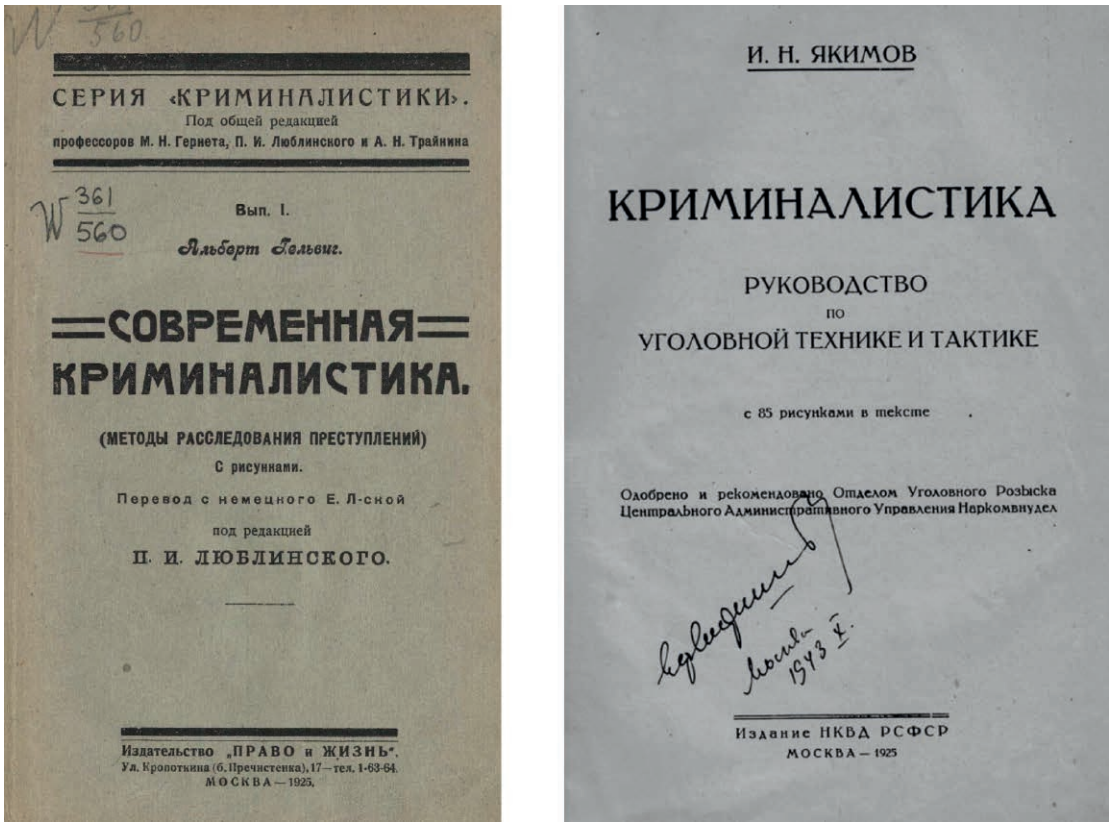

Рис. 3. Обложки книг А. Гельвига (слева) и И.Н. Якимова (справа)
Fig. 3. *The covers of the books by A. Gelwig's book (left) and I.N. Yakimov's (right)*

В 1941 году в СССР вышел русский перевод избранных частей «Руководства по криминалистике» Эдмона Локара, однако раздел о криптографии в него не вошел [31].

Криминалистика и криптология на современном этапе

В современных учебниках по криминалистике криптография не рассматривается. Не уделено внимания ей и в фундаментальном труде профессора Р.С. Белкина «Курс криминалистики» [32]. В книге «Цифровая криминалистика» для вузов издания 2021 года криптография упоминается только при рассмотрении разделов, посвященных блокчейну, электронной цифровой подписи, устройству SIM-карт, электронному ключу и криптозащите [33].

В рабочей программе дополнительной образовательной программы профессиональной переподготовки экспертов системы Минюста России по экспертной специальности 21.1. «Исследование информационных компьютерных средств», утвержденной Российским федеральным центром судебной экспертизы имени профессора А.Р. Шляхова при Минюсте России в 2024 году, в перечнях объектов исследования отсутствует упоминание о криптографических объектах и методах их исследования[8].

В настоящее время благодаря широкому использованию криптографии в информационно-телекоммуникационных технологиях (связь, анонимность в социальных сетях, финансовые технологии и др.) как никогда важно изучать эту науку в рамках криминалистики и судебной компьютерно-технической экспертизы. К тому же в последние годы наблюдается рост как числа разработок в области шифрования, осуществляемых представителями криминального мира, специализирующимися на киберпреступлениях, связанных с преодолением существующих систем информационной защиты, так и финансовых вложений представителей организованной преступности в разработку собственных криптографических систем, позволяющих скрывать преступные коммуникации и финансовые потоки, в том числе транснациональные. Данные обстоятельства обусло-

[8] Дополнительная образовательная программа профессиональной переподготовки по экспертной специальности 21.1. «Исследование информационных компьютерных средств». Утв. ФБУ РФЦСЭ имени профессора А.Р. Шляхова при Минюсте России (3 редакция). 2024.

вили сближение целей и задач специалистов по криптографии и связанной с ней кибербезопасности, криминалистов и следователей, специализирующихся на расследовании компьютерных преступлений, а также экспертов по судебной компьютерно-технической экспертизе.

Кроме того, интерес к криптографии усилился в связи с распространением компьютерных преступлений и дополнением Уголовного кодекса Российской Федерации главой 28 «Преступления в сфере компьютерной информации». Правоохранительные органы и суды столкнулись с необходимостью получения знаний как о цифровых технологиях в целом, так и изучения основ криптографии. При проведении следственных действий по делам о компьютерных преступлениях, изъятии и последующем исследовании компьютерных средств стало обязательным участие соответствующего специалиста (ст. 164.1 УК РФ «Особенности изъятия электронных носителей информации и копирования с них информации при производстве следственных действий»). Кроме того, частью 7 статьи 185 УПК РФ предусмотрено право на осмотр и выемку электронных или иных передаваемых по сетям электросвязи сообщений. При проведении таких следственных действий нередко приходится иметь дело с зашифрованной компьютерной информацией.

Судебные эксперты при проведении компьютерно-технических экспертиз сталкиваются с необходимостью расшифровки закодированной информации (главным образом в виде файлов, закодированного содержания компьютера), в том числе сообщений, переданных по системам кодированной мобильной или интернет-связи. При этом объектами исследования зачастую являются зашифрованные данные, связанные не только с делами о компьютерных преступлениях.

Типичными местами концентрации сведений, подверженных криптографической защите, являются:

– текстовые, голосовые, фото- и видеосообщения, передаваемые через сервисы мгновенного обмена данными;

– данные, передаваемые посредством электронных почтовых сервисов;

– данные, хранящиеся на компьютерах (на локальных или удаленных серверах) в виде пользовательских или системных файлов;

– данные, распространяемые посредством блокчейн-технологии. В них концентрируется криминалистически значимая информация (сообщения, координирующие преступную деятельность; изображения с детской порнографией; создание и использование криптовалюты; теневая бухгалтерская отчетность и т.п.).

При проведении судебных компьютерно-технических экспертиз периодически возникает необходимость преобразования зашифрованной информации в доступную для исследования, оценки и использования в судопроизводстве.

Известны четыре основных направления атак на шифры:

1. Прямой подбор ключей к шифрам методом последовательного перебора известной буквенно-цифровой и символьной информации, а также специально подготовленных справочников «паролей». Для этой цели используются отдельно оборудованные вычислительные устройства, сети вычислительных устройств, а также специализированные облачные сервисы. Путем перебора можно взломать любой современный шифр, все зависит лишь от мощности устройства и наличия нужного количества времени. К примеру, один современный компьютер способен проверить около десяти тысяч вариантов ключей в секунду, а специализированные центры, состоящие из тысячи компьютеров, способны за такое же время проверить десятки миллионов ключей.

2. Исследование современных алгоритмов шифрования с целью их дальнейшего взлома. Основная идея метода – обнаружение уязвимостей и «дыр» в алгоритмах шифрования и программных продуктах. В данный процесс инвестируются немалые деньги, и та информация, которая может в итоге быть получена, имеет большое значение как для правоохранительных структур, так и для разработчиков устройств.

3. Сотрудничество с разработчиками устройств, программ, алгоритмов шифрования и внедрение «бэкдоров», то есть неких программ, которые используются для получения несанкционированного удаленного доступа к защищенной информации за счет уязвимости систем безопасности.

Не всегда правоохранительные структуры получают доступ к зашифрованным данным в оптимальные сроки, именно поэтому разработчики могут оставить некую «лазейку» для дешифрования.

4. Криминалистический анализ оперативной памяти. С помощью специализированных методик исследуется информация из оперативной памяти, где могут быть обнаружены ключи шифрования.

Основными целями технико-криминалистического обеспечения деятельности по получению компьютерной информации, преобразованной методами криптографии, являются:

– предоставление возможности непосредственного использования субъектами расследования и/или судебными экспертами мобильных аппаратно-программных комплексов и специализированных компьютерных программ, позволяющих обходить блокировки в виде паролей и пинкодов;

– восстановление удаленных данных, расшифровка закодированных файлов, криптографических контейнеров;

– извлечение данных из облачных сервисов при отсутствии сведений об учетных данных пользователя[9].

Результатом применения специализированных технико-криминалистических средств является возможность дальнейшего преобразования компьютерной информации в доступную для восприятия форму, ее изъятия, последующего анализа, оценки и использования в интересах судопроизводства.

Поскольку при совершении ряда преступлений используется криптовалюта (кражи или вымогательство денежных средств, мошенничество, незаконная торговля наркотиками, коррупционные преступления, отмывание и легализация денежных средств, вымогательство, налоговые правонарушения и др.), в уголовно-правовой и криминалистической литературе появились термины «криптопреступления», «криптопреступность», «криптовалютные преступления» [34]. Однако для решения задач, возникающих при расследовании таких преступлений, привлекаются главным образом специалисты и эксперты в области движения криптовалютных средств, а не в области криптографии. Они должны обладать знаниями технологии блокчейн, а также знаниями о том, как функционируют программные продукты, используемые для совершения операций с криптовалютами [35, с. 675].

В процессе подготовки данной статьи была предпринята попытка изучения практики использования средств дешифрования при проведении судебной компьютерно-технической экспертизы по уголовным делам. Были изучены все приговоры судов общей юрисдикции за 2024 год, в которых встречалось хотя бы одно слово с корнем «крипт». Таких приговоров в базе данных «Право Тех» оказалось 160. Ни в одном из приговоров не приводилась информация о проведении судебной компьютерно-технической экспертизы, в ходе которой было бы осуществлено дешифрование или иное исследование каких-либо криптографически защищенных объектов, имеющих доказательственное значение. Основную часть употреблений слов с корнем «крипт» составили слова «криптовалюта» (40 приговоров), «криптокошелек» (7 приговоров), а также словосочетания «криптографически защищенная электронная цифровая подпись» (66 приговоров), «криптографически защищенный мессенджер “Telegram”» (37), «средства криптографической защиты» (10). Представляется, что такое положение дел в значительной степени обусловлено тем, что сотрудники подразделений судебной компьютерно-технической экспертизы государственных судебно-экспертных учреждений (за исключением находящихся в ведении ФСБ России), а также негосударственных судебно-экспертных учреждений из-за отсутствия необходимых программно-аппаратных средств криптографических исследований и соответствующих знаний и навыков отказываются от решения вопросов, связанных с криптографией.

Серьезным препятствием для эффективного решения задач судебной компьютерно-технической экспертизы является быстрое развитие индустрии программно-технических средств шифрования информации при заметном отставании разработок, предназначенных для криминали-

[9] Зиновьева Н.С. Компьютерная информация, преобразованная методами криптографии, в раскрытии и расследовании преступлений: автореф. дис. …канд. юрид. наук. Краснодар, 2021. С. 15.

стов средств дешифровки кодированной информации, представляющей интерес для целей судопроизводства и размещенной на компьютерах, средствах мобильной связи, разнообразных гаджетах, а также в облачных хранилищах.

В настоящее время существует ряд инструментов дешифрования, доступных судебным экспертам. Однако они обеспечивают решение далеко не всех возникающих перед экспертами задач.

Возможности судебной компьютерно-технической экспертизы по дешифрованию криминалистически значимой компьютерной информации напрямую зависят от уровня развития индустрии и технологий кибербезопасности. При этом важное значение имеет скорость внедрения средств дешифрования в повседневную практику этого вида экспертизы.

Основными требованиями, предъявляемыми к криминалистическим средствам исследования зашифрованной компьютерной информации, являются:

– высокая скорость дешифровки;

– простота использования соответствующего инструмента;

– многофункциональность криминалистических средств, обеспечивающая возможность преодоления паролей, анализа реестра компьютера, восстановление удаленных файлов, расшифровку закодированных файлов и других необходимых данных;

– точность и достоверность полученных результатов.

На рынке компьютерных средств предлагается несколько продуктов, предназначенных для расшифровки закодированных (защищенных) данных в процессе проведения судебной компьютерно-технической экспертизы.

Elcomsoft Forensic Disk Decryptor обеспечивает мгновенный доступ к данным, хранящимся в зашифрованных дисках и контейнерах BitLocker, FileVault 2, PGP Disk, TrueCrypt и VeraCrypt. Инструмент извлекает криптографические ключи из RAM-захватов, гибернации и файлов подкачки или использует текстовый пароль или ключи депонирования для расшифровки файлов и папок, хранящихся в криптоконтейнерах, или монтирует зашифрованные тома в качестве новых букв дисков для мгновенного доступа в реальном времени. Программа извлекает метаданные шифрования из зашифрованных дисков TrueCrypt, VeraCrypt, BitLocker, FileVault, PGP Disk и LUKS/LUKS2, дисков и контейнеров Jetico BestCrypt. Дополнительным решением является бесплатный портативный инструмент командной строки Elcomsoft Encrypted Disk Hunter, который позволяет быстро обнаружить наличие зашифрованных томов при выполнении анализа системы в реальном времени.

Elcomsoft Forensic Disk Decryptor может автоматически расшифровывать все содержимое зашифрованного контейнера, предоставляя эксперту полный, неограниченный доступ ко всей информации, хранящейся на зашифрованных томах.

Passware Kit Forensic – криптографическое решение для обнаружения электронных улик, которое позволяет, как утверждают его разработчики, получать отчеты и расшифровывать все защищенные паролем объекты на компьютере. Программа распознает более 280 типов файлов и работает в пакетном режиме восстановления паролей.

Passware Kit Forensic находит все зашифрованные или защищенные паролем документы, архивы и другие файлы. Сортирует по сложности расшифровки, осуществляет быстрое сканирование изображений памяти и файлов в одном режиме. Извлекает ключи шифрования для FileVault2, TrueCrypt, VeraCrypt и BitLocker для мгновенной расшифровки дисков и контейнеров, обеспечивает создание словаря паролей или извлечение паролей учетных записей для Windows и Mac.

EnCase Forensic включает EnCase Decryption Suite, инструмент для расшифровки дисков, томов, файлов и папок, записей реестра, зашифрованной электронной почты.

Комплексы программно-технических средств, предназначенных для судебно-экспертного исследования зашифрованной компьютерной информации, имеющиеся в распоряжении компьютерно-технических экспертных подразделений судебно-экспертных учреждений Минюста России, Следственного комитета и МВД Российской Федерации, не всегда позволяют успешно осуществить дешифрование закодированных объектов. Многие программы шифрования являются продуктами иностранных компаний и доступны широкому кругу пользователей. В то же время программно-технические средства извле-

чения ключей шифрования, преодоления систем защиты и раскодировки зашифрованных объектов в условиях санкций стали недоступными для обновления, что создает большие трудности в процессе судебно-экспертного исследования. Такое положение дел диктует необходимость разработки высокоэффективных отечественных средств дешифрования, предназначенных для использования судебными экспертами компьютерно-технических подразделений экспертно-криминалистических служб и судебно-экспертных учреждений соответствующих ведомств.

К сожалению, в отечественной криминалистике вопросам использования методов криптоанализа при проведении судебных экспертиз и некоторых других следственных действий уделяется недостаточно внимания. При этом результаты анализа истории взаимосвязи криминалистики и криптографии могут содействовать выработке стратегии дальнейших совместных исследований, направленных на повышение эффективности использования достижений криптографии в следственной и судебной практике, а также разработке и внедрению новых методик судебной компьютерно-технической экспертизы.

Большой вклад в сохранение истории криптографии и ее популяризацию вносит открытый в декабре 2021 года Научно-производственной компанией «Криптонит» первый и единственный в стране научно-технологический Музей криптографии, посвященный собственно криптографии, а также смежным дисциплинам и технологиям коммуникации. С помощью уникальной коллекции шифровальной техники, средств передачи информации и архивных документов, большинство из которых ранее составляло государственную тайну и было рассекречено специально для демонстрации в музее, экспозиция рассказывает о прошлом, настоящем и будущем криптографии, о людях и изобретениях, изменивших мир[10].

Заключение

Дополнение и уточнение истории криминалистики и криптографии важно для понимания их становления и развития. Описание незаслуженно забытого фундаментального труда, посвященного основам расследования преступлений флорентийского юриста-криминалиста Антонио Марии Коспи, и его книги об основах криптографии представляется полезным и позволяет более глубоко изучить и осмыслить исторический путь криминалистики и ее связь с криптографией. К сожалению, в итальянской исторической и криминалистической литературе фигуре А.М. Коспи уделено крайне мало внимания. Нет упоминаний о нем и в отечественных публикациях по всеобщей истории криминалистики, где безоговорочно признается приоритет австрийца Ганса Гросса, который либо не был знаком с книгой Коспи, либо не посчитал нужным упомянуть ее в своем Руководстве.

Российские и советские криминалисты в начале 20 века активно использовали многовековой мировой опыт анализа криптограмм и предпринимали определенные усилия по включению основ криптографии в профессиональную подготовку следователей и экспертов-криминалистов.

Криминалистика и криптография шли «рука об руку» вплоть до Первой Мировой войны 1914–1919 гг. В дальнейшем благодаря серьезным финансовым вливаниям и мобилизации научных ресурсов в военную, дипломатическую и контрразведывательную криптографию, криминалистическая криптография сначала заметно отстала в своем развитии, а в последние годы уступила место современным технологиям, разрабатываемым в частной и государственно-частной индустрии информационной безопасности (кибербезопасности) и успешно используемым в сфере судебной компьютерно-технической экспертизы и цифровой криминалистики. Такое положение дел диктует необходимость создания высокоэффективных отечественных средств дешифрования, предназначенных для использования судебными экспертами компьютерно-технических подразделений экспертно-криминалистических служб и судебно-экспертных учреждений соответствующих ведомств.

[10] Музей криптографии. https://cryptography-museum.ru/

СПИСОК ЛИТЕРАТУРЫ

1. Cospi A.M. I'l Giudice Criminalista. Firenze: nella stamperia di Zanobi Pignoni, 1643. 610 p.
2. Хазиев Ш.Н. Из истории криминалистики: Антонио Мария Коспи (1560-1635) // Теория и практика судебной экспертизы. 2023. Т. 18. № 4. С. 65–71. https://doi.org/10.30764/1819-2785-2023-4-65-71
3. Cospi A.M. La Interpretazione delle Cifre, Cioe Regola per Intendere Bene, e Facilmente Qualsiuoglia Cifra Semplice. Firenze: nella stamperia di Zanobi Pignoni, 1639. 48 p.
4. Cospi A.M. L'Interprétation des Chiffres, ou Reigle pour Bien Entendre et Expliquer Facilement Toutes Sortes de Chiffres Simples. Tiré de l'italien du Sr Ant. Maria Cospi… par F. I. F. N. P. M. Paris: chez Augustin Courbé, 1641. 98 p.
5. Schott G. Schola Steganographica. Nürnberg: Sumptibus Johannis Andreae Endteri &Wolfgangi Junioris haeredum, excudebat Jobus Hertz, 1665. 346 p.
6. Хазиев Ш.Н. Доктор Рудольф Арчибальд Рейсс и его роль в развитии международного сотрудничества в области судебной экспертизы // Теория и практика судебной экспертизы. 2013. № 2 (30). С. 123–129.
7. Locard E. La Cryptographie en Technique Policière. Étude sur L'emploi des Écritures Chiffrées par les Malfaiteurs. Lyon: A. Rey, 1912. 19 p.
8. Archives d'Anthropologie Criminelle, de Médecine Légale et de Psychologie Normale et Pathologique. 1912. Vol. 3. P. 555.
9. Archives d'Anthropologie Criminele, de Médecine L gale et de Psychologie Normale et Pathologique. 1913. Vol. 28. 964 p.
10. Salle M. Dr Edmond Locard, Expert, Lyon. «Percevoir l'invisible». Le Travail de L'expert en criture Selon Ed. Locard. 2010. 78 p.
11. Locard E. L'Enquête Criminelle et les Méthodes Scientifiques. Paris, 1920. 303 p.
12. Locard E. Traite de Criminalistique. Vol. 6. Lyon: Desviqne (Joannes), 1937. P. 495–1014.
13. Locard E. Le Commandant Bazeries: un Grand Cryptologue Françqis // Revue Internationale de Criminalistique. 1931. No. 10. 10 p.
14. Пернелл С. Хромая дама. Нерассказанная история женщины – тайного агента периода Второй мировой войны. М.: АСТ, 2023. 491 с.
15. Remarkable Women: The Life and Times of Virginia Hall (Part 2) // Rhap.so.dy in words. 20.11.2019. https://rhapsodyinwords.com/tag/suzanne-bertillon/
16. Locard E. Les Faux en Ecriture et Leur Expertise. Paris: Payot, 1959. 42 p.
17. Locard E. Cryptography in Criminal Matters // International Criminal Police Review. 1946. Vol. 1. No. 2. P. 17.
18. Artières P. *et al.* «Percevoir L'invisible». Le Travail de L'expert en Écriture Selon Edmond Locard (1877–1966). 2010. 70 p.
19. Locard J. Cours de Police Scientifique. 2-e edition. Lyon, 1951. 92 p.

REFERENCES

1. Cospi A.M. *I'l Giudice Criminalista.* Firenze: nella stamperia di Zanobi Pignoni, 1643. 610 p.
2. Khaziev Sh.N. From the History of Criminalistics: Antonio Maria Cospi (1560-1635). *Theory and Practice of Forensic Science.* 2023. Vol. 18. No. 4. P. 65–71. (In Russ.). https://doi.org/10.30764/1819-2785-2023-4-65-71
3. Cospi A.M. *La Interpretazione delle Cifre, Cioe Regola per Intendere Bene, e Facilmente Qualsiuoglia Cifra Semplice.* Firenze: nella stamperia di Zanobi Pignoni, 1639. 48 p.
4. Cospi A.M. *L'Interprétation des Chiffres, ou Reigle pour Bien Entendre et Expliquer Facilement Toutes Sortes de Chiffres Simples.* Tiré de l'italien du Sr Ant. Maria Cospi… par F. I. F. N. P. M. Paris: chez Augustin Courbé, 1641. 98 p.
5. Schott G. *Schola Steganographica.* Nürnberg: Sumptibus Johannis Andreae Endteri &Wolfgangi Junioris haeredum, excudebat Jobus Hertz, 1665. 346 p.
6. Khaziev Sh.N. Doctor Rudolf Archibald Reiss and His Role in the Development of International Cooperation in the Field of Forensic Science. *Theory and Practice of Forensic Science*. 2013. No. 2 (30). P. 123–129. (In Russ.).
7. Locard E. *La Cryptographie en Technique Policière. Étude sur L'emploi des Écritures Chiffrées par les Malfaiteurs.* Lyon: A. Rey, 1912. 19 p.
8. *Archives d'Anthropologie Criminele, de Médecine Légale et de Psychologie Normale et Pathologique.* 1912. Vol. 3. P. 555.
9. *Archives d'Anthropologie Criminele, de Médecine Légale et de Psychologie Normale et Pathologique.* 1913. Vol. 28. 964 p.
10. Salle M. *Dr Edmond Locard, Expert, Lyon. "Percevoir l'invisible". Le Travail de L'expert en Écriture Selon Ed. Locard.* 2010. 78 p.
11. Locard E. *L'Enquête Criminelle et les Méthodes Scientifiques.* Paris, 1920. 303 p.
12. Locard E. *Traite de Criminalistique. Vol. 6.* Lyon: Desviqne (Joannes), 1937. P. 495–1014.
13. Locard E. Le Commandant Bazeries: un Grand Cryptologue Françqis. *Revue Internationale de Criminalistique.* 1931. No. 10. 10 p.
14. Purnell S. *A Woman of No Importance: The Untold Story of Virginia Hall, WWII's Most Dangerous Spy.* Moscow: AST, 2023. 491 p. (In Russ.).
15. Remarkable Women: The Life and Times of Virginia Hall (Part 2). *Rhap.so.dy in words.* 20.11.2019. https://rhapsodyinwords.com/tag/suzanne-bertillon/
16. Locard E. *Les Faux en Ecriture et Leur Expertise.* Paris: Payot, 1959. 42 p.
17. Locard E. Cryptography in Criminal Matters. *International Criminal Police Review*. 1946. Vol. 1. No. 2. P. 17.
18. Artières P., *et al. "Percevoir l'invisible". Le Travail de L'expert en Écriture Selon Edmond Locard (1877–1966).* 2010. 70 p.
19. Locard J. *Cours de Police Scientifique. 2-e edition.* Lyon, 1951. 92 p.

20. Рейсс Р.А. Научная техника расследования преступлений. Курс лекций, прочтенных в г. Лозанне профессором Рейссом чинам русского судебного ведомства летом 1911 г. / Под ред. С.Н. Трегубова. СПб.: Сенатская типография, 1912. 178 с.
21. Трегубов С.Н. Основы уголовной техники. Научно-технические приемы расследования преступлений. Петроград: Издание Юридического книжного склада «Право», 1915. 334 с.

22. Бахарев В. О шифрах. Женева: Издание Союза русских социал-демократов, 1902. 24 с.

23. Розенталь П.И. Шифрованное письмо: критика употребляемых у нас систем шифра. Женева: Всеобщий еврейский рабочий союз в Литве, Польше и России (Бунд), 1904. 112 с.
24. Перегудова З.И. Главный криптограф политического сыска дореволюционной России И.А. Зыбин // Политическая Россия: прошлое и современность. Всероссийские исторические чтения «Гороховая, 2». Вып. 2. 2006. С. 40–56.
25. Зданович А.А., Измозик В.С. Сорок лет на секретной службе: жизнь и приключения Владимира Кривоша. М.: Кучково поле, 2007. 384 с.
26. Гребенников В. Российская криптология. История спецсвязи. Москва: Автор, 2023. 274 с.
27. Гребенников В. Криптология и секретная связь. Сделано в СССР. М.: Эксмо, 2017. 480 с.

28. Гельвиг А. Современная криминалистика (Методы расследования преступлений). Серия «Криминалистика» № 1 / Пер. с нем. Е. Л-ской; под ред. П.И. Люблинского. М.: Право и жизнь, 1925. 100 с.
29. Шнейкерт Г. Тайна преступника и пути к ее раскрытию (К учению о судебных доказательствах). Серия «Криминалистика». Вып. II / Пер. с нем.; под ред. П.И. Люблинского. М.: Право и жизнь, 1925. 64 с.
30. Якимов И.Н. Криминалистика. Руководство по уголовной технике и тактике. М.: НКВД РСФСР, 1925. 430 с.
31. Локар Э. Руководство по криминалистике / Пер. С.В. Познышева и Н.В. Терзиева; под ред. С.П. Митричева. М.: Юридическое издательство НКЮ СССР, 1941. 544 с.

32. Белкин Р.С. Курс криминалистики. 3-е изд. дополненное. М.: ЮНИТИ-ДАНА: Закон и право, 2001. 837 с.
33. Цифровая криминалистика: учебник для бакалавриата, специалитета и магистратуры / Под редакцией В.Б. Вехова, С. В. Зуева. М.: Юрайт, 2021. 417 с.
34. Сидоренко Э.Л. Криптопреступность как новое криминологическое явление // Общество и право. 2018. № 2 (64). С. 15–21.

20. Reiss R.A. *Scientific Technique of Crime Investigation. Lecture Course Delivered in Lausanne by Professor Reiss to Officials of the Russian Judicial Department in the Summer of 1911* / S.N. Tregubov (ed.). Saint Petersburg: Senatskaya tipografiya, 1912. 178 p. (In Russ.).
21. Tregubov S.N. *Fundamentals of Criminal Technique. Scientific and Technical Methods of Crime Investigation.* Petrograd: Izdanie Yuridicheskogo knizhnogo sklada “PRAVO”, 1915. 334 p. (In Russ.).
22. Bakharev V. *On Ciphers.* Geneva: Izdanie Soyuza russkikh sotsial-demokratov, 1902. 24 p. (In Russ.).
23. Rosenthal’ P.I. *Cipher Letter: Critique of the Cipher Systems Used by Us.* Geneva: Vseobshchii evreiskii rabochii soyuz v Litve, Pol’she i Rossii (Bund), 1904. 112 p. (In Russ.).
24. Peregudova Z.I. Chief Cryptographer of Political Investigation in Prerevolutionary Russia I.A. Zybin. *Political Russia: Past and Present. Historical Readings “Gorokhovaya, 2”*. Iss. 2ю 2006. P. 40–56. (In Russ.).

25. Zdanovich A.A., Izmozik V.S. *Forty Years in the Secret Service: The Life and Adventures of Vladimir Krivosh.* Moscow: Kuchkovo pole, 2007. 384 p. (In Russ.).
26. Grebennikov V. *Russian Cryptology. History of Special Communications.* Moscow: Author, 2023. 274 p. (In Russ.).
27. Grebennikov V. *Cryptology and Secret Communications. Made in the USSR.* Moscow: Eksmo, 2017. 480 c. (In Russ.).
28. Gelwig A. *Modern Forensic Science (Methods of Investigating Crimes)* / Trans. from Germ. E. L-skaya. P.I. Lyublinsky (ed.) Moscow: Pravo i zhizn’, 1925. 100 p. (In Russ.).

29. Schneikert G. *The Secret of the Criminal and the Ways to Solve It / Trans. from Germ. P.I. Lyublinsky.* Moscow: Pravo i zhizn’, 1925. 64 p. (In Russ.).

30. Yakimov I.N. *Forensic Science. Guide to Criminal Technique and Tactics.* Moscow: NKVD RSFSR, 1925. 430 p. (In Russ.).
31. Lokar E. *Handbook of Forensic Science* / Translated by prof. S.V. Poznysheva and N.V. Terziev. S.P. Mitrichev (ed.). Moscow: Yuridicheskoe izdatel’stvo NKYu SSSR, 1941. 544 p. (In Russ.).
32. Belkin R.S. *Course in Criminalistics. 3rd ed.*. Moscow: UNITY-DANA: Zakon i pravo, 2001. 837 p. (In Russ.).
33. *Digital Forensics: Textbook for Bachelor’s, Specialist and Master’s Degrees*. V.B. Vekhov, S.V. Zuev (eds.). Moscow: Yurait, 2021. 417 p. (In Russ.).
34. Sidorenko E.L. Crypto-crime as a New Criminological Phenomenon. *Society and Law.* 2018. No. 2 (64). P. 15–21. (In Russ.).

35. Гармаев Ю.П., Осипов Г.П. Привлечение специалиста для исследования криптовалют в уголовном, гражданском и арбитражном судопроизводствах // Вестник РУДН. Серия: Юридические науки. 2024. Т. 28. № 3. С. 669–684.

35. Garmaev Yu.P., Osipov G.P. Engaging a Specialist for the Investigation of Cryptocurrencies in Criminal, Civil and Arbitration Proceedings. *RUDN Journal of Law*. 2024. Vol. 28. No. 3. P. 669–684. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРАХ

Хазиев Шамиль Николаевич – д. юр. н., главный научный сотрудник отдела научно-методического обеспечения Российского федерального центра судебной экспертизы имени профессора А.Р. Шляхова при Минюсте России, советник по научной деятельности генерального директора АО «Научно-производственная компания “Криптонит”»; e-mail: sh.khaziev@sudexpert.ru

Штохов Александр Николаевич – заместитель генерального директора АО «Научно-производственная компания “Криптонит”»;
e-mail: a.shtokhov@kryptonite.ru

Статья поступила: 23.01.2025
После доработки: 17.02.2025
Принята к печати: 10.03.2025

ABOUT THE AUTHORS

Khaziev Shamil Nikolaevich – Doctor of Law, Principal Researcher at the Forensic Research Methodology Department of the Russian Federal Centre of Forensic Science named after professor A.R. Shlyakhov of the Ministry of Justice of the Russian Federation; Academic Advisor to the General Director of the Joint Stock Company “Research and Development Company “Kryptonite”;
e-mail: sh.khaziev@sudexpert.ru

Shtokhov Aleksander Nikolaevich – Deputy General Director of the Joint Stock Company “Research and Development Company “Kryptonite”;
e-mail: a.shtokhov@kryptonite.ru

Received: January 23, 2025
Revised: February 17, 2025
Accepted: March 10, 2025