ГОСУДАРСТВО И ПРАВО, 2024, № 10, с. 156–168
STATE AND LAW, 2024, No. 10, pp. 156–168

УКРЕПЛЕНИЕ ЗАКОННОСТИ И БОРЬБА С ПРЕСТУПНОСТЬЮ

УДК 343.98:004
ББК 67.52:32.8

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ОБЩЕЙ ТЕОРИИ КРИМИНАЛИСТИКИ СКВОЗЬ ПРИЗМУ СОВРЕМЕННЫХ ТЕХНОЛОГИЙ

© 2024 г. А. Н. Савенков[1, *], Е. Р. Россинская[2, **]

[1]Институт государства и права Российской академии наук, г. Москва
[2]Московский государственный юридический университет им. О.Е. Кутафина (МГЮА)

**E-mail: an61s@mail.ru*
***E-mail: elena.rossinskaya@gmail.com*

Поступила в редакцию 03.07.2024 г.

Аннотация. В статье рассмотрены некоторые актуальные направления развития общей теории криминалистики в русле интеграции и дифференциации научного знания с учетом тенденций глобальной цифровизации и интеграции современных технологий в сферу расследования преступлений. Осуществлен анализ актуальных определений предмета криминалистики, данных ведущими учеными-криминалистами России, Беларуси, Казахстана, Азербайджана и других стран, который показывает, что большинство из них так или иначе согласуется с определением предмета науки Р.С. Белкина. Сравнительный анализ цифровой криминалистики (В.Б. Вехов и С.В. Зуев), под которой авторы понимают частную теорию криминалистики, включает общую часть, весьма сходную с общими положениями разработанной нами теории информационно-компьютерного обеспечения криминалистической деятельности, и особенную часть, которая относится в первую очередь к развитию информационно-компьютерного обеспечения криминалистической техники и технологии. Намечены пути развития теории криминалистического следоведения, в котором с учетом новых криминалистических технологий место происшествия, потерпевший, способ преступления и преступник должны быть связаны через разнообразные механизмы следообразования. Рассмотрены способы компьютерных преступлений и концепция построения информационно-компьютерных криминалистических моделей компьютерных преступлений на базе теории информационно-компьютерного обеспечения криминалистической деятельности. За основу были выбраны корреляционные связи между комбинациями IT-технологий, применяемых для осуществления компьютерных преступлений, следовой картиной в виде цифровых следов и уровнем компетенций в IT-технологиях преступника и потерпевшего.

Ключевые слова: общая теория криминалистики, следоведение, способы преступлений, компьютерные преступления, цифровизация, цифровые следы, информационно-компьютерные модели.

Цитирование: *Савенков А.Н., Россинская Е.Р.* Актуальные направления развития общей теории криминалистики сквозь призму современных технологий // Государство и право. 2024. № 10. С. 156–168.

DOI: 10.31857/S1026945224100145

CURRENT DIRECTIONS IN THE DEVELOPMENT OF THE GENERAL CRIMINALISTIC THROUGH THE PRISM OF MODERN TECHNOLOGIES

© 2024 A. N. Savenkov[1, *], E. R. Rossinskaya[2, **]

[1]Institute of State and Law of the Russian Academy of Sciences, Moscow
[2]Kutafin Moscow State Law University (MSAL)

**E-mail: an61s@mail.ru*
***E-mail: elena.rossinskaya@gmail.com*

Received 03.07.2024

Abstract. The article examines some current trends in the development of the general theory of criminalistic in line with the integration and differentiation of scientific knowledge, considering trends in global digitalization and integration of modern technologies in the field of crime investigation. An analysis of current definitions of the subject of criminology given by leading forensic scientists from Russia, Belarus, Kazakhstan, Azerbaijan and other countries has been carried out, which shows that most of them, one way or another, are consistent with the definition of the subject of science by R.S. Belkin. A comparative analysis of digital criminalistic (V.B. Vekhov and S.V. Zuev), by which the authors understand a particular theory of criminalistic, includes a general part very similar to the general provisions of the theory of information and computer support for criminalistic activities developed by us and a special part that relates first to the development of information and computer support for criminalistic equipment and technology. The ways of developing the theory of criminalistic trace science are outlined, in which, considering new forensic technologies, the relationships between the scene of the incident, the victim, the method of crime and the criminal should be connected through various mechanisms of trace formation. The methods of computer crimes and the concept of constructing information and computer criminalistic models of computer crimes based on the theory of information and computer support for criminalistic activities are considered. The basis was chosen to be correlations between combinations of IT-technologies used to carry out computer crimes, the trace pattern in the form of digital footprints and the level of competence in IT-technologies of the criminal and the victim.

Key words: general theory of criminalistic, criminalistic trace science, methods of crime, computer crimes, digitalization, digital footprints, information-computer models.

For citation: *Savenkov, A.N., Rossinskaya, E.R. (2024).* Current directions in the development of the general criminalistic through the prism of modern technologies // Gosudarstvo i pravo=State and Law, No. 10, pp. 156–168.

В первой четверти XXI в. новый этап научно-технической революции ознаменовался всеобъемлющим проникновением технологий, и в первую очередь информационных компьютерных технологий, в различные области человеческой деятельности – экономическую, социальную, управленческую и другие. Наряду с неоспоримыми достижениями, технологизация и цифровизация принесли с собой целый ряд сложных негативных явлений, связанных с видоизменениями преступности, основными из которых являются: интеллектуализация преступной деятельности; слияние общеуголовной и экономической преступности; преступные попытки установить контроль над финансово-промышленными группами, отдельными предприятиями.

Криминальные структуры в полной мере приняли на вооружение цифровые технологии для совершения «высокотехнологичных» преступлений, новых способов совершения «традиционных» преступлений, создания систем конспирации и скрытой связи, для оказания активного противодействия правосудию[1].

[1] См.: *Савенков А.Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 5–18.

Очевидно, что на эти вызовы должна оперативно отвечать криминалистика – динамично развивающаяся юридическая наука синтетической природы, которая является основным проводником достижений естественных, технических и гуманитарных наук в сферу судопроизводства.

Сравнительный анализ определений предмета криминалистики, данных ведущими учеными-криминалистами России, Беларуси, Казахстана, Азербайджана и других стран показывает, что большинство из них так или иначе согласуется с определением предмета науки Р.С. Белкина[2]. Критики указывают, что в определении Р.С. Белкина перечислены далеко не все закономерности, изучаемые криминалистикой. Да это и невозможно, поскольку каждый из авторов выбирает главные с его точки зрения закономерности, изучаемые криминалистикой. Но совершенно справедливо высказывание А.А. Эксархопуло, что определение Р.С. Белкина отражает не все содержание предмета науки криминалистики, а главным образом его сущность[3]. Разделяем позицию В.Н. Карагодина, что пока «ни одному из инициаторов модернизации теоретико-доказательственной концепции предмета криминалистики или ее замены не удалось доказать наличия объективных потребностей в этом», что не означает отрицания необходимости развития криминалистической науки. Считаем справедливой точку зрения авторов учебника, полагающих, что определение Р.С. Белкина является наиболее полным и в то же время кратким по содержанию, объективно отражающим нынешний уровень развития криминалистики и позволяющим отграничить ее предмет от предметов других наук.

Мы так подробно остановились на предмете криминалистической науки, поскольку возражаем против размывания предмета криминалистики. Не следует каждый раз при появлении новых объектов или методов менять название, определение предмета науки, дробить ее на «отдельные криминалистики» на потребу дня, например, говорить о лингвистической криминалистике[4] или об экономической криминалистике[5], медицинской криминалистике[6]. Криминалистика – это целостная наука, обладающая собственным предметом, структурой, задачами, объектами и принципами[7].

Несколько иначе дело обстоит с т.н. электронной[8], или цифровой, криминалистикой. Как указывают авторы учебника по цифровой криминалистике[9], это название является условным аналогом отрасли знаний Digital Forensic, используемого в зарубежной юридической практике, и «представляет собой не самостоятельную науку, а одно из частных учений». Предмет цифровой криминалистики, по мнению В.Б. Вехова, С.В. Зуева и их соавторов, составляют «закономерности обнаружения, фиксации, предварительного исследования, использования компьютерной информации и средств ее обработки в целях выявления, раскрытия, расследования и предупреждения правонарушений, а также создания на знании этих закономерностей технических средств, приемов, методик и рекомендаций, направленных на оптимизацию деятельности по борьбе с правонарушениями». Данная теория включает общую часть, весьма сходную с общими положениями разработанной нами теории информационно-компьютерного обеспечения криминалистической деятельности[10], и особенную часть, которая относится в первую очередь к развитию информационно-компьютерного обеспечения криминалистической техники и технологии. Ее содержание также перекликается с нашим подходом[11]. Сравнительный анализ представлен в *табл. 1.*

---

[2] См.: *Ищенко Е.П.* Криминалистика: учеб. 3-е изд., испр. и доп. М., 2011. С. 4; Криминалистика: учеб. / Л.Я. Драпкин, В.Н. Карагодин. 2-е изд., перераб. и доп. М., 2011. С. 10; *Порубов Н.И., Грамович Г.И., Порубов А.Н.* Криминалистика: учеб. пособие / под ред. Н.И. Порубова. Минск, 2007. С. 6; Криминалистика: учеб. / под ред. Д.И. Сулейманова. 2-е изд., перераб. и доп. Баку, 2008. С. 62; *Россинская Е.Р., Гинзбург А.Я., Оганов Н.И., Бегалиев Е.Н.* Криминалистика негіздеі. Алматы, 2007. С. 18 (на казах. яз.).

[3] См.: *Эксархопуло А.А.* Криминалистика: учеб. СПб., 2009. С. 13, 14.

[4] См.: *Грачев М.А., Грачев А.М.* Современные проблемы лингвокриминалистики как науки // Вестник Череповецкого гос. ун-та. 2015. № 1. С. 26–29.

[5] См.: *Голубятников С.П.* Экономическая криминалистика: фантом или реальность // Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 118–121.

[6] См.: *Федосюткин Б.А.* Медицинская криминалистика: руководство. Ростов н/Д., 2006. С. 34, 35.

[7] См.: *Россинская Е.Р.* Ревизия определения предмета криминалистики: за и против // Библиотека криминалиста. 2012. № 4. С. 328–335.

[8] См.: *Вехов В.Б.* Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики: сб. тр. участников Междунар. науч.-практ. конф. Ростов н/Д., 2017. С. 40–46.

[9] См.: Цифровая криминалистика: учеб. для вузов / под ред. В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. М., 2024. С. 16–18.

[10] См.: *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193–202.

[11] См.: *Россинская Е.Р., Семикаленова А.И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник СПбУ. Право. 2020. Т. 11. Вып. 3. С. 745–759.

Таблица 1

Система теории информационно-компьютерного обеспечения криминалистической деятельности	Система цифровой криминалистики
1. Концепция теории информационно-компьютерного обеспечения криминалистической деятельности, включая предмет теории и ее объекты. 2. Учение о способах компьютерных преступлений/правонарушений. 3. Учение о цифровых следах как источниках криминалистически значимой компьютерной информации. 4. Учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники. 5. Учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий. 6. Учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений. 7. Учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений. 8. Учение о цифровизации системы криминалистической регистрации.	*Общая часть*: ее понятие, предмет, объект, цели, задачи, система, методологическая основа, науковедческие связи с существующими криминалистическими теориями (учениями) и другими науками, специальные термины и определения – терминологический аппарат, расширяющий язык криминалистики. *Особенная часть* – это комплекс частных взаимосвязанных учений об отдельных родах и видах компьютерной информации, ее материальных носителей, средств обработки и защиты: 1. Криминалистическое учение о цифровой (компьютерной) информации. 2. Криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей. 3. Криминалистическое использование цифровой (компьютерной) информации, средств ее обработки и защиты.

Полагаем, что подобная структура обоснована и заслуживает дальнейшего развития, но пока не очень ясно, как она вписывается в систему криминалистической науки.

Развитие криминалистики происходит благодаря изучению новых закономерностей, новых механизмов формирования следов, новых методов сбора, обнаружения, фиксации и изъятия криминалистически значимой информации, а также анализу и использованию этой информации в сфере криминалистической тактики и методики[12].

Рассмотрим некоторые направления развития и совершенствования ряда криминалистических учений – составных частей общей теории криминалистики в свете интеграции и дифференциации научного знания в условиях цифровой трансформации экосистемы.

Начнем с тенденций развития криминалистического учения о следах. Любое преступление вызывает следы – отражение преступных действий в окружающей среде. Различают криминалистическое понятие следов в широком и узком смысле. В узком смысле под следом понимается отображение на одном из объектов внешнего строения (морфологии) другого объекта. Элементами этого процесса являются объекты следообразования в трасологии – следообразующий, следовоспринимающий и вещество следа, следовой контакт как результат взаимодействия между ними[13]. «Трасология как область криминалистических знаний изучает закономерности морфологии поверхностей и функциональных свойств следообразующих объектов и механизма взаимодействия, ведущего к отображению их признаков в следах»[14]. Трасологические методы при изучении процессов следообразования по морфологическим признакам внешнего строения следообразующих и следовоспринимающих объектов используются не только в трасологии, но и в баллистике, при криминалистическом исследовании документов и почерка, взрывных устройств и других объектов.

В широком смысле следы – это любые материальные последствия преступления, т.е. любые изменения объекта или вещной обстановки, которые отражают взаимодействие объектов, их связь между собой и с расследуемым событием, особенности их морфологии, структуры и свойств, выражающихся в криминалистически значимых признаках. В целом криминалистическое следоведение – это учение, «изучающее закономерности образования различных следов, связанных с событием

[12] См.: *Савенков А.Н., Россинская Е.Р.* Вектор инновационного развития криминалистической науки в условиях глобальной цифровизации // Государство и право. 2023. № 5. С. 100–110.

[13] См.: *Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р.* Криминалистика. 4-е изд. перераб. и доп. М., 2013. С. 36.

[14] *Майлис Н.П.* Трасология и трасологическая экспертиза: курс лекций М., 2015. С. 12.

преступления, методы, приемы и средства их собирания и исследования, а также возможности их использования для выяснения обстоятельств содеянного, установления и изобличения преступника»[15].

Задачи исследования следов в криминалистике, как отмечал К.Д. Поль, состоят в установлении взаимосвязи между местом происшествия, потерпевшим, орудием преступления и преступником, и на этой основе оптимально реконструировать или подтвердить результатами аналитических исследований ход происшествия. Для доказательства соответствующей взаимосвязи им предложен принцип перекрестного переноса следов, схематически выраженный в «кресте следов»[16] (*рис. 1.*), причем значимость доказательства возрастает пропорционально количеству выявленных перекрещивающихся комплексов следов.

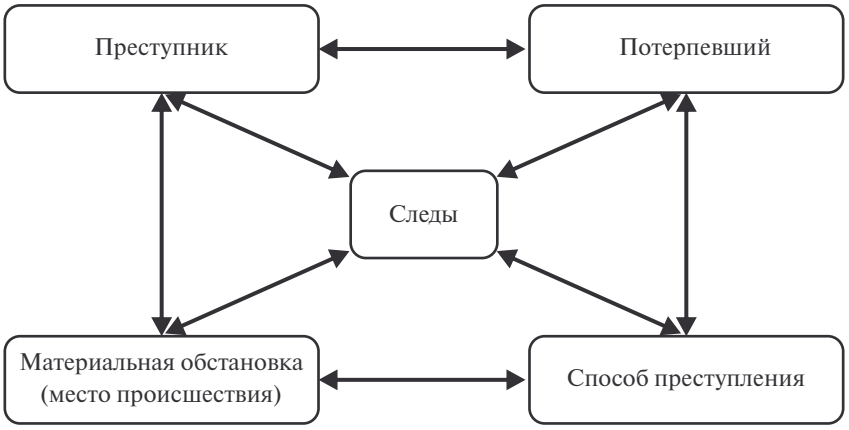

Рис. 1. «Крест следов».

Криминалистическое учение о механизме следообразования является одним из важнейших в общей теории криминалистической науки. Анализ современной криминалистической литературы показывает, что независимо от рода и вида следообразующих и следовоспринимающих объектов с гносеологических позиций есть нечто общее, объединяющее все элементы процесса следообразования и в то же время отражающее динамику процесса, позволяющее проникнуть в сущность следа как объекта познания, выявить его генезис и объяснить его. Этим общим является механизм следообразования. Именно на базе познания механизма следообразования развивается практика исследования следов, безразлично, идет ли речь о следах ног, транспортных средств, огнестрельного оружия, оттисках печатей или следов веществ, ольфакторных следов и других биологических следов человека.

Применение компьютерных средств и систем для совершения различных видов преступлений в соответствии с всеобщим законом отражения привело к формированию нового механизма следообразования, который связан с процессами возникновения, обработки и передачи компьютерной информации. Согласно определению Э. Таненбаума, «цифровой компьютер – это машина, которая может решать задачи, исполняя данные ей команды»[17]. Архитектура компьютера на своих нижних уровнях предусматривает ограниченный набор простых команд. Машинный код – набор инструкций, составленный из таких команд – выполняется непосредственно центральным процессором компьютера и труден для восприятия даже специалистами в области программирования. Еще ниже, в основе архитектуры компьютера, находится цифровой логический уровень, который реализуется в виде набора объектов, называемых вентилями, с использованием которых осуществляются простые логические операции с цифровыми сигналами, которые в компьютерной технике представлены в двоичной системе счисления, т.е. в виде символов 1 и 0. На расположенных выше уровнях архитектуры, содержащих огромное количество вентилей, строится ядро вычислительной системы. Передача цифровых данных, т.е. физическая трансляция битового потока в виде сигналов между конечными компьютерными системами для их дальнейшей обработки осуществляется с помощью распространения электромагнитных волн или

[15] *Ищенко Е.П.* Общий взгляд на криминалистическое следоведение // Вестник Восточно-Сибирского института МВД России. 2019. № 3 (90). С. 146–156.

[16] *Поль К.Д.* Естественно-научная криминалистика / пер. с нем.; под общ. ред. и со вступ. ст. В.Я. Колдина. М., 1985. С. 290, 291.

[17] *Таненбаум Э., Остин Т.* Архитектура компьютера. 6-е изд. СПб., 2013.

оптических импульсов в компьютерных сетях (локальных и глобальной сети Интернет)[18].

Таким образом, при подготовке, совершении и сокрытии преступлений с применением компьютерных средств и систем возникает в процессе возникновения, обработки, хранения и передачи отраженная в цифровой среде криминалистически значимая компьютерная информация о событиях или противоправных действиях. То есть любые действия с использованием компьютерных систем и их сетей оставляют цифровые следы в виде структур компьютерной информации –– в оперативной памяти компьютера, на носителях информации различных типов, на линиях связи и в коммутаторах[19].

Таким образом, *цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи*[20]. Цифровые следы являются следами *материальными*, так как, будучи оставленными в результате определенных событий, отражаются на *материальных объектах*, хотя в некоторых случаях период их существования весьма невелик. По *происхождению цифровые следы являются технологическими*, поскольку формирование данных следов обусловлено спецификой реализации информационных технологий, и для их преобразования в доступную для восприятия форму также используются информационные технологии. По механизму следообразования они могут быть отнесены к *электронным либо электромагнитным* в зависимости от носителя, на котором они отображены – твердотельном либо на магнитных дисках. Но возможны и механические следы – образуются в структуре материала оптического диска под воздействием лазерного луча.

Данную позицию разделяют многие авторы[21], однако, признавая материальную природу и технологическое происхождение цифровых следов, некоторые авторы называют подобные следы электронными или электронно-цифровыми[22]. Но следует поддержать В.А. Мещерякова, справедливо утверждающего, что словосочетание «электронно-цифровой» происходит из комбинации двух прилагательных «цифровой» и «электронный», что подчеркивает не только представление информации в цифровом виде, но и ее обработку, передачу и хранение с использованием электронных технологий. Однако при получающей все большее распространение передаче информации по оптическим каналам связи используются и квантовые технологии[23].

В.А. Мещеряков отмечает далее особенности процесса отражения при образовании цифровых (или, как он их называет, виртуальных[24]) следов, указывая, что этот процесс «в искусственной специально созданной для решения конкретных задач электронно-цифровой среде происходит не напрямую, как в ситуации с традиционными материальными следами в трасологии, когда имеется непосредственное взаимодействие следообразующего и следовоспринимающего объектов, а опосредованно, через целую иерархию формализованных (математических) моделей, используемых для описания реальных физических явлений. <...> Наблюдая цифру/число (по сути, материально зафиксированную информацию/сигнал), но ничего не зная о формализованной модели, положенной в основу электронно-цифрового отражения, мы не сможем понять, как она связана с событием преступления, и, как следствие, она не может рассматриваться в качестве следа. Она так и останется материализованной информацией, закрепленной в виде изменения какого-либо свойства материального объекта – носителя этой информации. <...> Важнейшим моментом при этом является использование формализованных моделей в качестве основы искусственной среды электронно-цифрового отражения. С точки зрения криминалистики важным является тот факт, что один и тот же объект или явление может быть зафиксировано с использованием различных формализованных (математических) моделей»[25].

Полагаем, что цифровые следы не исключение, поскольку помимо традиционных следов-отображений в трасологии существует великое

[18] См.: *Куроуз Д., Росс К.* Компьютерные сети: нисходящий подход. 6-е изд. М., 2016.

[19] См.: Теория информационно-компьютерного обеспечения криминалистической деятельности / под ред. Е.Р. Россинской. М., 2022. С. 44.

[20] См.: *Россинская Е.Р., Рядовский И.А.* Концепция цифровых следов в криминалистике. Аубакировские чтения: материалы Междунар. науч.-практ. конф. (19 февраля 2019 г.). Алматы, 2019. С. 6–9.

[21] См.: *Багмет А.М., Бычков В.В., Скобелин С.Ю., Ильин Н.Н.* Цифровые следы преступлений. М., 2021; *Гаврилин Ю.В., Гаспарян Г.З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: учеб. пособие. М., 2021. С. 54, 55.

[22] См.: Основы теории электронных доказательств / под ред. С.В. Зуева. М., 2019. С. 90.

[23] См.: *Мещеряков В.А.* Теоретические основы механизма следообразования в цифровой криминалистике. М., 2022.

[24] Наше несогласие с термином «виртуальный» было ранее обосновано в монографии «Теория информационно-компьютерного обеспечения криминалистической деятельности» (2022) и в данном случае не является принципиально значимым.

[25] *Мещеряков В.А.* Указ. соч. С. 105, 106.

множество следов, на первый взгляд неочевидно связанных с преступлением, но при исследовании которых для нахождения их связи с событием преступления используются технологии, представляющие собой формализованные модели, причем моделирование может быть не обязательно физическим. Так, в молекулярно-генетических исследованиях, в пожарно-технических или взрывотехнических исследованиях, исследованиях различных веществ и других «один и тот же объект или явление может быть зафиксировано с использованием различных формализованных (математических) моделей». А модели являются гносеологическим отражением, как указывал В.А. Штофф, «постольку, поскольку условием их формирования, построения и использования в процессе познания являются либо физическое подобие, либо аналогия, либо изоморфизм... С фактической (технической, логической, математической стороны) любая модель представляет собой по меньшей мере образ объекта»[26].

К тому же компьютерное моделирование, например 3D-сканирование, уже активно используется в криминалистике при собирании традиционных следов отображений[27], в классической трасологии для лучшего воспроизведения признаков следообразующего объекта[28] и пр.

Обобщая вышеизложенное, заключаем, что предложенный в середине прошлого века К.Д. Полем для наглядного отражения взаимосвязи между местом происшествия, потерпевшим, орудием преступления и преступником принцип перекрестного переноса следов, схематически выраженный в «кресте следов», должен претерпеть изменения, которые связаны с особенностями механизма следообразования. «Крест следов» был отражением механизма следообразования исключительно в трасологии, когда большинство криминалистов не видели еще различий между дефинициями «следоведение» и «трасология». Г.Л. Грановский, Б.И. Шевченко и ряд других авторов утверждали, что объектами следоведения являются только следы-отображения[29]. Но при этом Г.Л. Грановский дал характеристику «видам энергии или воздействий, в результате которых образуется след», обозначив эти воздействия как физическое, химическое и биологическое. Хотя он рассматривал только чисто внешние проявления этого воздействия на следовоспринимающий объект[30], уже обозначил косвенно иные механизмы следообразования, поскольку для перехода от внешних проявлений к внутренним изменениям надо сделать всего несколько шагов. Позднее И.Ф. Крылов пришел к выводу, что «ограничение содержания учения о следах лишь следами-отпечатками может повредить практике» и что учение о следах «должно включать в себя как учение собственно о следах (отображениях), так и учение об изменениях, проявляющихся на месте преступления, на жертве или на самом преступнике в результате воздействия последнего»[31], т.е. усматривал различие между объектами следоведения и трасологии.

Полагаем, что в современном следоведении с учетом новых криминалистических технологий «крест следов» должен выглядеть так, как отражено на *рис. 2.*

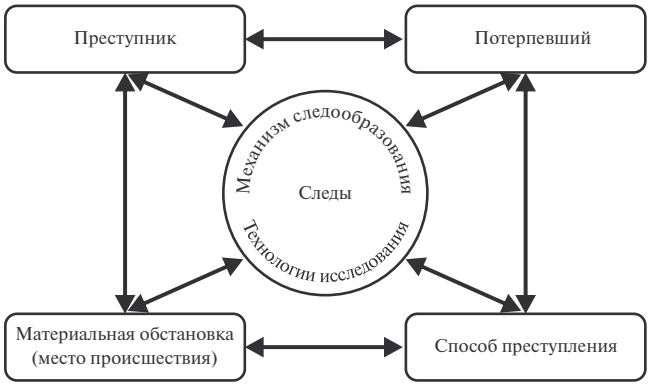

Рис. 2.

На наш взгляд, цифровые следы вписываются в схему «креста следов», поскольку таким же образом, как и остальные разновидности следов, связывают субъект со средством и местом совершения преступного посягательства на конкретный предмет, следовательно, цифровые следы могут содержать информацию обо всех элементах «креста следов».

Другим весьма актуальным направлением развития общей теории криминалистики является современная модернизация учения о способе преступления, который служит одним из важнейших

[26] *Штофф В.А.* Моделирование и философия. М. – Л., 1966. С. 148.

[27] См.: *Севастьянов П.В., Полов В.И., Томчик С.В. и др.* Использование цифровых технологий в технико-криминалистическом обеспечении осмотров мест происшествий: практические рекомендации / П.В. Севастьянов, В.И. Полов, С.В. Томчик [и др.]. М., 2022. С. 45.

[28] См.: *Майлис Н.П.* Цифровая трасология: современное состояние и пути решения проблем // Роль права в обеспечении благополучия человека: сб. докладов XXII Междунар. науч.-практ. конф.: в 5 ч. М., 2022. Ч. 4. С. 490–494.

[29] См.: *Грановский Г.Л.* Основы трасологии. М., 1974. С. 7; *Шевченко Б.И.* Теоретические основы трасологической идентификации в криминалистике. М., 1975. С. 11, 12.

[30] См.: *Грановский Г.Л.* Указ. соч. С. 17.

[31] *Крылов И.Ф.* Криминалистическое учение о следах. Л., 1976. С. 51.

звеньев механизма преступления[32]. Рассмотрим далее *модернизацию и*, как. Заметим, что, согласно классическому определению, криминалистика – это наука о закономерностях механизма преступления[33]. Касаясь этого вопроса, Г.Г. Зуйков писал: «Криминалистика изучает способ совершения преступления, по существу, как содержательное явление действительности, и на основе познания закономерностей его формирования, причин и форм повторяемости разрабатывает средства, приемы и методы обнаружения, собирания, исследования и оценки судебных доказательств»[34]. Способ преступления, по классическому определению Г.Г. Зуйкова, «представляет собой систему объединенных единым замыслом действий преступника (преступников) по подготовке, совершению и сокрытию преступления, детерминированных объективными и субъективными факторами, действий, сопряженных с использованием соответствующих орудий и средств»[35]. В зависимости от этого способы преступления делят на полноструктурные и неполноструктурные. Полноструктурный способ включает действия, относящиеся ко всем его элементам: подготовке, совершению и сокрытию. В тех случаях, когда преступление совершается без предварительной подготовки или когда субъект преступления не планирует действий по его сокрытию, налицо неполноструктурный способ совершения преступления[36]. При этом способ сокрытия преступления может быть не связан со способом совершения и осуществляться иными лицами.

Криминальные структуры в полной мере приняли на вооружение современные цифровые технологии для совершения «высокотехнологичных» преступлений, новых способов совершения «традиционных» преступлений, создания систем конспирации и скрытой связи, для оказания активного противодействия правосудию[37]. Еще в конце XX в. с началом широкого распространения компьютерных средств в социуме нами было предложено именовать «компьютерными преступлениями» преступления, совершаемые с использованием компьютерных средств и систем[38]. Причем дефиниция «компьютерное преступление» должна употребляться не в уголовно-правовом, а в криминалистическом аспекте, поскольку связана не с квалификацией, а именно со способом преступления и, соответственно, с методикой его раскрытия и расследования[39]. Компьютерные преступления имеют общую родовую криминалистическую характеристику[40], одним из основных элементов которой является способ преступления.

В криминалистике формирование частных криминалистических методик осуществляется в основном по видам преступлений. Однако существуют и другие основания для обобщения методик: по субъектам преступлений; по времени совершения преступлений; по месту совершения преступлений; по личности потерпевшего.

Предпринятый нами анализ способов компьютерных преступлений[41] показал, что они всегда являются полноструктурными, причем обычно комплекс мер, направленных на сокрытие следов преступления, предшествует покушению на его совершение. Но главное – одним и тем же способом, с использованием одних и тех же технологий могут совершаться как преступления в сфере компьютерной информации, так и другие виды компьютерных преступлений (мошенничества, кражи, вымогательства, создание групп смерти, организация массовых беспорядков и террористических актов, незаконный оборот наркотических средств, преступления в банковской сфере, незаконная организация азартных игр и пр.).

Например, одним из способов обеспечения анонимности действий в сети Интернет является использование цепочки прокси-серверов. VPN-технологии реализуют шифрование сетевого трафика между пользовательским компьютером и VPN-прокси-сервером – шлюзом выхода в Сеть и, таким образом, маскируется реальный IP-адрес пользователя. Для достижения более высокого уровня конспирации у провайдеров хостинговых услуг в любой стране преступниками могут быть арендованы вычислительные мощности, которые они настраивают на свои VPN-серверы или виртуальные машины.

---

[32] См.: *Белкин Р.С.* Курс криминалистики. 3-е изд., доп. М., 2001. С. 68.

[33] См.: *Белкин Р.С.* Криминалистика: проблемы, тенденции, перспективы, общие и частные теории. М., 1987. С. 26.

[34] *Зуйков Г.Г.* Установление способа совершения преступления. М., 1970. С. 11, 12.

[35] *Зуйков Г.Г.* Основы криминалистического учения о способе совершения и сокрытия преступления. Гл. 3 // Криминалистика: учеб. для юрид. вузов МВД СССР / под ред. Р.С. Белкина, В.П. Лаврова, И.М. Лузгина. М., 1987. Т. 1. С. 52.

[36] Там же.

[37] См.: *Савенков А.Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности. С. 5–18.

[38] См.: Криминалистика: учеб. для вузов / под ред. Р.С. Белкина. М., 1999. С. 948.

[39] См.: там же.

[40] См.: *Россинская Е.Р.* Криминалистика: учеб. для вузов. М., 2016. С. 440–442; *Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р.* Указ. соч. С. 903–905.

[41] *Россинская Е.Р., Рядовский И.А.* Современные способы компьютерных преступлений и закономерности их реализации // Lex russica. 2019. № 3 (148). С. 87–99.

Несанкционированный доступ к компьютерным средствам и сетям, на котором основано большинство способов компьютерных преступлений, осуществляется с помощью вредоносных программ, фактически являющихся орудиями преступлений: программы-вирусы, программы-черви и троянские программы. Большинство вредоносных программ с использованием модульной архитектуры сочетает набор видов деятельности, предоставляющий преступникам широкие возможности манипулирования информацией и поражающих даже облачные ресурсы. Причем возможно также внедрение вредоносного кода в распространяемое легальное программное обеспечение или распространение вредоносных программ в локальных сетях при применении легальных программных средств.

Вернемся теперь к проблемам криминалистической характеристики видов преступлений, поскольку она одна из главных составляющих любой криминалистической методики. Эта дефиниция в криминалистической литературе – объект постоянных дискуссий. Высказываются аргументы как за, так и против нее. Р.С. Белкин указывал, что «криминалистическая характеристика приобретает практическое значение лишь в тех случаях, когда между ее составляющими *установлены корреляционные связи* и зависимости, носящие закономерный характер». А пока «криминалистическая характеристика преступления, не оправдав возлагавшихся на нее надежд и ученых и практиков, изжила себя, и из реальности, которой она представлялась все эти годы, превратилась в иллюзию, в криминалистический фантом»[42].

Криминалистическая характеристика вида преступления в литературе рассматривается многими учеными как информационная модель преступления[43]. Е.П. Ищенко отмечал, что «под типовой информационной моделью понимается информационная система, построенная на основе статистической обработки репрезентативной выборки уголовных дел определенной категории, отражающая закономерные связи между элементами события преступления, используемая для построения типовых версий и формирования методики расследования данного вида преступлений»[44]. Однако в то время реализовать концепцию автоматизированной статистической обработки уголовных дел не представлялось возможным. В условиях современных тенденций перехода от заполняемых на компьютере бланков процессуальных документов к полноценному электронному уголовному делу[45] появляется реальная возможность формирования типовых информационных моделей по результатам выборки и обобщения больших массивов криминалистически значимой информации с использованием технологии больших данных (Big Data). Базируясь на этом подходе, А.А. Бессонов выступил с предложением: «создавать цифровые модели, максимально адаптированные к использованию в цифровой среде.., по сути, речь идет о цифровизации типовых криминалистических характеристик преступлений»[46].

Но, как уже указывалось выше, подготовка, совершение и сокрытие различных видов компьютерных преступлений может осуществляться одними и теми же способами. Поэтому объединение информационных моделей по видам преступлений не является результативным для компьютерных преступлений, необходимо изменить подход к отбору и систематизации криминалистически значимых признаков преступлений.

Нами была сформулирована концепция построения информационно-компьютерных криминалистических моделей компьютерных преступлений на базе теории информационно-компьютерного обеспечения криминалистической деятельности[47]. За основу был выбран не вид преступления, а *корреляционные связи* между комбинациями IT-технологий, применяемых для осуществления компьютерных преступлений, следовой картиной в виде цифровых следов и компетенциями в информационных компьютерных технологиях преступника и потерпевшей стороны.

Информационно-компьютерные модели группируются по сложности способов реализации преступных деяний, включая используемые IT-технологии и корреляции с этими способами уровней компетенции преступника/преступников либо

---

[42] *Белкин Р.С.* Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. С. 220–224.

[43] См.: *Колдин В.Я., Ищенко Е.П.* Типовая информационная модель преступления как основа методики расследования // Правоведение. 2006. № 6 (269). С. 128–144; *Ковалев С.А., Вехов В.Б.* Основы компьютерного моделирования при расследовании преступлений в сфере компьютерной информации. М., 2015. С. 32–43.

[44] *Ищенко Е.П.* Как наполнить фантом криминалистической характеристики преступлений реальным содержанием // Информационный бюллетень № 17 по материалам Криминалистических чтений «Научная состоятельность криминалистической характеристики преступлений». М., 2002. С. 8–14.

[45] См.: Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий / под ред. Л.Н. Масленниковой. М., 2024. С. 250–253.

[46] *Бессонов А.А.* Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13). С. 58–61.

[47] См.: *Россинская Е.Р., Семикаленова А.И.* Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа») // Вестник Томского гос. ун-та. Право. 2022. № 42. С. 68–80.

преступного сообщества, предметами посягательства. Существуют также корреляционные связи между способом компьютерного преступления и уровнем IT-компетентности потерпевшего, например начинающий пользователь, квалифицированный пользователь, специалист в области IT-технологий.

Проиллюстрируем это примерами. Один из основных способов несанкционированного доступа к компьютерным системам – это фишинговые письма с вредоносными вложениями или ссылками. При открытии вложения загружается и устанавливается троянская программа[48], а при переходе по ссылке пользователь попадает на сайт с вредоносными программами[49], которые находят уязвимости в системе и загружают вредоносное ПО. Пользователям постоянно советуют не открывать вложения и не переходить по неизвестным ссылкам в электронных письмах. Использование подобных способов позволяет оценить уровень компетенции как злоумышленника, так и жертвы.

Значительно сложнее способы, где имеется модульная архитектура. Информация о компьютерной системе собирается главным модулем пользователя и направляется на управляющий сервер, который загружает на дополнительные модули, используемые для совершения преступного деяния. Таким образом могут быть атакованы как компьютеры физических лиц, так и крупные корпоративные сети, например для хищения денежных средств либо конфиденциальной информации[50]. Для подготовки, совершения и сокрытия таких преступлений нужна группа или сообщество квалифицированных IT-специалистов. Потерпевшая сторона – это обычно опытные пользователи или системные администраторы.

* * *

В заключение заметим, что развитие общей теории криминалистики на этапе научно-технической революции обеспечивает системный комплексный подход к совершенствованию криминалистической техники, тактики и методики расследования преступлений.

[48] См.: *Bert Rankin*. How Malware Works – Malicious Strategies and Tactics. URL: https://www.lastline.com/blog/how-malware-works-malicious-strategies-and-tactics (дата обращения: 02.11.2021).

[49] См.: *Custer B.H.M., Pool R.L.D., Cornelisse R.* Banking malware and the laundering of its profits // European Journal of Criminology. 2019. No. 16 (6). Pp. 728–745.

[50] См.: *Левцов В.* Анатомия таргетированной атаки. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 05.11.2021).

СПИСОК ЛИТЕРАТУРЫ

1. *Аверьянова Т.В., Белкин Р.С., Корухов Ю.Г., Россинская Е.Р.* Криминалистика. 4-е изд. перераб. и доп. М., 2013. С. 36, 903–905.
2. *Багмет А.М., Бычков В.В., Скобелин С.Ю., Ильин Н.Н.* Цифровые следы преступлений. М., 2021.
3. *Белкин Р.С.* Криминалистика: проблемы, тенденции, перспективы, общие и частные теории. М., 1987. С. 26.
4. *Белкин Р.С.* Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. М., 2001. С. 220–224.
5. *Белкин Р.С.* Курс криминалистики. 3-е изд., доп. М., 2001. С. 68.
6. *Бессонов А.А.* Цифровая криминалистическая модель преступления как основа противодействия киберпреступности // Академическая мысль. 2020. № 4 (13). С. 58–61.
7. *Вехов В.Б.* Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики: сб. тр. участников Междунар. науч.-практ. конф. Ростов н/Д., 2017. С. 40–46.
8. *Гаврилин Ю.В., Гаспарян Г.З.* Расследование хищений денежных средств, совершенных с использованием информационных банковских технологий: учеб. пособие. М., 2021. С. 54, 55.
9. *Голубятников С.П.* Экономическая криминалистика: фантом или реальность // Вестник Нижегородской академии МВД России. 2017. № 4 (40). С. 118–121.
10. *Грановский Г.Л.* Основы трасологии. М., 1974. С. 7, 17.
11. *Грачев М.А., Грачев А.М.* Современные проблемы лингвокриминалистики как науки // Вестник Череповецкого гос. ун-та. 2015. № 1. С. 26–29.
12. *Зуйков Г.Г.* Основы криминалистического учения о способе совершения и сокрытия преступления. Гл. 3 // Криминалистика: учеб. для юрид. вузов МВД СССР / под ред. Р.С. Белкина, В.П. Лаврова, И.М. Лузгина. М., 1987. Т. 1. С. 52.
13. *Зуйков Г.Г.* Установление способа совершения преступления. М., 1970. С. 11, 12.
14. *Ищенко Е.П.* Как наполнить фантом криминалистической характеристики преступлений реальным содержанием // Информационный бюллетень № 17 по материалам Криминалистических чтений «Научная состоятельность криминалистической характеристики преступлений». М., 2002. С. 8–14.
15. *Ищенко Е.П.* Криминалистика: учеб. 3-е изд., испр. и доп. М., 2011. С. 4.
16. *Ищенко Е.П.* Общий взгляд на криминалистическое следоведение // Вестник Восточно-Сибирского института МВД России. 2019. № 3 (90). С. 146–156.
17. *Ковалев С.А., Вехов В.Б.* Основы компьютерного моделирования при расследовании преступлений в сфере компьютерной информации. М., 2015. С. 32–43.
18. *Колдин В.Я., Ищенко Е.П.* Типовая информационная модель преступления как основа методики расследования // Правоведение. 2006. № 6 (269). С. 128–144.

19. Концепция построения уголовного судопроизводства, обеспечивающего доступ к правосудию в условиях развития цифровых технологий / под ред. Л.Н. Масленниковой. М., 2024. С. 250–253.

20. Криминалистика: учеб. / Л.Я. Драпкин, В.Н. Карагодин. 2-е изд., перераб. и доп. М., 2011. С. 10.

21. Криминалистика: учеб. / под ред. Д.И. Сулейманова. 2-е изд., перераб. и доп. Баку, 2008. С. 62.

22. Криминалистика: учеб. для вузов / под ред. Р.С. Белкина. М., 1999. С. 948.

23. *Крылов И.Ф.* Криминалистическое учение о следах. Л., 1976. С. 51.

24. *Куроуз Д., Росс К.* Компьютерные сети: нисходящий подход. 6-е изд. М., 2016.

25. *Левцов В.* Анатомия таргетированной атаки. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (дата обращения: 05.11.2021).

26. *Майлис Н.П.* Трасология и трасологическая экспертиза: курс лекций М., 2015. С. 12.

27. *Майлис Н.П.* Цифровая трасология: современное состояние и пути решения проблем // Роль права в обеспечении благополучия человека: сб. докладов XXII Междунар. науч.-практ. конф.: в 5 ч. М., 2022. Ч. 4. С. 490–494.

28. *Мещеряков В.А.* Теоретические основы механизма следообразования в цифровой криминалистике. М., 2022. С. 105, 106.

29. Основы теории электронных доказательств / под ред. С.В. Зуева. М., 2019. С. 90.

30. *Поль К.Д.* Естественно-научная криминалистика / пер. с нем.; под общ. ред. и со вступ. ст. В.Я. Колдина. М., 1985. С. 290, 291.

31. *Порубов Н.И., Грамович Г.И., Порубов А.Н.* Криминалистика: учеб. пособие / под ред. Н.И. Порубова. Минск, 2007. С. 6.

32. *Россинская Е.Р.* Криминалистика: учеб. для вузов. М., 2016. С. 440–442.

33. *Россинская Е.Р.* Ревизия определения предмета криминалистики: за и против // Библиотека криминалиста. 2012. № 4. С. 328–335.

34. *Россинская Е.Р.* Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности // Вестник Восточно-Сибирского института МВД России. 2019. № 2 (89). С. 193–202.

35. *Россинская Е.Р., Гинзбург А.Я., Оганов Н.И., Бегалиев Е.Н.* Криминалистика негіздеі. Алматы, 2007. С. 18 (на казах. яз.).

36. *Россинская Е.Р., Рядовский И.А.* Концепция цифровых следов в криминалистике. Аубакировские чтения: материалы Междунар. науч.-практ. конф. (19 февраля 2019 г.). Алматы, 2019. С. 6–9.

37. *Россинская Е.Р., Рядовский И.А.* Современные способы компьютерных преступлений и закономерности их реализации // Lex russica. 2019. № 3 (148). С. 87–99.

38. *Россинская Е.Р., Семикаленова А.И.* Информационно-компьютерные криминалистические модели компьютерных преступлений как элементы криминалистических методик (на примере «кибершантажа») // Вестник Томского гос. ун-та. Право. 2022. № 42. С. 68–80.

39. *Россинская Е.Р., Семикаленова А.И.* Основы учения о криминалистическом исследовании компьютерных средств и систем как часть теории информационно-компьютерного обеспечения криминалистической деятельности // Вестник СПбУ. Право. 2020. Т. 11. Вып. 3. С. 745–759.

40. *Савенков А.Н.* Противодействие киберпреступности в финансово-кредитной сфере как вектор обеспечения глобальной безопасности // Государство и право. 2017. № 10. С. 5–18.

41. *Савенков А.Н., Россинская Е.Р.* Вектор инновационного развития криминалистической науки в условиях глобальной цифровизации // Государство и право. 2023. № 5. С. 100–110.

42. *Севастьянов П.В., Полов В.И., Томчик С.В. и др.* Использование цифровых технологий в технико-криминалистическом обеспечении осмотров мест происшествий: практические рекомендации. М., 2022. С. 45.

43. *Таненбаум Э., Остин Т.* Архитектура компьютера. 6-е изд. СПб., 2013.

44. Теория информационно-компьютерного обеспечения криминалистической деятельности / под ред. Е.Р. Россинской. М., 2022. С. 44.

45. *Федосюткин Б.А.* Медицинская криминалистика: руководство. Ростов н/Д., 2006. С. 34, 35.

46. Цифровая криминалистика: учеб. для вузов / под ред. В.Б. Вехова, С.В. Зуева. 2-е изд., перераб. и доп. М., 2024. С. 16–18.

47. *Шевченко Б.И.* Теоретические основы трасологической идентификации в криминалистике. М., 1975. С. 11, 12.

48. *Штофф В.А.* Моделирование и философия. М. – Л., 1966. С. 148.

49. *Эксархопуло А.А.* Криминалистика: учеб. СПб., 2009. С. 13, 14.

50. *Bert Rankin.* How Malware Works – Malicious Strategies and Tactics. URL: https://www.lastline.com/blog/how-malware-works-malicious-strategies-and-tactics (дата обращения: 02.11.2021).

51. *Custer B.H.M., Pool R.L.D., Cornelisse R.* Banking malware and the laundering of its profits // European Journal of Criminology. 2019. No. 16 (6). Pp. 728–745.

REFERENCES

1. *Averyanova T.V., Belkin R.S., Korukhov Yu. G., Rossinskaya E.R.* Criminalistics. 4th ed. rev. and add. M., 2013. Pp. 36, 903–905 (in Russ.).

2. *Bagmet A.M., Bychkov V.V., Skobelin S. Yu., Ilyin N.N.* Digital blind crimes. M., 2021 (in Russ.).

3. *Belkin R.S.* Criminalistics: problems, trends, prospects, general and particular theories. M., 1987. P. 26 (in Russ.).

4. *Belkin R.S.* Criminalistics: problems of today. Topical issues of Russian criminology. M., 2001. Pp. 220–224 (in Russ.).

5. *Belkin R.S.* Course of criminology. 3rd ed., supplement. M., 2001. P. 68 (in Russ.).

6. *Bessonov A.A.* Digital criminalistic crime model as a basis for countering cybercrime // Academic thought. 2020. No. 4 (13). Pp. 58–61 (in Russ.).

7. *Vekhov V.B.* Electronic criminalistics: concept and system. // Criminalistics: topical issues of theory and practice: collection of tr. participants of the International Scientific and Practical Conference. Rostov-on-Don, 2017. Pp. 40–46 (in Russ.).

8. *Gavrilin Yu. V., Gasparyan G.Z.* Investigation of embezzlement of funds committed using information banking technologies: textbook. M., 2021. Pp. 54, 55 (in Russ.).

9. *Golubyatnikov S.P.* Economic criminalistics: a phantom or reality // Herald of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. 2017. No. 4 (40). Pp. 118–121 (in Russ.).

10. *Granovsky G.L.* Fundamentals of tracology. M., 1974. Pp. 7, 17 (in Russ.).

11. *Grachev M.A., Grachev A.M.* Modern problems of linguocriminalism as a science // Herald of Cherepovets State University. 2015. No. 1. Pp. 26–29 (in Russ.).

12. *Zuikov G.G.* Fundamentals of criminalistic teaching on the method of committing and concealing a crime. Chapter 3 // Criminalistics: textbook for law universities of the Ministry of Internal Affairs of the USSR / ed. by R.S. Belkin, V.P. Lavrov, I.M. Luzgin. M., 1987. Vol. 1. P. 52 (in Russ.).

13. *Zuikov G.G.* Establishing the method of committing a crime. M., 1970. Pp. 11, 12 (in Russ.).

14. *Ishchenko E.P.* How to fill the phantom of the criminalistic characteristics of crimes with real content // Newsletter No. 17 based on the materials of Criminalistic readings "Scientific consistency of the criminalistic characteristics of crimes". M., 2002. Pp. 8–14 (in Russ.).

15. *Ishchenko E.P.* Criminalistics: textbook. 3rd ed., rev. and add. M., 2011. P. 4 (in Russ.).

16. *Ishchenko E.P.* A general view on forensic investigation // Herald of the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. No. 3 (90). Pp. 146–156 (in Russ.).

17. *Kovalev S.A., Vekhov V.B.* Fundamentals of computer modeling in the investigation of crimes in the field of computer information. M., 2015. Pp. 32–43 (in Russ.).

18. *Koldin V. Ya., Ishchenko E.P.* Typical information model of crime as the basis of investigation methodology // Jurisprudence. 2006. No. 6 (269). Pp. 128–144 (in Russ.).

19. The concept of building criminal proceedings providing access to justice in the context of the development of digital technologies / ed. by L.N. Maslennikova. M., 2024. Pp. 250–253 (in Russ.).

20. Criminalistics: studies / L. Ya. Drapkin, V.N. Karagodin. 2nd ed., reprint and add. M., 2011. P. 10 (in Russ.).

21. Criminalistics: textbook / ed. by D.I. Suleymanov. 2nd ed., rev. and add. Baku, 2008. P. 62 (in Russ.).

22. Criminalistics: textbook for universities / ed. by R.S. Belkin. M., 1999. P. 948 (in Russ.).

23. *Krylov I.F.* Criminalistic doctrine of traces. L., 1976. P. 51 (in Russ.).

24. *Kurouz D., Ross K.* Computer networks: a top-down approach. 6th ed. M., 2016 (in Russ.).

25. *Levtsov V.* Anatomy of a targeted attack. URL: https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/ (accessed: 05.11.2021) (in Russ.).

26. *Mailis N.P.* Tracology and tracological expertise: a course of lectures. M., 2015. P. 12 (in Russ.).

27. *Mailis N.P.* Digital tracology: the current state and ways to solve problems // The role of law in ensuring human well-being: collection of reports XXII International Scientific and Practical Conference: in 5 parts. M., 2022. Part 4. Pp. 490–494 (in Russ.).

28. *Meshcheryakov V.A.* Theoretical foundations the mechanism of trace formation in digital criminalistics. M., 2022. Pp. 105, 106 (in Russ.).

29. Fundamentals of the theory of electronic evidence / ed. by S.V. Zuev. M., 2019. P. 90 (in Russ.).

30. *Paul K.D.* Natural Science criminalistics / transl. from German; under the general ed. and with an introduction by V. Ya. Koldin. M., 1985. Pp. 290, 291 (in Russ.).

31. *Porubov N.I., Gramovich G.I., Porubov A.N.* Criminalistics: textbook / ed. by N.I. Porubov. Minsk, 2007. P. 6 (in Russ.).

32. *Rossinskaya E.R.* Criminalistics: textbook for universities. M., 2016. Pp. 440–442 (in Russ.).

33. *Rossinskaya E.R.* Revision of the definition of the subject of criminalistics: pros and cons // Library of criminalist. 2012. No. 4. Pp. 328–335 (in Russ.).

34. *Rossinskaya E.R.* Theory of information and computer support for forensic activities: concept, system, basic patterns // Heraldof the East Siberian Institute of the Ministry of Internal Affairs of Russia. 2019. No. 2 (89). Pp. 193–202 (in Russ.).

35. *Rossinskaya E.R., Ginzburg A. Ya., Oganov N.I., Begaliev E.N.* Criminalistics of negizdei. Almaty, 2007. P. 18 (in Kazakh.).

36. *Rossinskaya E.R., Ryadovsky I.A.* The concept of digital traces in criminology. Aubakirov readings: materials of the International Scientific and Practical Conference (February 19, 2019). Almaty, 2019. Pp. 6–9 (in Russ.).

37. *Rossinskaya E.R., Ryadovsky I.A.* Modern methods of computer crimes and patterns of their implementation // Lex russica. 2019. No. 3 (148). Pp. 87–99 (in Russ.).

38. *Rossinskaya E.R., Semikalenova A.I.* Information and computer criminalistic models of computer crimes as elements of criminalistic techniques (on the example of "cybershantage") // Herald of the Tomsk State University. Law. 2022. No. 42. Pp. 68–80 (in Russ.).

39. *Rossinskaya E.R., Semikalenova A.I.* Fundamentals of the doctrine of forensic research of computer tools and systems as part of the theory of information and computer support for forensic activities // Herald of the SPbU. Law. 2020. Vol. 11. Iss. 3. Pp. 745–759 (in Russ.).

40. *Savenkov A.N.* Countering cybercrime in the financial and credit sphere as a vector of ensuring global security // State and Law. 2017. No. 10. Pp. 5–18 (in Russ.).

41. *Savenkov A.N., Rossinskaya E.R.* Vector of innovative development of forensic science in the context of global digitalization // State and Law. 2023. No. 5. Pp. 100–110 (in Russ.).

42. *Sevastyanov P.V., Polov V.I., Tomchik S.V. et al.* The use of digital technologies in the technical and forensic support of inspections of accident sites: practical recommendations. M., 2022. P. 45 (in Russ.).

43. *Tanenbaum E., Ostin T.* Computer architecture. 6th ed. SPb., 2013 (in Russ.).

44. Theory of information and computer support for forensic activities / ed. by E.R. Rossinskaya. M., 2022. P. 44 (in Russ.).

45. *Fedosyutkin B.A.* Medical criminalistics: a guide. Rostov-on-Don, 2006. Pp. 34, 35 (in Russ.).

46. Digital criminalistics: textbook for universities / ed. by V.B. Vekhov, S.V. Zuev. 2nd ed., rev. and add. M., 2024. Pp. 16–18 (in Russ.).

47. *Shevchenko B.I.* Theoretical foundations of tracological identification in criminology. M., 1975. Pp. 11, 12 (in Russ.).

48. *Shtoff V.A.* Modeling and philosophy. M. – L., 1966. P. 148 (in Russ.).

49. *Exarchopulo A.A.* Criminalistics: textbook. SPb., 2009. Pp. 13, 14 (in Russ.).

50. *Bert Rankin.* How Malware Works – Malicious Strategies and Tactics. URL: https://www.lastline.com/blog/how-malware-works-malicious-strategies-and-tactics (accessed: 02.11.2021).

51. *Custer B.H.M., Pool R.L.D., Cornelisse R.* Banking malware and the laundering of its profits // European Journal of Criminology. 2019. No. 16 (6). Pp. 728–745.

Сведения об авторах

САВЕНКОВ Александр Николаевич –
член-корреспондент РАН,
доктор юридических наук, профессор,
заслуженный юрист РФ,
директор Института государства и права
Российской академии наук;
119019 г. Москва, ул. Знаменка, д. 10

РОССИНСКАЯ Елена Рафаиловна –
доктор юридических наук, профессор,
заслуженный деятель науки РФ,
почетный работник высшего
профессионального
образования РФ,
заведующая кафедрой судебных экспертиз,
научный руководитель
Института судебных экспертиз
Московского государственного юридического
университета им. О.Е. Кутафина (МГЮА);
125993 г. Москва, ул. Садовая-Кудринская, д. 9

Authors' information

SAVENKOV Alexander N. –
Corresponding Member of the Russian Academy
of Sciences, Doctor of Law, Professor,
Honored Lawyer of the Russian Federation,
Director of the Institute of State and Law
of the Russian Academy of Sciences;
10 Znamenka str., 119019 Moscow, Russia

ROSSINSKAYA Elena R. –
Doctor of Law, Professor,
Honored Scientist of the Russian Federation,
Honorary Worker of Higher Professional Education
of the Russian Federation, Head of the Forensic
Expertise Department, Scientific Supervisor
of the Forensic Expertise Institute at Kutafin
Moscow State Law University (MSAL);
9 Sadovaya-Kudrinskaya str.,
125993 Moscow, Russia