УДК 343.9

З. И. Харисова

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Уфимский университет науки и технологий, Уфа, Россия
Поступила в редакцию 05.05.2025 г.
Принята к публикации 15.05.2025 г.
doi: 10.5922/vestnikhum-2025-2-2

Для цитирования: *Харисова З. И.* Криминалистическая характеристика создания, использования и распространения вредоносных компьютерных программ // Вестник Балтийского федерального университета им. И. Канта. Сер.: Гуманитарные и общественные науки. 2025. №2. С. 20—33. doi: 10.5922/vestnikhum-2025-2-2.

Вредоносное программное обеспечение и вирусные фишинговые атаки уже несколько лет подряд остаются одним из самых действенных инструментов проникновения в информационную инфраструктуру. В подавляющем большинстве эксплуатация вредоносных программ связана с получением доступа к системам, содержащим конфиденциальную информацию, и ее хищением, что является наименее затратным способом доставки и выполнения вредоносного кода на устройстве получателя. Поскольку рост противоправных деяний, связанных с созданием, использованием и распространением вредоносных компьютерных программ, — это значимый фактор самовоспроизводства киберпреступлений, целесообразно рассмотрение возможностей оптимизации процесса их расследования, в частности изучение элементов, входящих в их криминалистическую характеристику. Объектом исследования выступили правоотношения, возникающие при расследовании преступлений в сфере компьютерной информации, связанных с созданием, использованием и распространением вредоносных компьютерных программ, основной целью при этом было раскрытие содержания элементов криминалистической характеристики указанных преступных деяний с учетом современного развития информационных технологий и тенденций эксплуатации вредоносного программного обеспечения. Теоретическую значимость исследования составляет описание криминалистической характеристики рассматриваемых преступлений, которая может послужить основой для формирования их информационной модели (цифровых двойников), что концептуально выступает научной новизной. Прикладное значение типовых криминалистических характеристик преступлений в сфере компьютерной информации — возможность их использования при формировании частных криминалистических методик расследования, создании новых криминалистических учетов на основе баз данных цифровых доказательств, а также разработки специализированного программного обеспечения в виде систем поддержки принятия решений, применяемых, например, при выдвижении следственных версий и планировании расследования.

Ключевые слова: компьютерные преступления, вредоносные программы, криминалистическая характеристика преступлений, цифровая модель преступления, цифровой двойник, цифровая криминалистика, искусственный интеллект

Современное право нацелено на урегулирование вновь появляющихся форм отношений практически всех сфер деятельности человека, где объектами, субъектами, а порой и средствами все чаще выступают высокие технологии, что закономерно формирует новый вид права, именуемый высокотехнологичным и представляющим собой логистичный, наукоемкий и технологичный регулятор общественных отношений, который не только регламентирует вновь возникающие отношения, связанные с высокими технологиями, но и активно использует их в правоприменении [1, с. 742]. Возникновение новых субъектов права, объектов регулирования и высокотехнологичных средств совершения преступлений, в том числе в виде вредоносного программного обеспечения (далее — ПО), в основном вынуждает законодателей принимать меры по разработке нормативных правовых актов, регулирующих новые правоотношения. Однако ключевым аспектом очередного этапа развития права является наличие новых инструментов и технологий, повышающих эффективность функционирования этой отрасли.

Вредоносное ПО все чаще становится инструментом преступников для осуществления несанкционированного доступа к охраняемой законом информации, кражи персональных данных граждан, вымогательства, шпионажа, атак на государственные структуры и пр. В условиях повсеместной цифровизации создание, использование и распространение вредоносного ПО (ст. 273 УК РФ) может нанести значительный ущерб экономической жизни общества, например при внедрении в банковское ПО, а в отдельных случаях причинить вред здоровью различной тяжести, привести к смерти людей, в частности при внедрении в информационные системы персональных данных, эксплуатируемые в медицинских учреждениях и т. п.

Уникальность каждого из применяемых способов и средств совершения преступлений в сфере компьютерной информации, составным элементом которых являются рассматриваемые преступные деяния, определяет индивидуальность в их раскрытии, расследовании, а также в поиске и фиксации доказательств. Определить особенности преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, предоставляя необходимые методы обнаружения, изъятия и анализа электронных доказательств, позволяет область знаний, возникшая на стыке правовых и технических наук [2, с. 6], именуемая в России цифровой криминалистикой, или форензикой (*англ.* computer forensics — наука об исследовании цифровых доказательств [3, с. 11]).

С учетом очевидной необходимости модернизации правовых подходов к урегулированию вновь появляющихся общественных отношений, связанных с инновационными, эволюционными и синергетическими процессами, обусловленными внедрением информационных технологий [4, с. 80], а также в связи с широкой распространенностью в настоящее время рассматриваемых преступных деяний [5, с. 55] актуальной задачей является рассмотрение возможностей оптимизации процесса расследования преступлений, связанных с созданием, исполь-

зованием и распространением вредоносных компьютерных программ, в частности изучение элементов, входящих в их криминалистическую характеристику, а также применение их при использовании современных методов компьютерной криминалистики, реализуемых на основе технологий анализа больших данных и алгоритмов искусственного интеллекта, что позволит следователю (дознавателю) ориентироваться в ситуации нехватки времени либо опыта [6, с. 30].

За последние три десятка лет вопросы целесообразности формирования криминалистических моделей преступлений (цифровых, информационных и пр.), а также компьютерного моделирования их расследования рассматривались довольно часто (Т. С. Волчецкая, В. Е. Корноухов, Е. П. Ищенко, В. Я. Колдин, В. О. Давыдов, В. Б. Вехов, Р. Л. Ахмедишин, А. А. Бессонов, Е. Р. Россинская, А. И. Семикаленова, У. А. Мусаева и др.), однако, являясь фундаментальными в данной области, в большинстве своем они касались общих аспектов моделирования механизма преступных деяний и алгоритмизации процесса расследования, который позволяет повысить профессиональную компетентность субъектов раскрытия и расследования преступлений и показатели антикриминальной деятельности, а также дополнить и внести вклад во все фундаментальные направления современной криминалистической науки [8, с. 640]. При этом вопрос повышения эффективности расследования (в том числе алгоритмизации) преступлений, связанных с созданием, использованием и распространением вредоносных программ на основе криминалистической модели преступления, не рассматривался.

Вредоносное ПО — это форма представления совокупности данных и команд, обеспечивающих функционирование компьютера либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования электронных данных или нейтрализации средств защиты информации [9]. Способом совершения данного преступления является действие, выраженное в виде создания вредоносного ПО, а равно использования или распространение такого ПО либо иной компьютерной информации.

Под созданием вредоносного ПО подразумевается результат деятельности, выразившейся в представлении в объективной форме совокупности данных и команд, предназначенных для функционирования информационно-телекоммуникационной системы либо компьютера с целью уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также с целью нарушения работы информационной системы. Действия, направленные на создание вредоносной программы, не доведенные до конца по причинам, не зависящим от воли виновного, могут быть квалифицированы как покушение на преступление.

Распространение предполагает как возмездную, так и безвозмездную передачу ПО, либо вредоносной информации, либо электронного носителя информации с его содержанием. Использование ПО либо

вредоносной информации имеет место при внедрении ПО в компьютер или информационную систему независимо от того, повлекло ли это последствия, поскольку преступление окончено в момент совершения соответствующих действий.

К числу основных криминалистических категорий как наиболее общих и значимых для науки и практики понятий криминалистики относятся понятия криминалистической характеристики преступления, которая, являясь базовым элементом криминалистической методики, образует систему сведений о типичных криминалистически значимых признаках преступлений и связях между ними [10, с. 8], а также типовой (родовой, групповой, видовой) криминалистической характеристики преступления. Под типовой криминалистической характеристикой преступления понимается научная абстракция, отражающая систему взаимосвязанных и корреляционно зависимых элементов той или иной категории (группы) преступлений и способствующая определению основных направлений в расследовании общественно опасного деяния [11, с. 111].

Криминалистическая характеристика складывается из элементов, в совокупности составляющих систему характерных криминалистических признаков конкретного преступления, на основе которых становится возможным сформировать методику его расследования. По этой причине в свете рассмотрения теоретических основ расследования рассматриваемых преступлений целесообразно выделить элементы их криминалистической характеристики.

На основе исследования материалов уголовных дел по преступлениям, связанным с созданием, использованием и распространением вредоносного ПО, их криминалистическую характеристику предлагается изложить в следующем виде:

— способ совершения преступления (с описанием типичных следов преступления, способов их сокрытия, вероятных мест их нахождения и распространенности (серийности) преступного деяния);

— обстановка (место (среда), время совершения) преступления;

— личность преступника;

— личность потерпевшего и / или предмет посягательства.

Отдельно стоит отметить такой элемент, как серийность преступного деяния, являющийся одним из обязательных реквизитов [12] для указания в статистической карточке преступления, содержание которого, например, может выступить основой для формирования нового криминалистического учета цифровых доказательств, что сонаправлено с одной из основных задач государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий [13].

Переходя к рассмотрению содержания элементов криминалистической характеристики рассматриваемых преступлений, стоит отметить, что основными способами создания вредоносного ПО являются написание исходного кода на языке программирования с использованием вредоносных алгоритмов; модификация легального ПО [14, с. 702]

с внедрением вредоносного функционала в виде бэкдоров (*англ.* backdoor — лазейка); использование специализированных сервисов в виде автоматизированных MaaS-конструкторов (*англ.* malware-as-a-service (MaaS)) — вредоносное ПО, предоставляющееся как услуга, позволяющих создавать программы без глубоких знаний в области информационных технологий; создание новой версии программного проекта с открытым исходным кодом путем форкинга (*англ.* forking — ветвление); создание ПО, которое использует уязвимости в легальных программах для распространения вредоносных функций в виде эксплойта (*англ.* exploit — эксплуатировать)); внедрение буткитов (*англ.* boot — загрузка и kit — набор инструментов) — комплекса вредоносного ПО, которое изменяет сигнатуру исходного кода для уклонения от обнаружения антивирусами; генерация адаптивного вредоносного кода с применением алгоритмов искусственного интеллекта и пр. Ввиду того что непосредственное создание вредоносного ПО требует знаний в области программирования, кибербезопасности и эксплуатации уязвимостей, довольно часто преступники прибегают к приобретению готовых вредоносных продуктов на теневых площадках сети Даркнет.

Среди основных способов использования вредоносного ПО на сегодняшний день можно выделить сбор конфиденциальных данных в целях кибершпионажа; шифрование данных; создание ботнетов для заражения компьютера (например, для организации DDoS-атак, несанкционированного копирования компьютерной информации и пр.); рассылку спама или криптоджекинга (майнинга криптовалют); SQL-инъекции; компрометацию систем безопасности (установка бэкдоров для несанкционированного доступа и пр.); создание ресурсов с использованием вредоносных скриптов; деструктивное воздействие вредоносным ПО на информацию или технические средства (уничтожение данных, вывод из строя информационной инфраструктуры); нейтрализацию средств защиты информации; обход лицензий ПО и антивирусов; воздействие вредоносного ПО на объекты критической информационной инфраструктуры Российской Федерации, распространение ПО с возможностями VPN-прокси-сервера и создания бот-сетей из зараженных ею компьютеров с сокрытием IP-адресов [15, с. 31], сканирование информационной системы, эксплуатацию уязвимостей и пр.

Способы распространения вредоносного ПО зависят от целей преступника и технических возможностей жертвы и могут представлять собой распространение вредоносных ссылок и ПО на веб-ресурсах, в файлообменных пиринговых сетях, торрент-трекерах, сети Блокчейн, а также в электронных узлах и локальных информационно-вычислительных сетях автотранспортных средств [16, с. 17], в виде вложений через мессенджеры, электронную почту и социальные сети; заражение устройств через недоработки в ПО и операционных системах устройств, принадлежащих жертве (например возможно воздействие на уязвимость нулевого дня (*англ.* zero-day) — уязвимость в ПО, против которой еще не разработаны защитные механизмы и не были выпущены обновления безопасности) и т. п.; манипулирование пользователями

с помощью применения методов социальной инженерии с целью побуждения их скачать и запустить вредоносное ПО; взлом протоколов безопасности для загрузки вредоносного кода; заражение носителей информации и IoT-устройств; использование вредоносного ПО для кражи лицензий, учетных данных и пр.

Процессы, возникшие в ходе случайных действий либо стечения обстоятельств, относят к непреднамеренным, например: использование разработчиками легального ПО открытых библиотек и баз данных, содержащих вредоносный код или критические уязвимости; внедрение вредоносного кода в проекты с открытым исходным кодом; создание прототипов автоматизированных программ для тестирования различных сервисов, которые случайно выходят из-под контроля, что довольно часто встречается при генерации кода с использованием искусственного интеллекта и т. п. Кроме того, вредоносные программы могут использоваться непреднамеренно, например пользователем или администратором информационной системы. Так, довольно часто встречается ситуация, когда в отсутствие действенных средств защиты информации пользователи скачивают и запускают на первый взгляд легальное, но зараженное ПО, не подозревая о его вредоносной активности, что часто объясняется использованием нелицензионных версий программ, распространяемых на безвозмездной основе.

Анализ массива уголовных дел позволил выявить основные средства создания, использования и распространения вредоносного ПО. При непосредственном доступе ими могут выступать носители информации, эксплуатируемые с техническими средствами, а при опосредованном доступе — сетевое оборудование, средства доступа в информационные системы (средства вычислительной техники, мобильные средства связи и пр.), различное ПО (например, кейлоггеры (*англ.* key — клавиша и logger — регистрирующее устройство в виде клавиатурного шпиона), руткиты (*англ.* rootkit — набор программных средств, в виде исполняемых файлов, скриптов и пр., обеспечивающих маскировку объектов, управление и сбор данных), трояны (*англ.* trojan — троянская вирусная программа, проникающая в компьютер под видом легального ПО) и пр.), способное к распространению в локальных информационных системах и служащих в целях выполнения какого-либо деструктивного действия (удаление, блокирование или изменение файлов) и пр.

В целом к средствам хранения вредоносного ПО относятся материальные носители: жесткие и оптические диски, USB-накопители, карты памяти и т. п., средством их обработки служит вычислительное устройство (процессор) компьютера. Средства разработки вредоносного ПО могут включать в себя компиляторы и интерпретаторы (языки программирования, используемые для написания ПО); ПО в виде фреймворков для тестирования эксплойтов и бэкдоров; конструкторы вредоносного ПО, в том числе функционирующие на основе искусственного интеллекта, ПО для шифрования и маскировки вредоносного кода.

Средствами использования вредоносного ПО являются, например, управляемые группы зараженных устройств, используемые для DDoS-атак,

спама и криптоджекинга (ботнет-сети), а также инструменты, обеспечивающие полный доступ к зараженному устройству; программы-шифровальщики и вымогатели, используемые для блокировки данных и вымогательства.

К средствам распространения вредоносного ПО преимущественно относятся зараженные компьютеры (носители информации), сети передачи данных, веб-ресурсы и прочие хранилища данных.

Минимизировать риск раскрытия преступником своей личности и источников происхождения вредоносного ПО позволяют следующие методы сокрытия следов: использование анонимных сетей (Tor, I2P, VPN) с целью сокрытия IP-адреса или MAC-идентификатора средства совершения преступления и анонимных (фиктивных) учетных записей для внедрения ПО в информационную систему или в целях обсуждения и дальнейшего его распространения. Для исключения отслеживания банковских операций применяются цифровые фиатные активы; шифрование исходного кода вредоносного ПО, обфускация (запутывание алгоритмов и маскировка вредоносных функций) для затруднения анализа; создание динамически изменяемых версий ПО для обхода детектирования антивирусами; маскировка вредоносного ПО под стандартное легальное ПО, входящее в состав операционной системы.

Для сокрытия следов разработки вредоносного ПО, как правило, используются изолированные виртуальные машины [17, с. 103]. При успешном внедрении вредоносного ПО преступник переходит к мерам по сокрытию своей деятельности в зараженном устройстве. Так, например, осуществляется маскировка вредоносных процессов и сетевой активности в операционной системе, обход или отключение антивирусных систем; манипуляция атрибутами создания, изменения и доступа к файлам (изменение временных меток файлов жертвы); использование самоуничтожаемых вредоносных программ после выполнения задачи; очистка системных логов и следов активности и пр.

Типичными следами создания, использования и распространения вредоносного ПО в общем случае являются следы установленного ПО с признаками вредоносного функционала, изменения в конфигурации операционной системы устройства, журналах подключений к компьютерам или информационным системам, удаленные, модифицированные или блокированные файлы данных и т. п. и материальные следы на компьютерной периферии. К такого рода следам также относятся артефакты в исходном коде ПО (метаданные файлов, идентифицирующих разработчика, дату компиляции, используемые библиотеки, сигнатуры компиляторов и сред разработки, использование типичных функций из открытых репозиториев или подобных, выявляемых ранее атак); IP-адреса и доменные имена серверов управления ПО; параметры задействованных виртуальных машин и обращения к серверам; временные файлы данных, содержащие информацию о запуске вредоносного кода; журналы системных событий; следы использования вредоносного ПО в файловой системе, оперативной памяти, сетевом трафике; следы распространения вредоносного ПО в сети Интернет, в

фишинговых электронных рассылках (структура заголовков, IP-адреса отправителей, SMTP-сервера и пр.), сообщениях мессенджеров (фишинговые ссылки), вредоносных вложениях (документы с макросами, исполняемые файлы и пр.)) в компрометированных веб-сайтах [18, с. 28] и облачных сервисах, торрент-трекерах и т. п.

Таким образом, основными следообразующими и следовоспринимающими объектами при создании, использовании и распространении вредоносного ПО могут выступать системное и прикладное ПО; поименованные области записей на носителях информации; электронные файлы; базы данных; идентификаторы в сети передачи данных (IP-адрес устройства или MAC-адрес его сетевой карты, IMEI-коды мобильных устройств, DNS-адреса; реестры операционных систем; сетевой трафик; цифровые финансовые активы и электронные кошельки; IMS-, SMS- и MMS-сообщения и т. п.

Вероятными местами расположения типичных следов создания, использования и распространения вредоносного ПО в цифровом виде являются носители информации различных устройств, облачные хранилища данных, в том числе файлы и каталоги хранения данных, файлы конфигурации программ удаленного доступа и пр.

Распространенность преступного деяния выражается в установлении факта схожести преступного деяния, например на основе полученных сведений об использовании в преступной схеме способа совершения преступления, тиражирования вредоносного ПО. Так, идентифицирующими признаками схожести по рассматриваемым деяниям могут выступить отдельные техники и тактики, которые обнаруживаются с помощью наборов матриц, представляющих собой основанные на реально существующих наблюдениях базы данных инцидентов безопасности [19], идентичные контрольные суммы ПО, а также реквизиты в виде MAC-идентификаторов или IP-адресов устройств, IMEI-кодов задействованных при распространении вредоносного ПО мобильных средств связи; электронных адресов и т. п. Стоит также отметить, что с учетом развития технологий возможно создание и распространение вредоносного ПО с применением технологий искусственного интеллекта с возможностью автоматической адаптации к системам защиты; методов машинного обучения для поиска уязвимостей в легальном ПО; генерации кода для обхода антивирусных сигнатур; интеграции их в мультимедиаконтент.

Преступления, связанные с созданием, использованием и распространением вредоносного ПО, как правило, совершаются в условиях анонимности, с помощью эффективных методов сокрытия цифровых следов неправомерных воздействий. Обстановка совершения рассматриваемого преступления предполагает как непосредственный доступ к объекту посягательства (преимущественно в момент отсутствия потенциальной жертвы), так и удаленный (при наличии подключения к сети Интернет) и применение программно-аппаратных средств.

Местом совершения указанного преступления являются как конкретные компьютеры, серверы или информационные системы, так и локальные территории, учреждения и организации, в которых эксплу-

атируется объект воздействия либо критическая информационная инфраструктура. Довольно часто местом совершения преступления становится локация, где физически располагается средство совершения преступления (компьютеры и серверное оборудование, в том числе арендованные), облачные хранилища, а также веб-сайты и ресурсы сети Даркнет.

В подавляющем большинстве случаев местом (средой) использования и распространения вредоносных компьютерных программ выступает киберпространство ввиду его распространенности среди населения, реже — метапространство, блокчейн (распределенные реестры) либо гибридные инфраструктуры (распределенные облачные системы хранения данных и пр.). Таким образом, как правило, место реализации преступного умысла в интернет-пространстве — локация, где фактически располагалось компьютерное оборудование, посредством которого воплощен преступный план. Данная локация не ограничивается городом, территорией или конкретной страной, поскольку зачастую рассматриваемый вид преступлений носит трансграничный характер.

Временем совершения преступления признается время окончания преступного деяния вне зависимости от момента наступления последствий. Время создания, использования и распространения вредоносного ПО не всегда устанавливается точно, поскольку совершение преступления часто связано с задействованием различных компьютеров, ПО, информационных систем и прочего, реестры функционирования которых бывает довольно сложно сопоставить. Кроме того, работа указанных средств связана со временем, установленным в их системе, и оно может быть легко изменено преступником в целях искажения типичных следов.

Создание, использование и распространение вредоносного ПО ограничено временными рамками, и в зависимости от специфики конкретного случая может возникнуть необходимость определения времени создания ПО или наступления вредоносных последствий. Разработка вредоносных программ может быть довольно длительной, а процесс распространения или внедрения в систему отдельно взятого пользователя занимать считанные секунды.

Как правило, лицо, разрабатывающее, использующее и распространяющее вредоносное ПО, имеет высшее или среднее инженерно-техническое [20, с. 219] образование, обладает навыками программирования и системного администрирования сетей, а также знаниями в области информационных технологий, сетевой безопасности, криптографии, реверс-инжиниринга, в сфере оборота электронных средств платежей, банковской деятельности и международных платежных систем, национальной платежной системы Российской Федерации. Совершаемые преступления часто носят серийный характер ввиду массовости распространения идентичного ПО и сопровождаются тщательными действиями по сокрытию следов преступной деятельности. Анализ уголовных дел показывает, что преступники часто являются бывшими сотрудниками компаний, обладающими инсайдерской информацией, тщательно готовятся к атаке конкретного лица или объекта.

Основными мотивами создания, использования и распространения вредоносного ПО выступают корыстные побуждения (получение материальной выгоды), личная неприязнь к объекту воздействия, вымогательство или мошенничество, хулиганство [21, с. 186], вандализм (разрушение информационных систем, атаки на технические средства, стремление манипулировать системами и пр.), шпионаж (например, получение сведений экономической направленности, о личной жизни) и пр.

Предметом рассматриваемого преступления является вредоносное ПО, а также иная компьютерная информация, обрабатываемая на компьютерах или в информационных системах, не являющаяся программой, но способная нанести вредоносное воздействие.

Личность потерпевшего можно связать с владельцем (пользователем) объекта, в отношении которого использовалось вредоносное ПО, либо лицом, правам и законным интересам которого причинен вред. Потерпевших по указанным преступлениям также можно разделить на категории по принадлежности к физическим или юридическим лицам, а также к государственным структурам.

Исходя из анализа сложившейся за последние несколько лет следственной и судебной практики, необходимо отметить отличительные особенности личности потерпевшего по рассматриваемому виду преступления. Потерпевшим является физическое, юридическое лицо или государственная структура, которым причинен вред в результате преступного деяния, связанного с распространением вредоносного ПО.

Типичная жертва среди физических лиц — пользователь сети Интернет, который не обладает специальными знаниями в области кибербезопасности, активный пользователь интернет-сервисов или сотрудник государственных органов (инженер-программист, аналитик, системный администратор, администратор информационной безопасности и пр.), ставший мишенью атаки, направленной на получение доступа к служебной системе. Среди юридических лиц типичными пострадавшими становятся коммерческие компании, производственные предприятия, образовательные и научные учреждения, средства массовой информации. Все чаще объектом воздействия становится критическая информационная инфраструктура Российской Федерации. Также потерпевшими признаются государственные органы власти, силовые структуры, нередко — медицинские учреждения.

Психологическими и поведенческими чертами и иными особенностями личности потерпевших от рассматриваемых деяний являются недостаточная цифровая грамотность, излишняя доверчивость, высокая активность в цифровом пространстве, наличие критически значимой информации, отказ от применения антивирусного ПО, использование слабой защиты данных авторизации, устаревшего ПО и пр.

Таким образом, можно сделать вывод, что криминалистическая характеристика преступлений в сфере компьютерной информации, связанных с созданием, использованием и распространением вредоносных компьютерных программ, фактически представляет собой информационно-теоретическую базу для создания типовых алгоритмов их расследования и программного обеспечения в виде систем поддержки

принятия решений. Изложенное позволяет сделать вывод о возможности формирования на их основе цифрового двойника преступления в виде его цифровой копии, позволяющей оптимизировать эффективность расследования. В качестве исходных дополнительных данных для построения такого рода информационно-компьютерной модели как объекта познания [22, с. 72] могут быть отобраны условные признаки, которые в наибольшей степени влияют на прогноз раскрываемости (взятые, например, из статистических карт по преступлениям прошлых лет) и, по сути, выступают значимыми элементами криминалистической характеристики преступления. Такого рода обучающую выборку для предлагаемой системы необходимо выявлять с учетом современного развития информационных технологий и тенденций их применения в противоправной деятельности.

Технологии, основанные на методах обработки больших данных, математической статистики, искусственного интеллекта и алгоритмах машинного обучения, могут предоставить возможность построения типовых криминалистических характеристик преступлений в виде цифровых моделей, отображаемых в машиночитаемой форме и представленных сведениями о криминалистически значимых признаках и их корреляционных связях между математическими категориями, уравнениями или неравенствами. Модели такого рода могут использоваться следователями для получения знаний о преступлениях различных видов либо для разработки специального ПО, сопровождающего следственную и судебно-экспертную деятельность.

Для построения цифровой модели преступления необходимо выделение корреляционных связей между элементами криминалистической характеристики преступлений, что удобнее всего осуществлять с применением математических методов и алгоритмов машинного обучения. При этом определить корреляционные связи между указанными элементами позволит лишь детализация всех возможных способов совершения преступлений в сфере компьютерной информации (тактик преступников), средств (техник, используемых преступниками), оставляемых ими следов и прочих составляющих. Детализация способов совершения преступлений, в свою очередь, сформирует основу для построения цифровой модели преступления в сфере компьютерной информации (цифрового двойника преступления), которая позволит моделировать полную структуру преступной деятельности (подготовка, совершение и сокрытие преступления), а также ход его расследования в цифровом виде на основе предварительно обученных алгоритмов искусственного интеллекта, при этом с анализом взаимосвязи путем сопоставления способов совершения преступлений (тактик) со средствами совершения преступлений (техниками), оставляющими цифровые следы.

Таким образом, цифровой двойник преступления, построенный на основе соответствующей современным реалиями криминалистической характеристики, будет представлять собой виртуальную модель, отражающую состояние и динамику реального преступления, связанного с

созданием, использованием и распространением вредоносных компьютерных программ, а в аналогии — и с иными преступными деяниями в сфере компьютерной информации. Указанное позволит:

— разработать специализированное ПО в виде системы поддержки принятия решений для специалистов, задействованных в расследовании и раскрытии преступлений рассматриваемого вида, с возможностью прогнозирования хода следственных действий;

— исследовать различные сценарии совершения преступных деяний;

— формировать на основе выявленного содержания элементов криминалистической характеристики преступлений новые криминалистические учеты цифровых доказательств и пр.

Список литературы

1. *Бертовский Л.В.* Высокотехнологичное право: понятие, генезис и перспективы // Вестник Российского университета дружбы народов. Сер.: Юридические науки. 2021. №25(4). С. 735—749. doi: 10.22363/2313-2337-2021-25-4-735-749.

2. *Образование* для правосудия: модуль «Введение в цифровую криминалистику. Киберпреступность». Глобальная программа Дохинской декларации // УНП ООН. URL: https://www.unodc.org/documents/e4j/cybercrime/cybercrime_module_4_introduction_to_digital_forensics_ru.pdf (дата обращения: 25.04.2025).

3. *Федотов Н.Н.* Форензика — компьютерная криминалистика. М., 2012.

4. *Полякова Т.А., Минбалеев А.В., Кроткова Н.В.* Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации // Государство и право. 2020. №5. С. 75—87. doi: 10.31857/S013207690009678-7.

5. *Гончарова М.В., Бабаев М.М., Черкасов Р.В.* Комплексный анализ состояния преступности в Российской Федерации по итогам 2024 года и ожидаемые тенденции ее развития. М., 2025.

6. *Джола В.А.* Использование Big Data при назначении и проведении судебно-экологических экспертиз // Вестник Балтийского федерального университета им. И. Канта. Сер.: Гуманитарные и общественные науки. 2024. №2. С. 26—33. doi: 10.5922/ sikbfu-2024-2-3.

7. *Волчецкая Т.С.* Учение о криминалистических ситуациях: генезис, современное состояние и перспективы развития // Союз криминалистов и криминологов. 2019. №2. С. 59—64. doi: 10.31085/2310-8681-2019-2-222-59-64.

8. *Варданян А.В., Макаренко И.А.* Дискредитация субъектов раскрытия и расследования преступлений и криминалистические методы ее нейтрализации // Всероссийский криминологический журнал. 2022. Т. 16, №5. С. 638—645. doi: 10.17150/2500-4255.2022.16(5).638-645.

9. *Классификация* и типы вредоносного программного обеспечения // Лаборатория Касперского. URL: https://www.kaspersky.ru/resource-center/threats/malware — classifications (дата обращения: 25.04.2025).

10. *Зеленский В.Д.* Криминалистическая методика расследования отдельных видов и групп преступлений. Краснодар, 2013.

11. *Каневский Л.Л.* Разработка типовых криминалистических характеристик преступлений и их использование в процессе расследования // Российский юридический журнал. 2000. №2 (26). С. 101—111.

12. *О едином* учете преступлений : приказ Генпрокуратуры России №39, МВД России №1070, МЧС России №1021, Минюста России №253, ФСБ России №780, Минэкономразвития России №353, ФСКН России №399 от 29 декабря 2005 г. Доступ из справ.-правовой системы «КонсультантПлюс».

13. *О создании* государственных информационных систем по противодействию правонарушениям (преступлениям), совершаемым с использованием информационно-телекоммуникационных технологий, и о внесении изменений в отдельные законодательные акты Российской Федерации : федер. закон от 25 марта 2025 г. №41-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

14. *Россинская Е.Р., Рядовский И.А.* Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. Т. 14, №5. С. 699—709. doi: 10.17150/2500-4255.2020.14(5).699-709.

15. *Антонян Е.А., Россинская Е.Р., Клещина Е.Н.* Обзор правоприменительной практики по противодействию киберпреступлений. М., 2024.

16. *Вехов В.Б.* Цифровая криминалистика транспортных средств // Мир криминалистики. 2024. №2. С. 15—20.

17. *Белей А.В., Томская С.И.* Компьютерное криминалистическое исследование вредоносного программного обеспечения // Правовая информатика. 2023. №2. С. 102—112. doi: 10.21681/1994-1404-2023-2-102-112.

18. *Богомолова А.Г., Кот Е.А.* Криминалистические аспекты кибербуллинга как формы деструктивного поведения в сети Интернет // Вестник Балтийского федерального университета им. И. Канта. Сер.: Гуманитарные и общественные науки. 2023. №2. С. 25—32. doi: 10.5922/sikbfu-2023-2-3.

19. *База* данных угроз безопасности информации «Mitre Att&ck» // Mitre. URL: https://attack.mitre.org (дата обращения: 25.04.2025).

20. *Абдулвалиев А.Ф.* Преступления, совершаемые с использованием информационных технологий: проблемы квалификации и особенности расследования. Тюмень, 2021.

21. *Макаренко И.А.* Тактические особенности получения информации о личности преступника при производстве осмотра места происшествия // Актуальные проблемы криминалистической тактики : матер. междунар. науч.-практ. конф. М., 2014. С. 184—188.

22. *Макаренко И.А., Эксархопуло А.А.* Современное состояние и проблемы развития понятийного аппарата учения о предмете криминалистики // Сибирские уголовно-процессуальные и криминалистические чтения. 2024. №4. С. 64—74. doi: 10.17150/2411-6122.2024.4.64-74.

Об авторе

Зарина Ирековна Харисова — канд. техн. наук, доц., Уфимский университет науки и технологий, Уфа, Россия.
E-mail: zarinaid@mail.ru
SPIN-Code: 8293-1823
ORCID: 0000-0002-3902-3459

Z.I. Kharisova

CRIMINALISTIC CHARACTERISTICS OF THE CREATION, USE AND DISTRIBUTION OF MALICIOUS SOFTWARE

Ufa University of Science and Technology, Ufa, Russia
Received 05 May 2025
Accepted 15 May 2025
doi: 10.5922/vestnikhum-2025-2-2

To cite this article: Kharisova Z.I. 2025, Forensic characteristics of creation, use and distribution of malicious computer programs, *Vestnik of Immanuel Kant Baltic Federal University. Series: Humanities and social science*, №2. P. 20—33. doi: 10.5922/vestnikhum-2025-2-2.

Malicious software and viral phishing attacks have remained for several consecutive years among the most effective tools for infiltrating information infrastructure. In the vast majority of cases, the exploitation of malicious software is associated with gaining access to systems containing confidential information and its theft, which constitutes the least costly method for delivering and executing malicious code on a recipient's device. Given that the increase in unlawful acts related to the creation, use, and distribution of malicious computer programs is a significant factor in the self-reproduction of cybercrime, it is reasonable to explore the possibilities for optimizing their investigation process, in particular by examining the elements that comprise their forensic profile. The object of the study is the legal relationships arising in the investigation of crimes in the field of computer information associated with the creation, use, and distribution of malicious computer programs. The main goal is to reveal the content of the elements of the forensic profile of these offenses, taking into account the current development of information technologies and trends in the exploitation of malicious software. The theoretical significance of the study lies in the description of the forensic profile of the examined crimes, which may serve as the basis for forming their informational model (digital twins), and this constitutes the conceptual scientific novelty. The applied value of typical forensic profiles of crimes in the field of computer information lies in their potential use for the development of specific forensic investigation techniques, the creation of new forensic records based on digital evidence databases, and the design of specialized software in the form of decision support systems used, for example, in the formulation of investigative hypotheses and planning of investigations.

Keywords: cybercrime, malicious software, criminalistic characteristics of crimes, digital model of crime, digital twin, digital forensics, artificial intelligence

The author

Dr Zarina I. Kharisova, Associate Professor, Senior Lecturer of the Chair of Criminalistics, Institute of Law, Ufa University of Science and Technology, Ufa, Russia.

E-mail: zarinaid@mail.ru

SPIN-Code: 8293-1823

ORCID: 0000-0002-3902-3459