Вестник РУДН. Серия: Юридические науки 2019 Т. 23. № 1. 123–140
RUDN JOURNAL OF LAW http://journals.rudn.ru/law

DOI: 10.22363/2313-2337-2019-23-1-123-140

ЗНАЧЕНИЕ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ ПРИ РАССЛЕДОВАНИИ УГОЛОВНЫХ ПРЕСТУПЛЕНИЙ

О.А. Островский

Алтайский государственный университет
634021, Томск, Россия, ул. Льва Толстого, д. 77/83

Современные информационные системы, такие как электронное обучение, электронное голосование, электронное здравоохранение и т. д., часто используются не по назначению для нерегулярных изменений данных (подделка данных). Эти факты заставляют пересмотреть меры безопасности и найти способ их улучшить. Доказательство компьютерного преступления сопровождаются очень сложными процессами, которые основаны на сборе цифровых доказательств, судебном анализе и расследовании. Криминалистический анализ систем баз данных является очень специфической и сложной задачей и поэтому является основным источником деятельности для исследований. В этой статье представляется тот факт, что классические методы сбора цифровых доказательств не являются подходящими и эффективными. Для повышения эффективности предлагается сочетание хорошо известных технологий, независимых от мира баз данных, и их применение в области криминалистики. Также предлагаются новые направления исследований в этой области.

Ключевые слова: цифровые следы, информационные следы, цифровые доказательства, цифровая криминалистика, базы данных

I. ВВЕДЕНИЕ

Экспоненциальное использование современных информационных технологий влияет на рост компьютерной преступности, главной целью которой является получение доходов незаконным путем, промышленный шпионаж, подделка данных, фальсификация данных и любая другая незаконная деятельность. С юридической точки зрения, каждое из перечисленных действий может иметь последствия.

Происходит возрастание большого объема данных во всех сферах человеческой деятельности, таких как: государственные учреждения, университеты, предприятия среднего и малого бизнеса и т. д. (Bagutdinov, 2017:39–45). Поэтому необходимо обеспечить безопасную среду для хранения данных. Случаи, когда данные, которые были злонамеренно изменены (подделка данных, мошенничество с данными и несанкционированный сбор данных), могут привести к серьезным и долгосрочным последствиям.

Фальсификация данных может быть выполнена с несанкционированным доступом, а в некоторых случаях авторизованными пользователями (Melinda, 2007:42).

Существуют множество различных областей, где возможен факт фальсификации:

- электронное обучение;
- электронный университет;
- электронное голосование;
- электронное здравоохранение;
- другие области.

Рассмотрим несколько примеров из разных областей, чтобы получить представление о том, какие модификации могут доминировать.

Сценарий 1. Современные электронные (дистанционные) системы образования сильно зависят от использования современных информационных систем (Bagutdinov, 2014:39–42). Как правило, большинство экзаменов переносятся с традиционной системы на модули онлайн-тестирования. Причин для этого много: быстрота, чистота (прозрачность тестирования), без субъективной оценки учителей, автоматизация проверки и т. д. Но что, если после экзамена учитель с сомнительной этикой изменит количество баллов по некоторым вопросам в системе? Это может быть как ненамеренное вмешательство, так и преднамеренное: человеческая ошибка (человеческий фактор), скрывающая его или ее ошибки, фальсификация результатов экзамена. «Исправление» может быть выполнено на уровне взаимодействия с пользователем или непосредственно в структуре базы данных (вторая требует особого набора навыков работы с базой данных и прав доступа, но этот способ чище и его сложнее отследить). С точки зрения студента, это может быть результатом сдачи зачета или экзамена, и доказать, что что-то произошло, может быть очень сложно. С системной точки зрения — ничего не произошло, потому что приложение использует существующую базу данных.

Сценарий 2. Фальсификация результатов выборов техническими средствами подсчета голосов. В преддверии подготовки любых выборов главной задачей ЦИК (Центральная избирательная комиссия) ставит повышение доверия избирателей к выборному процессу. И если невозможно преодолеть недоверие избирателей к членам избирательных комиссий всех уровней, то необходимо вызвать доверие местного электората к техническим средствам подсчета голосов — КОИБам (Комплексам Обработки Избирательных Бюллетеней) и КЭГам (Комплексам Электронного Голосования).

Традиционно сложилось так, что в надежде вызвать доверие избирателей ЦИК вместо того, чтобы выявить и устранить причины недоверия, планирует перед каждыми выборами информационно-разъяснительную работу, мощную рекламную кампанию в СМИ, пресс-конференции с кандидатами, представителями политических партий, наблюдателями, журналистами с демонстрацией видеороликов и КОИБ.

Возникает вопрос, какие же цели преследует ЦИК, если известно, что технически развитые страны при голосовании, как правило, используют прозрачные урны и ручной подсчет. Ответ на этот вопрос достаточно прост — за счет повышения доверия к технике — обеспечить и явку, и заказанный результат выборов.

Ставка делается на банальный политический трюк — подмену понятий — недоверие к организующим выборы людям надо сначала заменить на недоверие к технике, а затем показать, что вряд ли беспристрастная машина (как и калькулятор) ошибается или обманывает. Она не ошибается и не обманывает — она работает как ее запрограммируют. Вопрос в другом — кто их программирует.

Перед выборами с применением КОИБ ЦИК проводит крупномасштабные презентации для прессы и кандидатов. Если внимательно присмотреться, то можно выявить имитаторы бюллетеней, которые замечательно распознаются (как настоящие). И проверить-то нельзя — нет настоящих бюллетеней, не показывают их, и имитация очень похожа на ксерокопию, сделанную с настоящих. Если программа КОИБ имеет настройку «настоящий бюллетень — имитатор», то, как она настроена в момент голосования? Действительно ли она проверяет подлинность бюллетеней? Почему при тестировании до начала голосования наблюдателям не показывают тест «настоящий бюллетень — ксерокопия (имитация, подделка)»?

Весь процесс можно очень просто проверить на избирательном участке, сделав ксерокопии настоящих бюллетеней и опустив их в КОИБ — он должен выплюнуть обратно эти «небюллетени», а если нет — то, возможно, результаты выборов заранее фальсифицируют, обеспечивая возможность выброса в эту электронную урну ксерокопий.

Проверка настройки программы на правильный подсчет голосов. Достаточно одной строчки в программе, и она, отследив, что режим работы не тестовый, а началось реальное голосование (по дате и времени), может, к примеру, каждый третий голос, поданный за кандидатов, приплюсовывать одному из кандидатов, или каждый второй голос за оппозиционную партию плюсовать другой партии.

Оказывается, все настройки КОИБ выполняет частная фирма, которая распоряжается программным обеспечением, доставляет и контролирует КОИБы при использовании их на выборах. КОИБы хранятся между выборами на ее складе, её сотрудники являются операторами КОИБ на презентациях. Так что результаты выборов зависят от политического заказа этой фирме.

Правительства многих стран запрещают государственным службам использовать программное обеспечение без открытых исходных кодов, чтобы обезопаситься от закладок и недокументированных функций. ЦИК же не только не имеет прав на программное обеспечение КОИБ, но и не в состоянии даже проверить соответствие программного обеспечения КОИБ первоначально разработанному: при каждом новом применении на выборах замечаются новые мелкие ошибки, характерные при исправлениях и внесениях изменений в про-

грамму. КОИБ — это некое аппаратное звено Государственной Автоматизированной Системы. Проверить правильность подсчета можно только контрольными ручными пересчетами, несмотря на то, что бюллетени имеют несколько степеней защиты от подделки и опыт применения КОИБ не выявил каких-либо ошибок в подсчете голосов.

Тем не менее без печати бюллетени обнаруживались в КОИБах при ручных пересчетах, и воспринимал КОИБ действительные бюллетени как недействительные — хотя это незначительное влияние на конечный результат выборов. Здесь стоит отметить тот факт, что незначительным такая ошибка может быть только в случаях явного перевеса на выборах, а в случаях в разницу 1–2% эта программная ошибка имеет большое значение. Хотя из-за ошибок КОИБ на выборах 2005 г., где при ручном пересчете обнаружилась разница в 200 голосов, поменялся лидирующий кандидат, и проигравший кандидат подал в суд. На выборах 2005 г. ЦИК принял решение по обязательному ручному пересчету результатов голосования на «федеральных» КОИБ по определенным округам, где не фиксировалась фальсификация выборов. В результате контрольный пересчет голосов показал достоверность выданных КОИБами результатов, а также и то, что вручную пересчитали и получили результат быстрее, чем с помощью КОИБ. При этом стоит учесть, что фальсификация данных выборов может быть вызвана не только определенными лицами, но и банальной ошибкой в коде программы.

Давно известно, что сканер в КОИБ не цветной и, следовательно, при сканировании не отличает ксерокопии от настоящих бюллетеней. Программа анализирует только оптическую плотность, размеры, форму, зоны для внесения отметок избирателями и зону печати (с трудом). Можно от руки написать в зоне печати номер избирательной комиссии цифрами как на почтовых конвертах, и КОИБ не распознает, что это подделка печати. Очень часто на выборах функция КОИБ по распознаванию печати вообще отключалась. КОИБ не распознает ни микрошрифт, ни цветную защитную сетку на бюллетенях. Такая проверка не предусмотрена при разработке КОИБ. Оказывается, по техническим условиям их изготовления они проверяются только на имитаторах бюллетеней. Микрошрифт и цветная защитная сетка на бюллетенях предназначены только для глаз членов участковых комиссий. И если при обычном голосовании участковая избирательная комиссия при подсчете голосов отбросит все вброшенные в урны подделки бюллетеней на основании видимых нарушений их защиты, то кто при применении КОИБ без контрольного ручного пересчета это сделает, неизвестно. Без КОИБов при обычном голосовании только «нечестная» участковая избирательная комиссия или органы имеют возможность при подсчете голосов подбросить в общую кучу бюллетени, причем только оригинальные из числа невыданных избирателям или дополнительно напечатанных в типографии. В КОИБ же кто угодно может вложить ксерокопии бюллетеней. Фальсифицировать выборы стало намного проще.

Однако, с другой стороны, это дает возможность наблюдателям от кандидатов и партий письменно заявить о нарушении: «Мы видели, что в КОИБ ввели ксерокопии, он не должен принимать “небюллетени”, но принял и, следовательно, необходимо проверить, как он их засчитал; т.е. требуется ручной пересчет», или сразу заявить о недоверии к КОИБам на основании отсутствия теста проверки бюллетеней на подлинность. Облегчит ли это работу участковой избирательной комиссии, которая будет вынуждена следить за тем, чтобы в КОИБы вводили именно выданные комиссией бюллетени и ничего иного — неизвестно. А это проверка на бюллетене печати и, как следствие, заодно и за кого был отдан избирателем голос. Ксерокопирование и открытая попытка убедиться в защите интересов избирателей не запрещены законом. Народ не на словах, а на деле должен быть убежден в надежной защите и правильном учете своего волеизъявления.

Журналисты всех стран с удовольствием делают репортажи с избирательных участков в день голосования, запечатлевая исторический момент опускания «первыми лицами» власти бюллетеней в урны. Кино-фототехника точно фиксирует время этого момента. После сканирования КОИБ создает файл с изображением бюллетеня и также точно фиксирует время его создания. Можно подсмотреть и раньше, если подключить к КОИБ полноценные клавиатуру и монитор: внутри сканера китайского IBM-совместимого ПК под управлением Windows XP без какой-либо защиты от несанкционированного доступа к информации.

В КОИБе предусмотрены дополнительные входы USB — портов для подключения Bluetooth или WiFi адаптера и создания дополнительной беспроводной сети (до 100 метров), из которой с «компьютера за перегородкой» возможно во время голосования получить доступ ко всей информации в КОИБах, размещенных на избирательном участке, и управлять программой подсчета голосов.

На основании вышеизложенного возникает вопрос о законности применения таких технических средств подсчета голосов на выборах — не нарушается ли закон об основных гарантиях избирательных прав бесконтрольностью, простотой фальсификации, отсутствием защиты от подделок, а также доступностью тайны голосования.

Если детектор валют стоимостью в 10 тыс. руб. считает 100 банкнот в минуту, определяя номинал и подлинность рублей, евро и долларов, то, как же считает, не распознавая подделок, КОИБ стоимостью 75 тыс. руб. — это открытый вопрос. Возникает вопрос в целесообразности применении КОИБ. Не упрощает КОИБ работу участковых избирательных комиссий, не обеспечивает тайну волеизъявления избирателей, облегчает фальсификацию результатов голосования. Правду можно получить, если отделить декларируемые цели применения КОИБ на выборах от действительных.

Только широкая огласка позволит объективно оценить КОИБы, КЭГи и предотвратить запланированные фальсификации выборов. В прозрачных урнах видно все и всем.

Сценарий 3. Врач ставит диагноз и назначает терапию с использованием лекарств или без них. Непреднамеренные или преднамеренные ошибки в этом процессе могут привести к серьезным осложнениям и даже к смерти пациента. Чтобы покрыть его действия, врач может попытаться изменить медицинскую карту пациента и добавить некоторые дополнительные примечания или рецепт лекарства.

Все эти примеры можно классифицировать как компьютерное преступление. Компьютерное преступление также является преступлением, но с различными последствиями. В этих случаях мы используем цифровую или компьютерную экспертизу для сбора и научной проверки всех компонентов информационных систем и их аппаратного обеспечения во всех аспектах. Результатом этого процесса является определение деталей о цифровой преступной деятельности.

Цифровая криминалистика является наиболее важной частью процесса расследования (Averyanova, 2002:960). Факты, собранные в этом процессе, должны быть представлены в суде. Процесс сбора, анализа и сохранения цифровых данных основан на научных методах; действительны только такие доказательства. С другой стороны, цифровые доказательства определяются как любые данные, хранящиеся на компьютере или передаваемые по сети, которые могут подтвердить (поддержать) или опровергнуть теорию о том, кто совершил цифровое преступление (Chisum, 1999:623).

Цифровая криминалистика основана на конфискации цифровых доказательств: персональных компьютеров (ПК), ноутбуков, сотовых телефонов, модулей памяти USB и др., в том числе сохранении, просмотре, анализе и сообщении фактов.

II. ПРОБЛЕМЫ СО СБОРОМ ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ НА УРОВНЕ БАЗЫ ДАННЫХ

Процесс расследования и криминалистический анализ на уровне базы данных чрезвычайно сложен (Ostrovskij, 2017:3–6). В качестве иллюстрации рассмотрим гипотетическую ситуацию. В информационной системе банка произошла утечка данных. Несанкционированный доступ к банковским счетам клиентов приводит к проблемам с деньгами у определенного количества клиентов. Их счета «уходят в минус». Персонал банка ничего не может сделать с раскрытием дела на внутреннем уровне. Клиенты решают выдвинуть обвинения. Из отдела полиции отправляют команду цифровой криминалистики. У них есть задача собрать все улики о подозрительных сделках, изучить их и представить в суд низшей инстанции. Команда должна следовать точно определенной процедуре, чтобы предоставить действительные доказательства в суд. Но на ранней стадии расследования команда столкнулась с очень серьезными проблемами. Первый этап — сбор и копирование данных. В случае банковской информаци-

онной системы эти задачи очень трудно реализовать. Вот несколько ключевых моментов:

- Информационная система банка основана на архитектуре распределенной базы данных;
- Размер базы данных превышает 1 ТБ;
- Чтобы скопировать все диски с изображениями данных, систему необходимо остановить. Политика банка не позволяет останавливать систему.

Резервных носителей недостаточно, потому что команда не знает временные рамки совершения преступления (Melinda, 2007:42).

Этот пример четко описывает ситуацию, когда классическая цифровая криминалистика совершенно беспомощна. Невозможно собрать действительные цифровые доказательства и в то же время сохранить непрерывность бизнеса банка (Ostrovskij, 2018:294-296) (фаза сохранения). Практически один и тот же сценарий применяется ко всем сложным и распределенным информационным системам: (электронное голосование, электронное правительство, электронный университет, электронная коммерция и т. д.).

Общеизвестно, что современному информационному обществу крайне необходимо обеспечить безопасную среду хранения данных. Это исследование мотивировано тем фактом, что одно изменение в базе данных может сделать любой преступник — рядовой гражданин.

Методы. Чтобы получить все необходимые данные, которые можно использовать при проведении криминалистических исследований, система с базой данных должна предоставить ответ на три вопроса: кто, когда и что сделал. Единственный способ сделать это — сильная подсистема ведения журнала аудита. В зависимости от архитектуры приложения существует широкий спектр данных, которые необходимо собрать, чтобы ответить на все эти вопросы. Например, IP-адрес и поставщик интернет-услуг являются абсолютно несущественной информацией в системе. С другой стороны, система регистрации аудита в веб-среде должна собирать эту информацию.

В этом исследовании мы решили проанализировать некоторые из известных методов и приемов для сбора данных об активности пользователей. В зависимости от того, сколько деталей необходимо об измененных данных, сбор цифровых доказательств можно разделить на две группы: простые и сложные. Простой сбор цифровых доказательств включает в себя базовые данные о действиях в информационных системах. В основном это очень простые реализации, и нет особого смысла представлять их более подробно. Т.е. даны ответы на вопросы «Кто» и «Когда». Ключевым моментом является то, что такого количества информации недостаточно для предоставления достоверных цифровых доказательств криминалистического анализа. Самая большая проблема — это вопрос «Что?». В нашем исследовании мы рассмотрели следующие методы сбора цифровых доказательств:

- триггеры;
- журнал резервного копирования файлов;
- репликация (копирование);

Любое изменение данных в фоновом режиме информационной системы — это набор операторов SQL (вставка, обновление, удаление). Пользователь не знает об этом процессе. Прикладной уровень посредством логики вызывает хранимые процедуры SQL. С точки зрения пользователей это могут быть команды «Сохранить», «Удалить» или «Добавить» в конкретном приложении.

Триггеры являются очень мощными элементами в системе баз данных, которые при правильном использовании могут быть очень полезны и обнаруживают изменение данных любого вида (объект и/или уровень данных). Эффективность триггеров основана на том факте, что каждая транзакция проходит через уровень для обнаружения модификации данных. Этот слой расположен в последнем сегменте информационной системы самой базы данных. Любая другая позиция может быть изменена или скомпрометирована.

Триггеры — это процедуры программирования и специальная реализация кода SQL. Они выполняются автоматически на основе определенного события. События могут быть локальными (уровень базы данных) или глобальными (уровень сервера). Существующая СУБД (система управления реляционными базами данных) может работать с триггерами DML (язык манипулирования данными) и DDL (язык определения данных). DML может быть выполнен для любого события модификации данных (выделение, обновление, удаление) в таблицах базы данных. Некоторые из интересных триггеров DML — это группы «After» и «Instead of». С точки зрения сбора цифровых доказательств и вопроса «Что» в этом исследовании используются триггеры «After». Они могут выполняться при определенных событиях, когда кто-то пытается изменить или создать какой-либо объект базы данных (операторы create, alter и drop). Очень важно, что пользовательское приложение может изменять структуру базы данных. Но что, если администратор попытается уничтожить доказательства определенных действий? DDL триггер может предоставить доказательства этой активности.

Только критическая часть цифровых доказательств, собранных с помощью триггеров, является достоверными данными. Что делать, если кто-то с надлежащими правами доступа имеет доступ к таблицам с цифровыми доказательствами и может подделать данные? Если журнал аудита записи удален или подделан, доказательства больше не действительны, и эту деятельность очень трудно обнаружить. Одно из наших предварительных исследований было сосредоточено на решении этой проблемы.

Архив файлов журнала. Каждая операция в базе данных является транзакцией. Чтобы сохранить целостность данных, ядро базы данных сначала создает запись в журнале транзакций. После фиксации «сигнала» (означает, что каждая часть транзакции завершена) изменение данных заносится в базу данных.

Каждая система баз данных имеет своего рода файл журнала транзакций. Хорошая политика требует регулярного файла журнала транзакций. Концепция резервного копирования журнала на регулярной основе может быть ис-

пользована для сбора и хранения цифровых доказательств активности пользователей. Каждое изменение данных или объекта на уровне приложения или базы данных записывается в журнал транзакций и может использоваться для доказательства возможной преступной или незаконной деятельности в системе.

Модификация резервных копий журналов очень сложна. Даже администраторы систем баз данных не могут сделать это без последствий.

Недельная точка этого метода — период задержки между резервными копиями журнала. В это время, пока изменения все еще находятся в журнале и не сохраняются, злоумышленник может редактировать файл журнала с помощью специальных инструментов приложения. Из-за того, что резервная копия не существует, удаление информации из активного файла журнала необратимо.

Копирование (репликация). Репликация — это набор технологий для копирования и распространения данных и объектов базы данных из одной среды в другую, а затем синхронизации между базами данных для обеспечения согласованности (она может быть разнородной).

По сути, эта возможность базы данных позволяет иметь одинаковое или только подмножество данных из одной системы базы данных в другой. Большинство коммерческих систем баз данных имеют встроенную технологию репликации, и в основном их можно разделить на следующие категории:

- Слияние репликации;
- Репликация снимков;
- Транзакционная репликация;

Репликация слиянием позволяет различным сайтам работать автономно, а затем объединять обновления в единый результат. Поскольку изменение данных возможно в любом направлении, этот тип недостаточно хорош для сбора цифровых доказательств.

Репликация моментальных снимков распределяет данные точно так, как они появляются в определенный момент времени, и не отслеживает обновления данных. Когда происходит синхронизация, весь моментальный снимок создается и отправляется пользователям системы (Bagutdinov, 2018:14–18). Репликация моментальных снимков наиболее подходит, когда изменения данных существенны, но нечасты. Например, если сбытовая организация ведет прайс-лист на продукцию и все цены обновляются в одно и то же время один или два раза в год, рекомендуется реплицировать весь моментальный снимок данных после его изменения. Учитывая определенные типы данных, более частые снимки также могут быть уместными. Например, если сравнительно небольшая таблица обновляется в течение дня, но допустима некоторая задержка, изменения могут доставляться ночью. Этот период ожидания очень проблематичен с точки зрения сбора цифровых доказательств. Злоумышленник может изменить и скрыть доказательства этой активности в определенный период.

Репликация транзакций обычно начинается со снимка объектов и данных базы данных публикации. Как только делается первоначальный снимок, последующие изменения данных и изменения схемы обычно доставляются по

мере их появления (почти в реальном времени). Этот факт делает репликацию транзакций лучшим кандидатом в технологии репликации для сбора цифровых доказательств.

III. СБОР ЦИФРОВЫХ ДОКАЗАТЕЛЬСТВ НА УРОВНЕ БАЗЫ ДАННЫХ

Фактическое судебное расследование начинается с обширного сбора данных, в котором идентифицируются и закрепляются все данные и доказательства. При этом необходимо, чтобы следствие тщательно проработало доказательную базу — данные не должны быть искажены мерами безопасности. Для этой цели используется принцип четырех глаз и метод хеширования MD5. Надлежащий порядок сохранения доказательств закладывает основу для успешного расследования и собирает данные в соответствующем порядке. В большинстве случаев легче анализировать данные с определенным уровнем безопасности в информационно-телекоммуникационной системе без риска непреднамеренного изменения доказательств. Заблаговременное сохранение данных позволяет работать с доказательствами при восстановлении исходных конфигураций от резервных копий до затронутых систем. В принципе, все мероприятия тщательно записываются в журнал при выполнении сбора данных.

На этапе анализа данных следы доказательств тщательно анализируются. Поскольку все соответствующие информационно-телекоммуникационные системы должны считаться безопасными или управляемыми в целом, этот шаг фокусируется на извлечении критически важных собранных в то время данных и установлении взаимосвязи между отдельными следами. Это включает, в частности, проверку операционной системы, конфигурационных и пользовательских файлов для манипуляций, а также рассмотрение всех соответствующих записей журнала.

Сбор данных в отношении расследования. Локардское правило. Важным аспектом судебной экспертизы является правило Локарда, названное в честь знаменитого канадца Эдмонда Локара. В нем говорится, что «никакое действие не может быть предпринято человеком, не оставляя при этом множество следов».

Аналогичный принцип применяется и в цифровой криминалистике. Здесь следует учитывать, что во время выполнения операций анализа данных различные изменения происходят в системе хоста из-за выполнения процесса или операций с файлами, например, в памяти или в постоянном хранилище. Это также относится к периодам бездействия, когда система не находится в спящем режиме. Эти изменения состояния могут быть объяснены правилом Локарда и обобщены под термином «динамика доказательств» — скорее всего, это явление можно сравнить с «дождем», который уничтожает возможные доказательства на месте преступления до обнаружения.

Следует помнить, что почти каждая программа, без сомнений, оставляет следы на затронутой операционной системе. Экспорт инструментов сбора дан-

ных рискует переписать кэшированные данные или фрагменты данных в память или в кеш с более новыми действиями и тем самым уничтожить или «затенять» соответствующую информацию. Эти дополнительные следы затем мешают логике оценки. Например, консольное приложение для создания образов памяти WinEn, входящее в состав судебного пакета EnCase, хранит файл драйвера в стартовом каталоге с именем winen.sys (Muller, 2018:1). Кроме того, в реестре Windows создается новая системная служба с именем winen. Служба запускается автоматически при каждой перезагрузке. Это означает, что запись в журнале событий Windows будет оставлена позже. Следователи должны не только учитывать, что изменения статуса неизбежны при доступе к ним, но в то же время они должны иметь возможность прогнозировать, документировать и адекватно объяснять влияние своих действий на информационно-телекоммуникационную систему. На этом фоне неудивительно, что на переднем плане стоит своевременное и тщательное хранение основного содержимого памяти.

Период полураспада данных. Другой темой сбора данных из подозрительной системы является период полураспада данных. В принципе, некоторые чувствительные типы данных могут быть идентифицированы, чья долговечность может быть очень различной.

Обычно система сбора данных пытается сортировать эти разные типы данных по периоду полураспада, чтобы определить порядок сбора данных. Особый интерес представляет порядок волатильности. В идеале данные должны быть скопированы в порядке их полураспада. Тем не менее, желательно быстро и структурированно защищать изменчивые данные (содержимое кеша и основной памяти, состояние сетевых подключений, запущенных процессов, зарегистрированных пользователей и т.д.). Из всех более или менее изменчивых данных (файлы конфигурации физической/виртуальной информационно-телекоммуникационной системы, запись в журнале) должна быть своевременно сделана соответствующая копия.

Типы данных. Некоторые источники информации могут быть идентифицированы в недавно скомпрометированной системе, которые представляют интерес для обнаружения и потери при остановке информационно-телекоммуникационных систем. В частности, это:

- Текущее время (с отклонением от доверительного контрольного времени);
- Содержание основной памяти;
- Список запущенных процессов;
- Список зарегистрированных пользователей;
- Список открытых сокетов, список приложений, которые прослушивают открытые сокеты, список систем, которые в настоящее время подключены к сети или недавно имели содержимое кеша.

Система тестирования состоит из аппаратного и программного обеспечения для проведения анализа данных. Обычно для этих целей используется виртуальные машины VMware ESXi на базе операционной системы Windows

(VM). Вычислительная мощность обеспечивается виртуальным процессором и 4 ГБ основной памяти. Чтобы подключить систему к сети, она имеет виртуальный гигабитный контроллер. VM также оснащена двумя виртуальными жесткими дисками (каждый по 40 ГБ), которыми управляет контроллер SCSI — помимо включения сетевого хранилища. Кроме того, имеется привод DVD-ROM. Конфигурация привода завершается виртуальным диском.

Чтобы избежать нехватки ресурсов, значения конфигурации могут быть скорректированы в любое время — количество виртуальных процессоров, основных размеров памяти и конфигурация сети могут быть изменены ответственными администраторами VM по запросу. Помимо гибкости настройки системы судебная рабочая станция работает как любая стандартная аналогичная система.

Преимущества использования виртуальной обработке на VM обосновывается гибкостью настройки и безопасностью работы. После того, как система была настроена, ее можно реплицировать множество раз в зависимости от требований — это быстрый и простой ввод в эксплуатацию.

Гибкость такой системы демонстрируется постоянно растущим использованием виртуальных машин — например, виртуальные жесткие диски могут быть интегрированы напрямую, если это необходимо. Помимо прочего в системе предусмотрена возможность передавать судебные данные в систему анализа, в зависимости от местоположения виртуальной системы, без корректировки конфигурации сетевой инфраструктуры. В этом случае требуется создание криминалистического дубликата, дополнительного «диска» для подключения к взломанной виртуальной машине, который затем может быть подключен к системе анализа.

Тип доступа к системе играет важную роль в сборе данных. Обычно компоненты специально скомпилированного набора инструментов начинаются последовательно с носителя только для чтения (файл ISO / защищенный от записи CD / USB-накопитель), результаты записываются по сети в общий файл. Важное преимущество: он работает только с собственными безопасными и надежными исходными файлами, никакие подготовительные операции на стороне клиента не должны выполняться, и внешние носители данных не должны прикрепляться к затронутой системе.

Еще одно важное преимущество: выбранная процедура минимизирует взаимодействие с затронутой системой и, следовательно, также изменяет изменчивые данные — это требует адекватного учета правила Локарда. В программном обеспечении, используемом для обеспечения волатильности данных, необходимо различать Windows и Linux Toolkit. По своему основному принципу они схожи, так же как и по своей структуре: они полагаются на собственную доверенную внешнюю оболочку, вызывающие инструменты автоматизируются путем пакетной обработки.

Далее вызывается надежная оболочка и запускается сценарий автоматического сбора данных. Данные собираются в порядке их важности:

• записать текущее системное время и разницу в доверительное контрольное время;

• для «средних» приоритетов безопасности — резервное копирование содержимого основной памяти;

• информация о зарегистрированных пользователях;

• информация о сетевых подключениях;

• информация о запущенных процессах;

• отображение текущего порта, информация о текущем состоянии сети;

• защита различной системной информации (журналы событий, данные конфигурации и т. д.);

• резервное копирование памяти процесса (только для Linux).

Поскольку результаты расследования хранятся на центральном «сервере судебной экспертизы», ответственный администратор должен получать данные и рассчитывать контрольные суммы для защиты целостности доказательств.

Параллельно может выполняться ручной анализ поведения связи затронутой системы. По существу, роль играют следующие факторы:

• оценка потока данных может быть использована для определения общего объема данных;

• данные о поведении общения могут дать ценную информацию для дальнейшего анализа (необычное поведение связи, открытые порты и т. д.).

Все важные цифровые следы анализируются немедленно в контексте детальной оценки и компетентных администраторов. В зависимости от того, насколько продуктивны результаты анализа, необходимы следующие меры (которые также могут использоваться в комбинации):

• система должна быть отключена. Правильное закрытие временных меток MAC недоступных файлов, а также удаление или повторное создание некоторых файлов сделало бы невозможным переопределить пространство удаленных файлов и восстановить их;

• носители данных содержат множество критически важных данных — как часть судебного расследования, может быть либо создана выборочная резервная копия для случая соответствующих файлов, либо осуществлено полное судебное дублирование подключенных носителей.

Для криминалистического дубликата весь объем данных передается по биту на резервный носитель. Преимущество этого метода заключается в полноте предоставленных данных, выборочном извлечении данных и возможности глубокого анализа полученных данных. Недостатком является большой объем требований к времени и потреблению памяти. Как правило, судебное дублирование выполняется только по «высоким» приоритетным инцидентам безопасности. Селективное резервное копирование сохраняет только выбранные данные. Преимущество этого метода заключается в небольшом требовании времени и пространства для хранения. Недостатком, однако, является точное определение того, что должно быть скопировано, и отказ от последующего анализа данных.

IV. БУДУЩИЕ ИССЛЕДОВАНИЯ

Эта статья четко описывает, что системы баз данных очень специфичны, когда дело доходит до криминалистического анализа. Было показано, что классические методы сбора цифровых доказательств не подходят и эффективны в средах баз данных. Существует большое пространство для совершенствования, новых моделей и практического применения. Новое исследование должно иметь следующие направления:

1. Модель обнаружения несанкционированного доступа в хранилище цифровых доказательств и улучшения проверки с использованием алгоритмов хеширования и шифрования;

2. В цифровой среде, особенно в базе данных, очень трудно сказать, что кто-то пытался или попытается внести какие-либо изменения в данные. Например, что делать, если пользователь делает запрос или запускает отчет, чтобы собрать все номера социального страхования пользователей в базе данных? С точки зрения контроля доступа ничего подозрительного не произошло. Но это может быть первым шагом к продаже номеров социального страхования на черном рынке, откуда могут быть использованы кражи личных данных;

3. Конфиденциальность становится важной особенностью в современном обществе. Быстрый прогресс в области информационных технологий и появление технологий, защищающих конфиденциальность, сделали информационную конфиденциальность критически важной областью, которую необходимо защищать. Технология повышения конфиденциальности направлена на то, чтобы сделать принципы и законы по защите конфиденциальности неотъемлемой частью технологии. Таким образом, информационная система предназначена для встраивания компонентов, позволяющих контролировать соответствие системы правилам конфиденциальности (Kristen, 2004:623), (Sabah, 2007:165–169). Предлагается определить целевое назначение личной информации в виде цепочки действий по этому типу информации. Он должен включать в себя ведение журнала аудита и судебный анализ.

4. Производительность может быть большой проблемой из-за накладных расходов на обеспечение ведения журнала аудита. Очень важный вопрос: каковы накладные расходы, связанные с применением ведения журнала аудита? Перехват каждого выполнения запроса в системе с тысячами транзакций в секунду влияет на производительность системы.

5. Модель высокозащищенного хранилища цифровых доказательств (DER), которое должно включать все элементы из этого и предлагаемых направлений исследований. Новая модель должна быть построена так, чтобы удовлетворить все потребности в сборе, сохранении, защите, проверке и достоверности цифровых доказательств и криминалистического анализа.

V. ЗАКЛЮЧЕНИЕ

База данных является основой большинства информационных систем; мы проанализировали известные методы, которые существуют в мире баз данных. Целью исследования было доказать адекватность методов для сбора цифровых данных о процессах и активности пользователей. Результаты положительные, и при адекватном внедрении подсистемы ведения журнала аудита вполне способны справиться с этой задачей. В результате работы:

- Доказано, что стандартная цифровая криминалистическая процедура неэффективна или очень сложна для применения в системах баз данных, в зависимости от информационных систем и среды.
- Рассмотрено текущие исследования в этой области и найдены общие элементы.
- Определенно будущие направления в этой области. В каждом направлении можно улучшить модель обнаружения несанкционированного доступа с помощью следующих элементов: обнаружение намерений, элементы конфиденциальности в отношении собранных данных и проблема производительности применения этой модели в средах большого бизнеса. Это можно измерить в изолированной среде с применением статистических и сравнительных методов.

Цель этого и будущих исследований состоит в том, чтобы смоделировать создание и оценку Digital Evidence Repository (DER). Эта модель должна состоять из всех основных элементов, которые имеют отношение к этой области систем баз данных. В конце концов практическое и коммерческое применение DER во всех основных системах баз данных должно стать конечным пунктом этого и будущих исследований.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК / REFRENCES

Aver'yanova, T.V., Belkin, YU.G., Koruhov., Rossijskaya E.R. (2002) Kriminalistika: ucheb. dlya vuzov [Forensics: studies. for universities]. M. Pp. 960. (in Russian).

Аверьянова, Т.В. Криминалистика : учеб. для вузов / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов., Е.Р. Российская; под ред. проф. Р.С. Белкина. М., 2002. 960 с.

Azemovie, J., Music, D., (2009) Efficient model for detection data and data sheme tempering with purpose of valid forensic analysis. ICCEA Manila, Philippines. 211 p. (In English).

Bagutdinov, R.A. (2017) Gnoseologicheskie aspekty k opredeleniyu naznacheniya i sostava STZ v zadachah proektirovaniya i razrabotki robototekhnicheskih kompleksov [Epistemological aspects to the definition of the purpose and composition of the FCZ in the tasks of designing and developing robotic systems] // Programmnye sistemy i vychislitel'nye metody. № 1. Pp. 39–45. (in Russian).

Багутдинов Р.А. Гносеологические аспекты к определению назначения и состава СТЗ в задачах проектирования и разработки робототехнических комплексов Программные системы и вычислительные методы. 2017. № 1. С. 39–45.

Bagutdinov, R.A. (2014) Issledovanie novejshih informacionno-kommunikativnyh tekhnologij v srednem professional'nom obrazovanii [Study of the latest information and communica-

tion technologies in secondary vocational education]//V sbornike: Nauchnyj poisk v XXI veke Materialy I mezhdunarodnoj nauchnoj konferencii po evrazijskomu nauchnomu sotrudnichestvu. Pp. 39–42. (in Russian).

Багутдинов Р.А. Исследование новейших информационно-коммуникативных технологий в среднем профессиональном образовании В сборнике: Научный поиск в XXI веке Материалы I международной научной конференции по евразийскому научному сотрудничеству. Под редакцией В.А. Должикова. 2014. С. 39–42.

Bagutdinov, R.A. (2018) Classification characteristic for processing heterogeneous data. International Journal of Open Information Technologies. T. 6. (8). Pp. 14–18. (In English).

Bagutdinov, R.A. (2018) The processing of heterogeneous data for multisensory systems of technical vision on the example of analysis of temperature and gas concentration. In the collection: Youth and modern information technologies. Collection of works of the XV International scientific-practical conference of students, graduate students and young scientists. National Research Tomsk Polytechnic University. Pp. 25–26. (In English).

Bagutdinov, R.A., Zaharova, A.A. (2017) The task adaptation method for determining the optical flow problem of interactive objects recognition in real time / Journal of Physics: Conference Series. T. 803. (1). (In English).

Chisum, J.W. (1999) Crime Reconstruction and Evidence Dynamics, Presented at the Academy of Behavioral Profiling Annual Meeting, Montrey, CA. 623 p. (In English)

Ben-Gan, I., Sarka D., Wolter, R. (2005) Inside Microsoft SQL Server 2005: T-SQL Programming, Microsoft Press. 544 p. (In English).

JoyMalmgren, M., (2007) An Infrastructure for database tamper detection and forensic analysis. The University of Arizona, 42 p. (In English).

Karakoc, M.M., Varol, A. (2018) Can erase montage traces permanently in audio files /2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya. Pp. 1–5. (In English).

Pavlou, K., Richard T. (2005) Snodgrass, Forensic Analysis of Database Tampering, from Department of Computer Science, University of Arizona, 3531 p. (In English).

LeFevrey, K., Agrawaly, R., Ercegovac, V., Ramakrishnan, R., Xuy Y., DeWitt, D. (2004) Limiting Disclosure in Hippocratic Databases, Proceedings of the 30th VLDB Conference, Toronto Canada. 1277–1288 p. (In English).

Li, Y., Zhang, X., Li, X., Zhang, Y., Yang, J., He, Q. (2018) Mobile Phone Clustering From Speech Recordings Using Deep Representation and Spectral Clustering / in IEEE Transactions on Information Forensics and Security, vol. 13, no. 4. Pp. 965–977. (In English).

Muller, L. (2008) New version of EnCase includes stand-alone utility to capture RAM. Available at: URL: http://www.forensickb.com/2008/06/new-version-of-encase-includes-stand.html [Accessed Januare 17th 2019] (In English).

Ostrovskij, O.A. (2018) Algoritm meropriyatij po analizu situacii pri podozrenii v sovershenii prestuplenij v sfere komp'yuternoj informacii s uchetom specifiki istochnikov dannyh ehtoj informacii [Algorithm of measures to analyze the situation in case of suspicion of committing crimes in the field of computer information, taking into account the specifics of the data sources of this information]// Pravo i politika. 10. Pp. 32–37. (in Russian).

Островский О.А. Алгоритм мероприятий по анализу ситуации при подозрении в совершении преступлений в сфере компьютерной информации с учетом специфики источников данных этой информации. Право и политика. 2018. № 10. С. 32–37.

Pastuhov, P. S., Losavio, M. (2017) Ispol'zovanie informacionnyh tekhnologij dlya obespecheniya bezopasnosti lichnosti, obshchestva i gosudarstva [The use of information technology to ensure the security of the individual, society and the state] // Vestnik Permskogo universiteta. YUridicheskie nauki. 36. Pp. 231–236. (in Russian).

Пастухов П.С., Лосавио М. Использование информационных технологий для обеспечения безопасности личности, общества и государства // Вестник Пермского университета. Юридические науки. 2017. Вып. 36. С. 231–236.

Reyes, A. (2007) Cyber Crime Investigation, Syngress Publishing, 432 p. (In English)

Sabah, S. (2007) Al-Fedaghi, Beyond Purpose-Based Privacy Access Control, Computer Engineering Department Kuwait University, 165–169 p. (In English).

Spyrou, T., Darzentas, J., (1996) Intention Modeling: pproximating Computer User Intentions for Detection and Prediction of Intrusions. 319–336 p. (In English).

Gupta1, Sh.K., VikramGoyal, Gupta, A. (2006) Malafide Intension Based Detection of Privacy Violation in Information System, Bagchi and V. Atluri (Eds.): ICISS 2006, LNCS 4332, pp. 365–368. (In English).

Warf, B. (2001) Segue ways into cyberspace: Multiple geographies of the digital divide. Environment and Planning(B), 28(1). Pp. 3–19. (In English).

Wen, B., Luo, Z., Wen, Y. (2018) Evidence and Trust IoT: Collaborative Security Mechanism / 2018 Eighth International Conference on Information Science and Technology (ICIST), Cordoba. Pp. 98–9. (In English).

Waleed, J., Abdullah, D.A., Khudhur M.H. (2018) Comprehensive Display of Digital Image Copy-Move Forensics Techniques /2018 International Conference on Engineering Technology and their Applications (IICETA), Al-Najaf. Pp. 155–160. (In English).

Сведения об авторе:

Островский Олег Александрович — аспирант кафедры уголовного процесса и криминалистики Юридического факультета ФГБОУ ВО «Алтайский государственный университет»

ORCID ID: 0000-0001-9280-3211

Контактная информация:

e-mail: ostrovskii_80@mail.ru

Для цитирования:

Островский О.А. Значение цифровых доказательств при расследовании уголовных преступлений // Вестник Российского университета дружбы народов. Серия: Юридические науки. 2019. Т. 23. № 1. С. 123–140. DOI: 10.22363/2313-2337-2019-23-1-123-140.

THE VALUE OF DIGITAL EVIDENCE IN CRIMINAL INVESTIGATIONS

Oleg A. Ostrovsky

Altai State University

77/83, Leo Tolstoy st., Tomsk, Russia, 634021

Modern information systems, such as e-learning, e-voting, e-health, etc., are often used inappropriately for irregular data changes (data falsification). These facts force to review security measures and find a way to improve them. Proof of computer crime is accompanied by very complex processes that are based on the collection of digital evidence, forensic analysis and investigation. Forensic analysis of database systems is a very specific and complex task and therefore is the main source of inspiration for research. This article presents the fact that classical methods of collecting digital evidence are not suitable and effective. To improve efficiency, a combination of well-known, world-independent da-

tabase technologies and their application in the field of forensic science are proposed. It also offers new directions for research in this area.

Key words: digital traces, information traces, digital evidence, digital forensics, databases

Information about the author:

Oleg A. Ostrovsky — PhD-student, Department of Criminal Procedure and Criminalistics, Faculty of Law, Altai State University

ORCID ID: 0000-0001-9280-3211

Contact information:

e-mail: ostrovskii_80@mail.ru

For citation:

Ostrovsky O. A. The value of digital evidence in criminal investigations (2019). RUDN Jurnal of Law, 23 (1), pp. 123–140. DOI: 10.22363/2313-2337-2019-23-1-123-140.