ПРОБЛЕМЫ АНАЛИЗА ПРОГРАММНО-АППАРАТНЫХ СРЕДСТВ НЕЗАКОННОЙ ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ АЗАРТНЫХ ИГР И МЕТОДЫ ИХ ИЗУЧЕНИЯ

Астахова Л.В.¹, Волков А.В.², Григорьев В.В.³, Роговский А.А.⁴

Email: Astakhova1136@scientifictext.ru

¹Астахова Людмила Викторовна - доктор педагогических наук, профессор,
высшая школа электроники и компьютерных наук,
Южно-Уральский государственный университет (национальный исследовательский университет);
²Волков Андрей Владимирович - генеральный директор,
автономная некоммерческая организация Центр судебных экспертиз и научно-технических исследований;
³Григорьев Владимир Викторович - заместитель начальника отдела,
отдел по обеспечению экономической безопасности и противодействия коррупции,
управление МВД России по г. Челябинску;
⁴Роговский Александр Андреевич – представитель,
Всероссийская Организация Интеллектуальной собственности в Уральском федеральном округе,
г. Челябинск

Аннотация: в работе рассмотрена проблематика разработки и практического применения методов и средств проведения анализа программного и аппаратного обеспечения, которое применяется для незаконных организации и проведения азартных игр в Российской Федерации. На примере отдельных программных продуктов рассмотрены правовые и технические аспекты изучения средств организации азартных игр, установления их программного, функционального и технического статуса, перспективы развития научных методов исследования программно-аппаратных средств в сфере азартных игр.

Ключевые слова: азартные игры, незаконная игорная деятельность, уголовная ответственность, игровое оборудование, методика, расследование, осведомленность.

PROBLEMS OF THE ANALYSIS OF THE SOFTWARE OF THE ILLEGAL ORGANIZATION AND CONDUCTING THE GAMBLING GAMES AND THE METHODS OF THEIR STUDYING

Astakhova L.V.¹, Volkov A.V.², Grigoriev V.V.³, Rogovskiy A.A.⁴

¹Astakhova Ludmila Viktorovna - Doctor of Pedagogical Sciences, Professor,
HIGHER SCHOOL OF ELECTRONICS AND COMPUTER SCIENCE,
SOUTH URAL STATE UNIVERSITY (NATIONAL RESEARCH UNIVERSITY);
²Volkov Andrey Vladimirovich - General Director,
AUTONOMOUS NON-COMMERCIAL ORGANIZATION "CENTER FOR FORENSIC EXPERTISE AND SCIENTIFIC AND
TECHNICAL RESEARCH";
³Grigoriev Vladimir Viktorovich - Deputy Head,
DEPARTMENT FOR ENSURING ECONOMIC SECURITY AND ANTI-CORRUPTION;
⁴Rogovsky Alexander Andreevich – Representative,
ALL-RUSSIAN ORGANIZATION OF INTELLECTUAL PROPERTY IN THE URALS FEDERAL DISTRICT,
CHELYABINSK

Abstract: the paper considers the problems of development and practical application of methods and tools for analyzing software and hardware, which is used for illegal organization and conduct of gambling in the Russian Federation. The legal and technical aspects of studying the means of organizing gambling games, establishing their software, functional and technical status, and the prospects for the development of scientific methods for researching software and hardware in the sphere of gambling are examined on the example of individual software products.

Keywords: gambling, illegal gambling, criminal liability, gaming equipment, methodology, investigation, awareness.

УДК 343.56

За последние одиннадцать лет игорный бизнес в России стал популярным и прибыльным видом деятельности. Широкое распространение получили не только государственные лотереи, но и новые формы организации азартных игр: на смену классическим игровым автоматам пришли программные продукты для обычных электронных вычислительных машин. На конец 2016 г. в России функционировало более 80 тысяч игровых залов, в которых было размещено около 1200 тысяч игровых автоматов.

29 декабря 2006 г. был принят Федеральный закон «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» № 244-ФЗ [2], который ввел жесткие требования к организации и проведению азартных игр, а также к организаторам и посетителям игорных заведений. Федеральным законом от 20.07.2011 № 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации» [1], в УК РФ была введена ст. 171.2, предусматривающая ответственность «за незаконную организацию и (или) проведение азартных игр с использованием игрового оборудования вне игорной зоны, либо с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», а также средств связи, в том числе подвижной связи, либо без полученного в установленном порядке разрешения на осуществление деятельности по организации и проведению азартных игр в игорной зоне». Федеральным законом от 22.12.2014 № 430-ФЗ «О внесении изменений в статью 171.2 Уголовного кодекса Российской Федерации и статьи 14.1.1 и 28.3 Кодекса Российской Федерации об административных правонарушениях» в ст. 171.2 УК РФ были внесены изменения: теперь уголовная ответственность наступает вне зависимости от размера извлеченного дохода, т.е. за факт осуществления указанной деятельности [7]. Кроме того, был увеличен размер штрафа, предусмотренный санкцией данной статьи.

Однако, несмотря на изменения в законодательстве, постоянно появляются и развиваются принципиально новые технические, программные и аппаратные методы и средства незаконной организации и проведения азартных игр [5], реализуемые в форме попыток выдать игорную деятельность за иную, не подлежащую регулированию обозначенными федеральными законами, тем не менее, несущую общественную опасность [3]. В последнее время широкое распространение получили так называемые биржевые терминалы, представляющие собой игровые автоматы либо персональные компьютеры с установленным на них программным обеспечением, программно и функционально предназначенным для организации и проведения азартных игр. Цель настоящей работы – рассмотреть основные методы, технологии и примеры таких программных средств, получивших в последнее время широкое распространение, а также обосновать методику их изучения, проведения анализа, исследования и установления юридически значимых признаков, позволяющих техническим специалистам и экспертам с достаточной степенью уверенности относить то или иное программное обеспечение к категории предназначенного для организации и проведения азартных игр.

Программный комплекс «Холитрейд» («Holytrade», «Holitrade»). На сегодняшний день широкое распространение имеет программное обеспечение «Холитрейд». Используются также наименования «Holitrade», «Holytrade». Различия в этих наименованиях часто выступают причиной коллизий в ходе судебных разбирательств, однако на деле все перечисленные названия принадлежат и означают одну и ту же платформу.

Подробно указанная платформа и принцип ее работы рассмотрены в [9]. В ходе данного исследования по специально разработанной авторской методике была проанализирована работа программно-аппаратного комплекса «Холитрейд», распространенного в сфере незаконного проведения азартных игр в России, и сделаны выводы о том, что имеют место именно маскировка под указанные виды деятельности и подмена понятий. При этом имеет место нарушение действующего законодательства, путем введения в заблуждение граждан производится извлечение прибыли от незаконной организации и проведения азартных игр. Клиенты и пользователи таких программно-аппаратных комплексов также нарушают закон.

В ходе анализа было проведено исследование системного блока персонального компьютера с установленным на нем программным обеспечением «Холитрейд». Для исследования была использована разработанная методика:

- скачивание с сайтов i.holitrade.com, iholi.net программного обеспечения «loto», «operator»;
- установка указанного программного обеспечения на системный блок персонального компьютера;
- проведение анализа возможностей программного обеспечения;
- анализ сетевого взаимодействия программного обеспечения с внешними ресурсами;
- анализ особенностей алгоритмов, заложенных в основу программного обеспечения.

В ходе исследования установлено программное обеспечение «loto», версии 1.117.0.706, 2.2.0.711. Необходимо отметить, что от версии к версии программного обеспечения основной набор его функций, файловая структура и алгоритмы работы остаются неизменными, а смена версии зачастую носит косметический характер: предпринимается исправление мелких программных ошибок, добавление новых функций с сохранением старых. Коллизии, возникающие в правовой сфере в рамках различности номера версий, чаще всего несущественны и несостоятельны именно в силу сохранения алгоритмов и функционального состава программ.

Данное программное обеспечение представляет собой программу-клиент для обеспечения доступа к функциям встроенных программ и связи с серверами системы «Холитрейд».

Для функционирования указанная программа «loto» использует файл конфигурации, в котором хранятся основные настройки программы. Указанный файл расположен в одном каталоге с программой, имеет название «loto.ini». Сведения, содержащиеся в указанном файле, подробно рассмотрены в [9].

Факт использования программой «loto» указанного файла «loto.ini» подтверждается следующим:

- в ходе проведения исследования была произведена процедура проверки взаимодействия программы «loto» с файлом «loto.ini» путем перемещения файла «loto.ini» из папки с программой «loto». После этого был произведен запуск программы «loto». При отсутствии файла «loto.ini» в папке с программой «loto» программа «loto» при запуске сообщает об ошибке: «Не удастся определить MAC-адрес устройства». В случае, когда файл «loto.ini» присутствует в папке с программой «loto», указанное сообщение об ошибке не появляется. В файле «loto.ini» имеются строки:

«;MAC-адрес подставляемый в качестве имени киоска вместо оригинального MAC-адреса сетевой карты

ForceMac= wy005»,

указывающие на то, что программа «loto» получает сведения о MAC-адресе. В данном случае параметр ForceMac выступает в качестве уникального идентификатора экземпляра программы «loto», отсутствие которого не позволяет программе функционировать. По данному идентификатору каждый экземпляр программы «loto» идентифицируется в личном кабинете, описанном ниже, и благодаря этому идентификатору возможно осуществление удаленного управления экземпляром программы и персональным компьютером, на котором она установлена.

- в ходе проведения исследования была произведена процедура проверки взаимодействия программы «loto» с файлом «loto.ini» путем проверки реакции программы «loto» на изменение содержимого файла «loto.ini». В файле «loto.ini» имеются следующие строки:

«;номер com-порта к которому подключен купюроприемник

BillCom=0

...

;номер com-порта к которому подключен диспенсер, для SmartPayout указать тот же COM-порт что и купюроприемник

DispCom=0»,

указывающие на номера COM-портов, к которым подключаются устройства «купюроприемник» и «диспенсер».

Кроме этого, в папке с программой «loto» имеется папка «logs», в которой при запуске программы появляется файл с расширением «txt» и именем, соответствующим дате, когда запускается программа «loto». В данный файл программа «loto» записывает информацию о своей работе. В случае если в файле «loto.ini» параметр «BillCom», задающий номер COM-порта, к которому подключен купюроприемник, равен 0, программа «loto» в файл с информацией о своей работе записывает следующую информацию:

«Не задан com-порт купюроприемника».

В ходе проведения исследования параметр «BillCom» в файле «loto.ini» был приравнен к значению «20», после чего была запущена программа «loto». Программа «loto» в файл с информацией о своей работе записала следующую информацию:

«Инициализируем купюроприемник cashcode (порт 20)»

Таким образом, подтверждается, что программа «loto» обращается в процессе своей работы к файлу «loto.ini» для получения сведений о настройках своей работы.

Содержимое данного файла «loto.ini» указывает на то, что программа «loto» имеет возможность подключения устройств для ввода средств с их дальнейшей фиксацией в меню «Баланс» (количество внесенных средств).

Кроме этого, был произведен анализ сетевого взаимодействия представленной программы с внешними ресурсами.

Рассматриваемая программа в процессе своей работы отправляет и получает данные на адрес dyndns.org, используя в качестве параметров идентификации логин «holitrade». DynDNS представляет собой сервис, который позволяет пользователям получить личный адрес, который будет привязан к пользовательскому компьютеру, не имеющему постоянного IP-адреса.

Когда информация попадает на адрес relay.dyndns.org с логином «holitrade», сервер DynDNS пересылает её на адрес i.holitrade.com (iholi.net). Необходимо отметить, что платформа нередко меняет свое доменное имя для усложнения ее обнаружения и идентификации. По указанному адресу расположен личный кабинет пользователя системы «Холитрейд», в ходе анализа функций которого установлено следующее:

- В личном кабинете «Холитрейд» возможно управление (создание, редактирование, удаление) учетными записями, используемыми программой «loto» для своей работы.

- В рамках настройки указанных учетных записей возможно редактирование так называемого «процента отдачи» (по умолчанию равного 60%), который представляет собой значение процента

прибыли от выигрыша, получаемого в процессе функционирования программы «loto». Установить значение этого параметра ниже 60 невозможно. Кроме того, необходимо отметить, что при торговле бинарными опционами и на биржевых торгах в целом не предусмотрено существование какого-либо управляемого относительного параметра, влияющего на размер прибыли.

- В личном кабинете отсутствуют какие-либо ресурсы, имеющие отношение к биржевым торгам, бинарным опционам и схожим по смыслу функционирования площадкам. Имеются функции сбора статистики функционирования подключенных к личному кабинету программ «loto».

- Любые изменения параметров счета в программе «loto» отражаются в личном кабинете i.holitrade.com (iholi.net).

- Из указанного личного кабинета возможно осуществление прямого управления персональным компьютером, на котором установлено программное обеспечение «loto» (блокировка, выключение, возможность приема и передачи файлов).

В ходе анализа сетевого взаимодействия программы «loto» с внешними сервисами не установлено фактов обращения программы к каким-либо площадкам биржевых торгов, площадкам по торговле бинарными опционами и схожим по смыслу функционирования площадкам.

В программе «loto» предусмотрена настройка ставки и параметров игры. Программа поддерживает подключения устройств для списания электронных средств с игрового баланса. Указанная программа не относится к лотерейному оборудованию, т.к. не обладает соответствующими признаками.

В ходе исследования установлено программное обеспечение «operator», версии 1.117.0.706, 2.2.0.711. Ситуация со сменой номера версии программы аналогично описанной выше у программ «loto». Данное программное обеспечение представляет собой программу-клиент для обеспечения пополнений игровых баллов, списания игровых баллов, контроля установленных ставок и процента отдачи (выигрыша) на персональных компьютерах, на которых установлена описанная выше программа «loto», и для связи с серверами системы «Холитрейд».

При установке указанной программы создается каталог с именем «operator» (имя может быть изменено) со следующей структурой:

«operator.exe Config.ini». Для своего функционирования указанная программа «operator» использует файл конфигурации, в котором хранятся основные настройки программы. Указанный файл расположен в одном каталоге с программой «operator» с именем «config.ini». Данный файл содержит в себе сведения, которые подробно рассмотрены в [9].

Содержимое данного файла «config.ini» указывает на то, что программа «operator» использует адрес сервера, к которому программа осуществляет подключение для приема и/или передачи сведений о своей работе: <http://relay.dyndns.org/relay/> с именем клиента «holitrade».

Так как исследуемое программное обеспечение «loto», описанное выше, использует аналогичные параметры подключения для своей работы, можно утверждать, что они функционируют в комплексе. Программа «operator» выполняет функции для обеспечения пополнений игровых баллов, списания игровых баллов, контроля установленных ставок и процента отдачи (выигрыша), то есть, программа «operator» выполняет функции организации игрового процесса для программы «loto».

Кроме того, необходимо отметить следующие особенности:

- Программа «operator» имеет версию для установки на мобильные телефоны под управлением операционной системы «Android». Эта версия имеет возможности и функции, идентичные версии программы «operator» для персональных компьютеров.

- Описанное программное обеспечение «loto» и «operator» могут быть запущены в среде операционных систем семейства UNIX\Linux при условии использования эмуляторов программной среды операционных систем семейства «Windows» (например, эмулятора Wine).

В пользовательском соглашении (оферте) программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, указано, что оно используется для проведения бинарных опционов. Бинарный опцион – опцион (договор, по которому покупатель опциона (потенциальный покупатель или потенциальный продавец базового актива — товара, ценной бумаги) получает право совершить покупку или продажу данного актива по заранее оговоренной цене в определенный договором момент в будущем или на протяжении определенного отрезка времени), который в зависимости от выполнения оговоренного условия в оговоренное время либо обеспечивает фиксированный размер дохода (премию), либо не приносит ничего.

В интерфейсе программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, имеется график, в реальном времени отражающий курс валютной пары «евро\доллар». Пользовательским соглашением программного обеспечения (офертой) подразумевается, что программное обеспечение «loto», распространяемое ресурсами <http://i.holitrade.com>, <http://iholi.net>, должно обеспечивать проведение бинарного опциона, в котором в качестве актива выступает значение курса валютной пары «евро\доллар» в определенный момент времени.

Однако в ходе проведения анализа функций программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, установлены следующие признаки, что данное программное обеспечение не обеспечивает проведение бинарных опционов:

- проведение бинарного опциона предполагает возможность для пользователя указать, на какое из двух событий он ставит – на то, что курс валютной пары будет больше или меньше определенного значения. В интерфейсе программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, отсутствует возможность для пользователя выразить свое намерение поставить на любое из двух указанных событий – имеется только кнопка «Сделка», также имеется кнопка «Тренд», которая функционально неактивна в момент принятия пользователем решения.

- проведение бинарного опциона предполагает, что он заключается на определенный, заранее оговоренный момент времени либо промежуток времени. В интерфейсе программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, не предусмотрено функций, которые позволяли бы пользователю каким-либо образом определять конкретное время или промежуток времени, в который он хочет получить результат по опциону – происходит только фиксация времени, когда пользователь нажимает на кнопку «Сделка». Также происходит фиксация так называемого «времени исполнения» - только в том случае, если анимация, представленная в интерфейсе программного обеспечения, сообщает о выигрыше, и только после того, как пользователь еще раз нажмет кнопку «Сделка». До этого момента не отражается результат проведенной операции, а период ожидания между результатом анимации и нажатием на кнопку «Сделка» может быть произвольным

- результат проведенной операции в программном обеспечении «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, не связан с курсом валютной пары «евро\доллар» в момент завершения операции: этот результат достигается простым сложением фиксированного объема выигрыша, который отражается в анимации в интерфейсе программного обеспечения, и курса валютной пары «евро\доллар» в момент завершения операции, при этом этот момент определяется пользователем произвольно. При этом полученный результат не зависит от динамики курса валютной пары – изменение курса вверх или вниз не влияет на результат.

- анимация, с которой взаимодействует пользователь путем нажатия на кнопки интерфейса программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, является типичной реализацией интерфейса игрового оборудования – игрового автомата: имеется возможность осуществлять ставки на одну, две, три, четыре или пять линий, указывать размер ставки, а в случае выигрыша – провести «дополнительную игру» («BONUS GAME» в терминах программного обеспечения) путем нажатия на кнопку «Тренд», которая становится активной, если в представленной анимации происходит момент выигрыша. При этом результат такой «дополнительной игры» влияет на результат проведенной пользователем операции – в случае, если «Дополнительная игра» заканчивается успешно, увеличивается размер результата проведенной операции.

- в интерфейсе программного обеспечения «loto», распространяемого ресурсами <http://i.holitrade.com>, <http://iholi.net>, отражается неизвестный «тип опциона» - «OCEFXVON».

Факт наличия возможности осуществления ставок, факт возможности настройки процента выигрыша через личный кабинет i.holitrade.com (iholi.net), отсутствие связи с какими-либо биржевыми площадками и имеющиеся в программе «loto» функции указывают на то, что персональный компьютер, на который установлено такое программное обеспечение, может считаться игровым оборудованием, использование которого за пределами игровой зоны является незаконной организацией и проведением азартных игр, а само программное обеспечение «loto» и «operator» программно и функционально предназначены для организации и проведения азартных игр.

Резюмируя результаты анализа описанного программного обеспечения, можно составить следующую схему взаимодействия (Рис. 1).

Рис.1. Схема информационных потоков

- Программа «loto» отвечает за обеспечение игровых функций (доступ к играм, ставки, получение выигрыша).
- Программа «operator» осуществляет управление программами «loto» (пополнение баланса, включение\выключение программ, ведение статистики)
- Личный кабинет на сайте i.holitrade.com (iholi.net) выступает как средство управления пользователями (учетные записи для программы «operator», регистрация идентификаторов программ «loto», пополнение баланса, ведение статистики, настройка процента выигрыша, управление программами «operator» и «loto»).

• Между программами и личным кабинетом производится информационный обмен. Информационный обмен состоит из запросов, которые программы «loto» и «operator» отправляют на указанный в конфигурационных файлах адрес relay.dyndns.org, IP-адрес 148.251.166.211. Запросы выглядят следующим образом:

- запрос, отправляемый программами для проверки связи с сервером:

Длительность запроса 1.918705 секунд, адрес: 148.251.166.211, протокол TCP, длина запроса 66 байт, содержимое запроса: [SYN] Seq=0 Win=63443 Len=0 MSS=1460 WS=64 SACK_PERM=1

- запрос, отправляемый программами для получения и изменения своих настроек:

Длительность запроса 1.997432 секунд, адрес: 148.251.166.211, протокол HTTP, длина запроса 274 байт, содержимое запроса: GET /holitrade/gamelauncher.ini HTTP/1.1.

Общий алгоритм работы программного обеспечения «loto» пошагово (с ветвлениями в логике работы) выглядит следующим образом (описаны выполненные действия и функции, которые выполняет программное обеспечение. Состав и назначение функций установлены согласно общему алгоритму, описанному в заключении данной работы):

- осуществляется запуск программного обеспечения «loto» путем двойного нажатия левой кнопкой манипулятора типа «мышь» (либо путем однократного нажатия клавиши «Enter» стандартной клавиатуры) на ярлык программного обеспечения «loto», расположенного в каталоге операционной системы (либо путем аналогичных действий с исполняемым файлом программы «loto» в каталоге ее установки);

- запускается программное обеспечение «loto». Процесс запуска сопровождается появлением на экране окна с фоном темно-зеленого цвета и надписью «Загрузка»;

- затем появляется окно с заголовком «выбор анимации». В представленном окне в верхней части расположено несколько кнопок, при нажатии на которые происходит переключение (смена) содержимого раздела окна, расположенного под описанными кнопками: в указанном разделе в графическом виде с подписями расположены кнопки выбора так называемой «анимации». При нажатии левой кнопкой манипулятора типа «мышь» на любую из кнопок (в частности, в ходе проведения исследования – на кнопку «фруктовый коктейль») происходит смена содержимого окна программного обеспечения;

- после выбора анимации появляется окно с текстовым полем, в котором размещено соглашение-оферта, под текстовым полем расположены две кнопки: «Принять» и «Отказаться». При нажатии на кнопку «Отказаться» происходит возврат к предыдущему окну с выбором «анимации». При нажатии на кнопку «Принять» происходит переход к следующему окну;

- затем появляется окно с фоном темно-зеленого цвета, в котором в верхней части представлены пункты: наименование «Holytrade», версия программного обеспечения, поле «счет» с цифровым значением счета (равное 0 до тех пор, пока счет не пополнен), поле «телефон поддержки» (пустое); в левой части представлены кнопки светло-зеленого цвета «выбор анимации», «забрать деньги», таблица с полями «время открытия», «тип опциона», «премия», «кол-во опционов», «цена открытия», «время исполнения», «цена закрытия», «результат». До совершения каких-либо действий поля в таблице пусты; кнопка «переключить вид», кнопка «авторотг»; график с подписью «валютная пара EUR\USD», на котором раз в секунду изменяются значения в виде линейного графика желтого цвета. В нижней части – представлены кнопки «плечо 1», «плечо 2», «плечо 3», «плечо 4», «плечо 5», кнопка «кол-во лотов», кнопка «тренд» (неактивная), кнопка «сделка». В центральной части интерфейса имеется графический блок с тремя линиями и пятью столбцами, подписями «1», «2», «6», «4», «9», «1», «8», «5», «7» по левому и правому краям и пятнадцатью блоками, в каждом из которых содержится графическое изображение фруктов: вишни, лимона, яблока, персика, арбуза, а также графические изображения надписей «Fruit cocktail». Над описанными пятнадцатью блоками расположены три поля: поле «Total Bet» («Общая ставка»), поле «Lines» («Линии»), поле «Credit» («Баланс»). Функционал описанных кнопок:

1. При нажатии левой кнопкой манипулятора типа «мышь» на кнопку «выбор анимации» происходит возврат к выбору анимации, описанному выше.

2. При нажатии левой кнопкой манипулятора типа «мышь» на кнопку «забрать деньги» появляется надпись «обратитесь к администратору» и выход в окно с выбором анимации.

3. При нажатии левой кнопкой манипулятора типа «мышь» на кнопку «переключить вид» в окне графический блок с 15 графическими блоками становится меньшим и перемещается в левый нижний угол (на то место, где расположен график валютной пары), а сам график валютной пары занимает место графического блока. При этом раз в секунду продолжает происходить обновление так называемого графика валютной пары.

4. При нажатии левой кнопкой манипулятора типа «мышь» на кнопки «плечо 1», «плечо 2», «плечо 3», «плечо 4», «плечо 5», «количество лотов» на экране в графическом блоке происходит изменение полей «Lines» («Линии»), «Total Bet» («Общая ставка»), «Credit» («Баланс»). При этом поле «Баланс» уменьшается, а поля «Общая ставка» и «Линии» увеличиваются пропорционально цифровому значению нажатой кнопки, а по левому и правому краю загораются (становятся активными) соответствующие пункты (пункты соответствуют выбранному «плечу», то есть выбранному количеству линий, на которые делается ставка). По своей логике указанные кнопки, графический интерфейс и описанные графические элементы полностью соответствуют функциям игрового автомата: осуществляется ставка на заданное количество линий заданной суммы, пропорционально уменьшается активный баланс. При этом в процессе нажатия на указанные кнопки программное обеспечение не осуществляет никаких сетевых запросов, то есть действия пользователя, нажимающего на кнопки, ни с чем не соотносятся (в частности, если бы исследуемое программное обеспечение было предназначено для торговли биржевыми опционами, программное обеспечение должно было бы обеспечивать функцию проверки доступного для торговли количества опционов и доступного для пользователя объема его счета).

5. Кнопка «Тренд» не активна.

6. При нажатии левой кнопкой манипулятора типа «мышь» на кнопку «Сделка» начинается вращение барабанов описанного графического интерфейса, при этом в описанной левой таблице фиксируется поле «время открытия» (соответствует времени нажатия на кнопку «сделка»), «тип опциона» (всегда равен «OCEFXVON» независимо от любых действий пользователя), «кол-во опционов», «цена открытия» (поле принимает произвольное значение, не связанное с курсом какой-либо валютной пары), затем по прошествии нескольких секунд (не строгого количества – от 1.95 секунд до 2.7 секунд в ходе проведения исследования) фиксируется значение поля «время исполнения» (значение равно значению поля «время открытия» плюс то время, на протяжении которого крутились барабаны), «цена закрытия» (поле принимает произвольное значение, не связанное с курсом какой-либо валютной пары), «результат» (полностью соответствует значению выигранных кредитов, отраженному в графическом интерфейсе описываемого окна). В случае, если в графическом интерфейсе выпадает так называемая «выигрышная комбинация» (соответствует выигрышным комбинациям игровых автоматов типа «Игрософт»), в блоке с графиком «валютная пара» появляются прямоугольники красного цвета с подписью над ними, подпись соответствует значению поля «цена закрытия», при этом появившиеся прямоугольники и значения никак не связаны с имеющимся графиком и его значениями.

7. В случае если выпавшая выигрышная комбинация превышает обычный выигрышный порог (то есть, если совпадающих значений выигрышных графических элементов по количеству больше, чем то количество, на которое ставил пользователь), становится активной кнопка «тренд». При нажатии на кнопку «тренд» происходит смена активного окна программного обеспечения. На экране вместо графического окна с 15 графическими блоками появляется окно с пятью игральными картами и заголовок

«бонусная игра» («BONUS GAME»), повернутыми к пользователю «рубашками вверх». При нажатии на одну или несколько (по желанию пользователя) кнопок «плечо» происходит графическая индикация соответствующей кнопки карты, после нажатия на кнопку «сделка» выбранные пользователем карты переворачиваются и программное обеспечение производит сверку комбинации открытых карт с выигрышными комбинациями азартной игры типа «покер». В случае, если выбранные пользователем карты соответствуют выигрышной покерной комбинации, размер выигрыша пользователя пропорционально увеличивается, затем происходит возврат к предыдущему графическому окну с 15 графическими блоками. При этом на протяжении всей «бонусной игры» не происходит каких-либо активных отметок на графике «валютной пары», значение поля «результат» в левой таблице увеличивается пропорционально полученному значению выигрыша в результате «бонусной игры».

8. При нажатии левой кнопкой манипулятора типа «мышь» на кнопку «Автоторг» происходит процесс, аналогичный описанному в п. 6 процессу, при этом процесс повторяется циклически до тех пор, пока у пользователя отличный от нуля положительный активный баланс. При этом не происходит «бонусной игры», описанной в пункте 7.

При этом любое изменение (выигрыш или проигрыш) отражается на значении поля «Счет» и поля «Общий баланс» (в большую или меньшую сторону соответственно). При этом каждое изменение баланса пользователя сопровождается сетевым запросом по адресу личного кабинета системы «Холитрейд», в теле указанного запроса содержится значение, на которое изменяется текущий активный баланс, и идентификатор программного обеспечения, соответствующий значению записи «ForceMac», указанному в файле конфигурации «loto.ini» исследуемого программного обеспечения «loto». При этом каждое нажатие на кнопку «Сделка» сопровождается вызовом функции генератора случайных чисел, а каждый запуск программного обеспечения «loto» сопровождается в том числе специальным запросом к личному кабинету системы «Холитрейд».

В ходе анализа функций выделенного программного обеспечения «loto» было установлено, что программное обеспечение «loto» функционирует совместно с программным обеспечением «operator», которое также относится к платформе «Холитрейд». Общий алгоритм работы программного обеспечения «operator» выглядит следующим образом:

1. При запуске программного обеспечения «operator» (путем двойного нажатия левой кнопкой мыши на ярлык или исполняемый файл либо путем запуска с мобильного телефона) происходит открытие активного окна программного обеспечения «operator». При этом требуется ввод актуальных учетных данных – логина и пароля.

2. В интерфейсе программного обеспечения «operator» имеются следующие функции:

- активное окно, отражающее запущенные и активные экземпляры программного обеспечения «loto», идентификаторы которого привязаны через личный кабинет системы «Холитрейд» к учетным данным программного обеспечения «operator».

- кнопки пополнения баланса программного обеспечения «loto» на 10, 50, 100, 200, 500, 1000 или произвольное количество кредитов. При этом нажатие на указанные кнопки сразу же отражается на работе программного обеспечения «loto» - на указанную сумму пополняется текущий активный баланс пользователя;

- в интерфейсе программного обеспечения «operator» отображается сумма выигранных и проигранных кредитов в таблице с полями «Вход», «Выход» и «Баланс»

- в интерфейсе программного обеспечения «operator» путем нажатия на кнопку «настройки группы» появляется окно, в котором можно задать так называемый «процент отдачи». Значение указанного процесса напрямую влияет на результаты игры в программе «loto».

Таким образом, общий алгоритм работы программ «loto» и «operator» выглядит следующим образом:

1. Осуществляется запуск программного обеспечения «loto». Осуществляется запуск программного обеспечения «operator». Активные экземпляры программного обеспечения «loto» отображаются в интерфейсе программного обеспечения «operator».

2. Через программу «operator» осуществляется пополнение баланса программ «loto».

3. В программе «loto» осуществляется выбор так называемой «анимации» и становится доступным процесс игры.

4. Осуществляется процесс игры в программе «loto».

5. Все процессы пополнения баланса и выигрыша/проигрыша сопровождаются информационным обменом о соответствующих фактах через личный кабинет системы «Холитрейд» между программами «loto» и «operator».

6. Каждый запуск процесса игры путем нажатия кнопки «Сделка» или каждая итерация процесса игры, инициализируемая после нажатия на кнопку «Автоторг», в программе «loto» сопровождается вызовом функции генератора случайных чисел.

7. Общий процесс игры в программе «loto» (соотношение выигранных и проигранных кредитов) соответствует заданному через программу «operator» значению поля «процент отдачи» (процент выигрыша).

8. Программа «operator» поддерживает функции: удаленное выключение системного блока, на котором установлено программное обеспечение «loto»; очистка папки «logs» программного обеспечения «loto»; полное удаление программы «loto» с конкретного системного блока.

Исходя из вышесказанного, можно сделать однозначный вывод о программном и функциональном предназначении исследуемой программной платформы для организации и проведения азартных игр.

Программная платформа «Холитрейд» в поставке с программным обеспечением «WinLocker». В силу того, что с течением времени и накоплением правовой и судебной практики, программная платформа «Холитрейд» стала все чаще фигурировать в судах различной инстанции как игровая платформа, ее распространители предприняли шаги для сокрытия функционального и файлового состава платформы, усложнения проведения исследований и экспертиз. В качестве инструмента для усложнения и сокрытия в состав программной платформы «Холитрейд» было включено прикладное программное обеспечение «WinLocker».

Данное программное обеспечение выполняет сразу несколько функций:

1. Криптографическая защита программной платформы «Холитрейд». Программное обеспечение «WinLocker» создает зашифрованный файловый контейнер, который подключается к операционной системе как виртуальный жесткий диск, внутри которого хранится программная платформа «Холитрейд». Для подключения такого виртуального жесткого диска необходимо знать криптографический ключ, который использовался для шифрования, в связи с чем в рамках проведения исследований и экспертиз у специалистов и экспертов возникают трудности, выражающиеся в невозможности осуществить доступ к исследуемой программной платформе.

2. Программа «WinLocker» осуществляет связь с личным кабинетом программной платформы «Холитрейд» и обеспечивает функции обновления программной платформы, а также функции контроля: на стороне личного кабинета возможно осуществление блокировки работы программы «WinLocker», что делает полностью недоступным зашифрованный файловый контейнер с программной платформой «Холитрейд».

3. Блокировка доступа пользователя к любым функциям ЭВМ, кроме непосредственной работы с программной платформой «Холитрейд» (программами «loto» и «operator»).

В остальном программная платформа «Холитрейд» не претерпела изменений с программной и функциональной точки зрения. Программа «WinLocker» может рассматриваться как некая внешняя оболочка, предназначенная одновременно для защиты программ от несанкционированного доступа извне и для их обновления (в случае, если доступ осуществляется санкционированно). При этом необходимо отметить, что, несмотря на попытки распространителей скрыть наличие программной платформы «Холитрейд», сам факт наличия программы «WinLocker» однозначно указывает на наличие совместно с ней программной платформы «Холитрейд», так как программа «WinLocker» не относится к общедоступным программам с универсальным функционалом, а предназначена именно для обеспечения работы программной платформы «Холитрейд».

В качестве обобщающего результата проведенного научного исследования была сформулирована общая методика проведения исследования программных платформ, программно и функционально предназначенных для организации и проведения азартных игр. Данная методика может применяться при проведении исследований и экспертиз программных, аппаратных и программно-аппаратных средств в качестве базовой методики, в частности, если специалист или эксперт проводят анализ в рамках доследственных, следственных или судебных действий по статье 171.2 УК РФ. В методике в качестве объекта указаны системные блоки ЭВМ (как наиболее часто встречающиеся объекты), но ее применение справедливо для любых ЭВМ, обладающих необходимыми техническими и программными характеристиками. Методика состоит из следующих этапов:

1. Проведения полного посекторного копирования содержимого жесткого диска представленного системного блока на технический жесткий диск с использованием специализированного программного обеспечения.

2. Установка технического жесткого диска, содержащего посекторную копию жесткого диска представленного системного блока, в представленный системный блок в соответствующие разъемы. Данный метод проведения исследования содержимого посекторной копии жесткого диска представленного системного блока обеспечивает неизменность информации на представленном объекте, а также обеспечивает полное соответствие аппаратного обеспечения (для исключения потенциальных проблем с загрузкой операционной системы на аппаратном обеспечении, которое отличается от представленного системного блока).

3. Загрузка операционной системы из исследуемой копии содержимого жесткого диска представленного системного блока путем включения представленного системного блока. Происходит

инициализация базовой системы ввода-вывода представленного системного блока, затем происходит загрузка операционной системы, содержащейся в посекторной копии жесткого диска представленного системного блока.

4. Анализ первичной программной среды загруженной операционной системы. Под первичной программной средой понимается набор автоматически загружаемых системных и прикладных программ, запуск которых происходит при загрузке операционной системы (в том числе графического интерфейса операционной системы и содержимого стандартного начального каталога операционной системы, обычно называемого «Рабочий стол» операционной системы).

5. Составление перечня автоматически запускаемого при загрузке операционной системы программного обеспечения. Установление каталогов, в которых установлено указанное программное обеспечение, с целью однозначной идентификации расположения программ.

6. Определение класса и назначения автоматически запускаемого при загрузке операционной системы программного обеспечения путем идентификации (в случае если программное обеспечение известно по характерным признакам: наименование, расположение, структура входящих в состав файлов и иных характерных признаков), либо путем анализа неизвестного программного обеспечения (установление идентификационных признаков: наименования, размера и расположения исполняемых файлов, основных свойств исполняемых файлов, расположения, формата и содержимого файлов конфигурации, используемых ресурсов операционной системы и программного обеспечения и иных признаков, позволяющих в совокупности определить класс и назначение программного обеспечения).

7. Составление перечня, определение класса и назначения установленного на жестком диске представленного системного блока программного обеспечения (способом, аналогичным описанному в пп. 5-6 выше).

8. Выделение из общего перечня программного обеспечения, имеющегося на жестком диске представленного системного блока, программного обеспечения, соответствующего целям исследования.

9. Детальное изучение исходного кода выделенного программного обеспечения на предмет установления функционала (путем анализа исходного кода программного обеспечения – при его доступности, либо путем реверсивного анализа исходного кода программного обеспечения путем дезассемблирования – т.е. путем последовательного изучения команд, выполняемых процессором ПЭВМ в процессе работы запущенного программного обеспечения).

10. Определение функций, которые выполняются анализируемым программным обеспечением. Классификация функций по их цели: общеиспользуемые (встречаются в большинстве прикладного и системного программного обеспечения – работа с файлами, операции чтения и записи в файловую систему и оперативную память, работа с датой и временем и другие общеиспользуемые), специальные (специфичные для конкретного прикладного или программного обеспечения, как то – в совокупности обеспечивающие организацию и проведение азартных игр).

11. Выделение из специальных функций тех, которые по своей сути соответствуют действующему законодательству в области предмета проведения экспертизы (в частности, наличие генератора случайных или псевдослучайных чисел, специфичного для программ, предназначенных для организации и проведения азартных игр).

12. Проведение функционального тестирования выделенного программного обеспечения: выполнение всех доступных пользователю команд посредством графического интерфейса (при его наличии – путем нажатия на кнопки графического интерфейса с фиксацией происходящего после нажатия процесса, путем перехода по пунктам меню и/или ссылкам) либо посредством ввода команд в консоль (командную строку) программного обеспечения (если программное обеспечение это позволяет и эксперту известен набор поддерживаемых команд, в том числе в результате проведенного анализа исходного кода). В функциональное тестирование также входит анализ используемых выделенным программным обеспечением ресурсов – конфигурационных файлов, сетевых протоколов, способов передачи данных (сетевых, файловых, через оперативную память либо иных), способов и форм фиксации результатов своей работы (запись истории работы в файлы истории, запись истории работы в журнал работы операционной системы либо иных). Также в функциональное тестирование входит анализ функций программного обеспечения, которое аналогично выделенному – в тех случаях, если проведение полноценного функционального тестирования выделенного программного обеспечения на представленном системном блоке затруднено или невозможно (в частности, если для исследования выделенного программного обеспечения требуются специальные сведения – логины, пароли, ключи и аналогичные им) и если по характерным признакам гарантируется идентичность выделенного программного обеспечения аналогичному. К характерным признакам, на основе которых делается вывод об идентичности, относятся: идентичность файловой структуры программного обеспечения, идентичность конфигурационных файлов, идентичность исходного кода (при возможности) либо идентичность дезассемблированного исходного кода, идентичность содержимого информации

(информационных пакетов) и адресатов в процессе информационного обмена и иные совпадающие характерные признаки.

13. Составление аналитического отчета, описывающего общий алгоритм работы выделенного программного обеспечения (обеспечиваемых им функций, процессов и результатов).

14. Выключение представленного системного блока и уничтожение созданной посекторной копии жесткого диска представленного системного блока.

15. Формулирование выводов о функциональном и программном назначении выделенного программного обеспечения для достижения целей исследования.

Таким образом, в рамках данного исследования были рассмотрены основные проблемы анализа программно-аппаратных средств незаконной организации и проведения азартных игр, изучены несколько наиболее распространенных средств и обоснована методика их анализа. В современных условиях представляется важным дальнейшее развитие научных исследований в этом направлении, так как многообразие форм, видов, методов и средств незаконной игровой деятельности продолжает увеличиваться с каждым днем, что обосновывает острую потребность в проработанных и объективных методиках анализа.

Список литературы / References

1. Федеральный закон от 20.07.2011 № 250-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации».
2. Федеральный закон от 29.12.2006 № 244-ФЗ (ред. от 22.07.2014) «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации».
3. Пионтковский А.А. Вопросы общей части уголовного права в практике судебно-прокурорских органов. М.: Госюрнадзор, 1954. 130 с.
4. Аветисян Б.Р. К вопросу о соучастии при квалификации преступных деяний по статье 171.2 УК РФ / Б.Р. Аветисян // Правозащитник, 2015. № 3. С. 6.
5. Мосечкин И.Н. Объективная сторона незаконных организации и проведения азартных игр. / И.Н. Мосечкин // Фундаментальные исследования, 2015. № 2 (часть 14). С. 3210-3213.
6. Лихолетов А.А. Уголовно-правовые и криминологические проблемы противодействия незаконному игорному бизнесу: автореф. дис... канд. юрид. наук. Саратов, 2013. 27 с.
7. Чесноков Л.С. Административная и уголовная ответственность за незаконную организацию и проведение азартных игр. / Л.С. Чесноков // Советник юриста, 2011. № 10. С. 91-96.
8. Семенов Н.В., Замараева Н.А. Проблемы применения специальных знаний при расследовании преступлений, связанных с незаконной игровой деятельностью (статья 171.2. УК РФ «незаконные организация и проведение азартных игр») / Н.В. Семенов, Н.А. Замараева // Теория и практика судебной экспертизы, 2012. № 3 (27). С. 94-97.
9. Астахова Л.В., Волков А.В., Григорьев В.В. Методика анализа программно-аппаратных средств незаконной организации и проведения азартных игр в Российской Федерации / Л.В. Астахова, А.В. Волков, В.В. Григорьев // Наука, техника и образование, 2016. № 5 (23). С. 25-39.