УДК 343.985.2

И.В. Поддубный

К ВОПРОСУ ОБ ИСПОЛЬЗОВАНИИ ФИГУРАНТАМИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ЦЕЛЯХ СОКРЫТИЯ ХИЩЕНИЙ С БАНКОВСКИХ СЧЕТОВ ГРАЖДАН

В статье обосновывается актуальность исследования хищений с банковских счетов граждан, совершаемых с использованием информационно-коммуникационных технологий. Анализируются и кратко характеризуются основные информационно-коммуникационные технологии и приемы, используемые преступниками для маскировки преступной деятельности. Автором раскрывается термин «киберпреступление», в котором отражены основные признаки данного явления. На основе анализа официальной статистики экспонируется значительный рост преступлений рассматриваемой категории. Приводятся различные точки зрения на терминологию, касающуюся сокрытия преступления, а также маскировки преступной деятельности фигурантами. Приводятся основные методы и приемы маскировки злоумышленников в сети Интернет, такие как использование виртуальных частных сетей, шифрующих передаваемые данные и позволяющие подменять IP-адрес компьютерных устройств; прокси-серверов, которые при подключении становится посредником для выхода абонента в сеть Интернет. Уделяется внимание использованию socks-протоколов, с помощью которых обмен данных происходит по специальным протоколам. Отдельно исследуются проблемы раскрытия хищения с банковских карт, в ходе которых используются электронные денежные сервисы (Visa, QIWI, Wallet, WebMoney, Яндекс Деньги и др.), зарегистрированные на третьих лиц.

Ключевые слова: сокрытие, маскировка, фигуранты, банковский счет, электронные денежные средства, программы-вымогатели, хищение, анонимность, сеть «Интернет», информационные технологии.

DOI: 10.35634/2412-9593-2020-30-3-424-430

Динамичное внедрение новейших информационных технологий и коммуникационных средств в различные сферы деятельности современного общества привело не только к развитию позитивных явлений, но и выявило целый ряд негативных факторов. Совершенствование информационных и цифровых технологий, наращивание возможностей интернет-пространства создает благоприятные условия для совершения так называемых киберпреступлений.

Киберпреступление – это общее название для всех типов криминальной активности с использованием вычислительных машин и (или) Интернета. Киберпреступление может совершаться с помощью различных методов и инструментов, например, фишинг, вирусы, шпионское ПО, программы-вымогатели и социальная инженерия. Чаще всего оно совершается с целью кражи личных данных или финансовых средств. Есть все основания полагать, что именно преступность данного вида будет активно развиваться, влиять на развитие других преступлений и, возможно, порождать новые виды преступной деятельности. Также необходимо отметить, что быстрое развитие информационных технологий привело к возникновению новых способов противодействия расследованию преступлений.

В настоящее время для облегчения совершения преступлений, эффективного сокрытия преступной деятельности и своей личности преступники активно используют последние достижения в области информационных технологий.

Число зарегистрированных преступлений с использованием информационных технологий растет из года в год. Согласно отчету ГИАЦ МВД России, в январе – декабре 2019 г. было зарегистрировано 294,4 тыс. преступлений, совершенных с использованием информационно телекоммуникационных технологий, что на 68,5 % больше, чем за аналогичный период прошлого года. В общем числе зарегистрированных преступлений их удельный вес увеличился с 8,8 % в январе – декабре 2018 г. до 14,5 % в январе – декабре 2019 г. Практически все такие преступления (98,4 %) выявляются органами внутренних дел.

Почти половина данных преступлений (48,5 %) относится к категориям тяжких и особо тяжких: 142,7 тыс. (+149,0 %); половина (53,3 %) совершается с использованием сети «Интернет»: 157,0 тыс. (+45,4 %), более трети (39,5 %) – с использованием средств мобильной связи: 116,2 тыс. (+89,5 %).

Четыре преступления из пяти (80,0 %) совершаются путем кражи или мошенничества: 235,5 тыс. (+83,2 %), каждое двенадцатое (8,4 %) – с целью незаконного производства, сбыта или пересылки наркотических средств: 24,7 тыс. (+31,2 %) (официальный сайт МВД России).

Активное использование информационных технологий способствует видоизменению функциональной стороны преступления. К примеру, сегодня большое количество преступлений, связанных с хищением денежных средств граждан, которые ранее совершались «классическим» способом, теперь совершаются дистанционно, посредством использования достижений в области информационно-телекоммуникационных технологий. Особая распространенность хищений с банковских счетов граждан, совершаемых с использованием информационных технологий, а также постоянное совершенствование способов и приемов осуществления данной преступной деятельности требуют от правоохранительных органов постоянного изучения особенностей такого противоправного явления.

В своем выступлении заместитель министра внутренних дел Российской Федерации – начальник Следственного департамента МВД России генерал-лейтенант юстиции А.В. Романов заявил, что хищения, совершаемые с применением средств сотовой связи, сети Интернет, уголовные проявления в сфере телекоммуникаций и компьютерной информации – принципиально новый вид преступности. Методы конспирации злоумышленников, используемые ими способы и средства достижения корыстных целей, существенно отличаются от традиционных (цит. по: [1]).

Действия по сокрытию данного рода противоправных деяний препятствуют оперативному выявлению события преступления и установлению виновных лиц. Как правило, фигуранты преследуют цель − скрыть реальные данные, на основе которых субъект расследования может установить наличие или отсутствие признаков состава преступления, информацию о личности и реальном местонахождении преступника, а также любые обстоятельства, которые могут иметь доказательственное значение по делу и, соответственно, подтвердить виновность или невиновность лица.

Общепризнанным является понятие сокрытия преступления, предложенное Р.С. Белкиным, который определил содержание сокрытия через его способы как деятельность (элемент преступной деятельности), направленную на воспрепятствование расследованию путем утаивания, уничтожения, маскировки или фальсификации следов преступления, их носителей и преступника [2].

Под содержанием способов сокрытия понимается совокупность взаимосвязанных приемов сокрытия, обеспечивающих достижение поставленной цели. Содержательная сторона способа сокрытия важна для установления личности преступника, механизма осуществления противоправной деятельности, а также обнаружения следов преступления.

Р.С. Белкин выделил несколько способов сокрытия преступлений:

– утаивание информации и (или) ее носителей;

– уничтожение информации и (или) ее носителей;

– маскировка информации и (или) ее носителей;

– фальсификация информации и (или) ее носителей;

– смешанные способы, выражающиеся в различных инсценировках [2].

Маскировка, осуществляемая фигурантами, имеет место на всех стадиях совершения преступления, а также непосредственно после его реализации. Главная цель преступника состоит в передаче правоохранительным органам ложных, маскирующих данных с целью сокрытия истинной информации о преступном деянии.

Под маскировкой следует понимать действия или бездействие преступников или иных лиц, направленные на полное или частичное уничтожение, изменение, сокрытие следов подготавливаемого, совершаемого или совершенного преступления с целью введения в заблуждение, дезинформации как лиц, ведущих расследование, так и потерпевших, свидетелей относительно конкретных соучастников, способа совершения преступления, местонахождения трупа, предметов, добытых преступным путем, орудий преступлений и иных следов [3].

На сегодняшний день с помощью различного программного обеспечения и услуг, предоставляемых различными сервисами, у преступников появляется возможность эффективно скрывать необходимую информацию от субъекта расследования.

Использование при маскировке информационных технологий применяется преимущественно на стадии подготовки к совершению преступления, то есть само преступление еще не совершено, а маскировочные действия уже совершены. В данном случае цель злоумышленника – передать субъекту расследования ложную, маскирующую информацию с целью сокрытия истины. Одним из важнейших критериев маскировки преступников является соблюдение так называемой анонимности в сети, подразумевающее укрытие своих действий в сети Интернет и противодействие идентификации личности виновного.

Так, к информационно-технологическим средствам и приемам, используемым преступниками для маскировки противоправных деяний, относятся:

1) **использование технологии – VPN**. VPN – Virtual Private Network, то есть виртуальная частная сеть. Это сеть, работающая поверх сети Интернет. Она надежно шифрует передаваемые данные, позволяя скрыть реальный IP-адрес и поменять его на IP-адрес другой страны. IP-адрес (от англ. Internet Protocol Address) – уникальный идентификатор (адрес) устройства (обычно компьютера), подключенного к локальной сети или сети Интернет.

Принцип технологии заключается в создании поверх сети защищенного соединения (его можно назвать туннелем между компьютером и сервером). При соединении происходит шифрование и защита отправляемых данных. Использование VPN-соединения дает возможность безопасно направлять всю необходимую информацию через сервер, фактически установленный в любой точке мира. Данная технология позволяет скрыть реальный IP-адрес и защитить от попыток взлома и отслеживания передаваемых данных. Для использования VPN можно воспользоваться специальными VPN сервисами, такими как HotspotShield, TunnelBear, HideMe и др.;

2) **использование прокси-серверов (анонимных)**. Прокси-сервер (от англ. Proxy – право пользоваться от чужого имени) – удаленный компьютер, который при подключении к нему машины лица становится посредником для выхода абонента в сеть Интернет. Прокси передает все запросы программ абонента в сеть и, получив ответ, отправляет их обратно абоненту.

Как известно, уникальный IP-адрес присваивается каждому компьютеру, подключаемому к сети Интернет. Данный IP-адрес содержит данные о стране и регионе пользователя, данные о его провайдере и номере компьютера в сети самого провайдера.

Свой IP-адрес имеет также любой прокси-сервер, то есть, работая в сети Интернет, используя прокси сервер, пользователь остается анонимным, так как все запросы в Интернет будут осуществляться именно через прокси. Таким образом, информация, оставляемая в сети Интернет, будет содержать данные об IP-адресе прокси-сервера, а не абонента, выходившего в сеть.

Если проводить аналогию с VPN, то последняя в техническом плане более совершенна, VPN-соединение защищено качественней, так как используются различные методы шифрования и защиты утечек IP. Наряду с анонимным прокси-сервером существуют так называемые прозрачные прокси-серверы, которые не скрывают реальный IP-адрес пользователя, а лишь подменяют версии операционных систем, версии устройств и т. д. В отличие от VPN шифрование передаваемых данных пользователя не происходит.

Отдельно стоит отметить использование **socks-протоколов** (англ. socks – носки). Принцип действия очень схож с принципом действия прокси-сервера. Но главное отличие состоит в том, что обмен данных происходит по специальным протоколам, с помощью которых передача IP-адреса абонента становится невозможной (socks4, socks5 и т.д.).

Для использования прокси-сервера пользователь может воспользоваться специальными программами (утилитами), такими как PlatinumHide IP, ProxySwitcherPro, CCProxy, SafeIP, или подключиться через ручную настройку своего браузера (Браузер или веб-обозреватель – прикладное программное обеспечение для просмотра страниц, содержания веб-документов, компьютерных файлов и их каталогов; управления веб-приложениями, а также для решения других задач.);

3) **использование сайтов анонимайзеров**. Принцип действия сайтов анонимайзеров по принципу работы схож с прокси-сервером, исключение – наличие у сайта своего интерфейса. Пользователю необходимо зайти на сайт-анонимайзер и в адресной строке ввести адрес интересующей интернет-страницы, которую необходимо посетить анонимно. Обмен информацией будет проходить через сервер-анонимайзер, тем самым IP-адрес пользователя остается нераскрытым;

4) **использование распределенной сети Tor**. Tor (сокр. от англ. The Onion Router) – это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищенное от прослушивания. Рассматривается как анонимная сеть виртуальных тоннелей, предоставляющая передачу данных в зашифрованном виде. Иными словами, сеть Tor представляет собой систему, состоящую из тысяч компьютеров, распределенных по всему миру, которые используют одинаковое программное обеспечение и подключены друг к другу. Некоторые из этих компьютеров и являются узлами Tor, которые обеспечивают передачу информации внутри сети. Любое соединение клиента с каким-либо сайтом будет проходить минимум через три случайных узла (компьютера), крайний из

которых называется выходным, и Сайт, к которому обращается пользователь будет видеть IP-адрес конечного узла, а не компьютера пользователя.

Необходимость в специальных программах для смены статического адреса исключается. Браузер сам преобразует реальный адрес в фиктивный, а также блокирует потенциально опасные опции обычных браузеров – cookie, кэш, историю работы (фактически реализуя опцию «Инкогнито» в Google Chrome). Причем если информация передается по защищенному протоколу «HTTPS», то даже выходной узел сети не сможет увидеть передаваемые исходные данные;

5) **использование IP-телефонии.** 1 ноября 2019 г. министр внутренних дел Российской Федерации генерал полиции В. А. Колокольцев провел заседание коллегии МВД России, на котором среди новых угроз отметил мошенничество с использованием сотовой связи, а также средств IP-телефонии. Преступники научились подменять подлинные телефонные номера кредитных организаций, государственных служб и выдавать себя за их сотрудников. Использование IP-телефонии позволяет осуществлять подмену реального номера и совершать звонки через специальное приложение по протоколу IP, не требуя от звонящего наличия сотового телефона или подключения к базовой станции. Также в целях маскировки своих информационных данных и IP-номеров злоумышленники используют возможности информационно-телекоммуникационных технологий, обеспечивающих анонимность в сети Интернет, которые ранее были описаны в статье (TOR, VPN, и др.).

Следует отметить, что использование преступниками в целях маскировки IP-телефонии тесно связано с использованием специального метода добывания информации, получившего название «претекстинг». Под термином «претекстинг» подразумевается действие или, скорее, атака на гражданина, совершаемая по предварительно подготовленному сценарию (тексту) с целью получения определенных сведений или побуждения на выполнение конкретных действий. Претекстинг применяется не только при телефонных звонках, но и по различным мессенджерам (Skype, WhatsApp, Viber). Для реализации метода преступник должен заранее собрать как можно больше установочных данных об объекте – его имя, дату рождения, серию и номер его паспорта, марку и государственный номер личного автотранспорта, место жительства и (или) регистрации, место работы, сумму на счете и т. д.

Для реализации данного метода злоумышленник представляется другим лицом (сотрудником финансово-кредитного учреждения, родственником, государственным служащим и т.д.). Соблюдение данных условий вводит в заблуждение человека, позволяет преступнику войти в доверие и добыть необходимую информацию либо побудить к определенному действию.

Рассмотрим пример реализации данного метода: преступник осуществляет звонок на телефон потерпевшего и, представившись сотрудником банка, обращаясь к гражданину по имени, сообщает о том, что с его банковской карты была осуществлена попытка снятия денежных средств (или о еще какой-либо «подозрительной» операции). При этом преступник в диалоге специально проговаривает какие-либо личные данные гражданина, чтобы у потерпевшего не оставалось никаких сомнений в достоверности сообщаемых ему сведений. Далее, для того чтобы «решить» проблему, злоумышленник просит продиктовать все реквизиты банковской карты, включая CVV-код, расположенный на обратной стороне. Гражданин выполняет все требования звонящего, не сомневаясь, что разговаривает с работником банка. После получения необходимой информации о карте у злоумышленника появляется возможность осуществить хищение денежных средств с банковского счета гражданина;

6) **использование программного обеспечения для смены MAC – адреса (физического адреса).** MAC-адрес – это уникальный идентификатор, который присваивается каждой единице сетевого оборудования, позволяя идентифицировать каждую точку подключения, каждый узел сети и доставлять данные только для корректной передачи данных и предоставления услуг. Каждая сетевая карта имеет MAC-адрес, жестко прописанный производителем в его электронной начинке, он уникален для каждого производителя и устройства. MAC-адрес используется при организации доступа в Интернет или в какую-либо другую сеть. Изменить реальный MAC-адрес сетевой карты можно с помощью специальных программ, таких как TMAC, TECHNITIUM MAC ADDRESS CHANGER и др. С помощью данных программ можно также изменить MAC-адрес WIFI-адаптера;

7) **использование сервисов приема СМС-сообщений**. Использование сервисов, предоставляющих временный номер для приема СМС-сообщений, в настоящее время приобрело особую актуальность. Многие мессенджеры, известные социальные сети, интернет-магазины и прочие ресурсы сети стали проводить процедуру идентификации пользователя путем отправки специального кода на телефонный номер. То есть при прохождении процедуры проверки на указанный человеком номер

телефона будет отправлено СМС, содержащее проверочный код, который впоследствии нужно будет ввести для подтверждения авторизации.

В настоящее время существует множество сервисов, предоставляющих целый ряд мобильных номеров из диапазона операторов связи разных стран, с помощью которых можно зарегистрироваться на любом интересующем сайте, при этом не раскрывая свой настоящий номер. Воспользоваться данной услугой можно с помощью следующих сервисов sms-activate.ru, simsms.orgc, proovl.com и др.;

8) **использование для совершения преступления идентификационного электронного модуля (SIM – карты) абонента сотовой связи, зарегистрированного на третье лицо**. Используя подобные SIM-карты, преступник подменяет реальную информацию о лице, причастном к совершению противоправного деяния.

SIM-карты, зарегистрированные на третьих лиц, злоумышленники могут приобрести, к примеру, в интернет-магазинах, существующих в той же вышеупомянутой сети TOR, у недобросовестного представителя компании сотовой связи или в нестационарном пункте продажи, так называемой стойке, который может располагаться на вокзалах, в переходах между станциями метро.

Так, во время проведения совместного мероприятия управлением Роскомнадзора и МВД по Омской области 1 июля 2019 г. был установлен факт незаконной продажи SIM-карт. Документов, удостоверяющих личность абонента, продавец не требовал, и регистрации номеров на конкретных лиц по паспортам не происходило [4]. Также стоит отметить, что SIM – карту, оформленную на третье лицо, можно использовать в беспроводном модеме мобильной связи;

9) **использование сторонних беспроводных точек доступа в сети Интернет – Wi-Fi роутеров**. Бесплатный Wi-Fi в кафе, гостиницах, торговых центрах и других общественных местах уже давно перестал быть редкой услугой, сегодня это распространено повсеместно. Данной возможностью выхода в сеть Интернет зачастую пользуются и преступники, поскольку устройству злоумышленника будет присвоен IP-адрес Wi-Fi-роутера так же, как и всем остальным людям, пользовавшимся данной сетью Wi-Fi. Работа в сети путем подключения к «общественному» Wi-Fi зачастую осуществляется с использованием VPN;

10) **использование для получения / перевода денежных средств, банковских карт, оформленных на третьих лиц, электронных средств платежа и электронных денежных средств (Visa, QIWI, Wallet, WebMoney, Яндекс Деньги и др), использование криптовалют.**

Еще один из самых распространенных приемов, применяемых преступниками при осуществлении противоправной деятельности. С помощью банковской карты или банковского счета можно переводить деньги на электронный кошелек. Можно производить денежные переводы и безналичные расчеты в сети Интернет, осуществлять переводы на свою банковскую карту или расчетный счет с целью дальнейшего обналичивания [5].

В условиях современных реалий в качестве способа легализации денежных средств, полученных преступным путем, все чаще используется конвертация денежных средств в цифровую (виртуальную) валюту, что обусловлено в первую очередь отсутствием возможности контролировать оборот таких денежных средств.

Появление такой виртуальной валюты, как «криптовалюта» постепенно стало изменять процедуру финансовых расчетов, осуществляемых преступниками. В широком научном плане криптовалюта – это цифровые счетные единицы или, иными словами, децентрализованная конвертируемая валюта, основанная на математических принципах, которая защищена с помощью криптографических методов [6]. Криптовалюта – это цифровая (виртуальная) валюта, не имеющая физического выражения.

В настоящее время находить и эффективно использовать информацию об операциях с виртуальной валютой для выявления противоправной деятельности лиц, ее использующих, органам правопорядка не позволяет несовершенство правового регулирования. Поскольку анонимизировать личность и пользователя сети Интернет, и владельца виртуальной валюты не составляет труда, а оборот виртуальной валюты неподконтролен, выбор средств противодействия преступности в указанной сфере для правоохранительных органов крайне ограничен. Указанные обстоятельства в своей совокупности служат катализатором для процесса перехода финансовой деятельности преступников в виртуальную плоскость;

11) **использование сетевых псевдонимов для регистрации аккаунтов в социальных сетях**. Преступники, совершая преступления посредством использования социальных сетей (Вконтакте, Одноклассники и др.), зачастую полностью подменяют информацию о себе, в частности, имя (ник-

нейм), пол, возраст, место жительства и т.д. Также, помимо текстовой информации, может искажаться и графическая путем размещения в личном профиле фотографий третьего лица.

Приведенный выше перечень информационно-технологических средств и приемов, используемых преступниками с целью маскировки противоправной деятельности, не является исчерпывающим. В настоящее время наблюдается следующая тенденция: лица для осуществления преступной деятельности берут на вооружение новые появляющиеся функциональные возможности информационных технологий, которые позволяют им эффективно противодействовать правоохранительным органам и оставаться незамеченным.

Такие примеры свидетельствуют о том, что информационные технологии предоставили преступникам эффективные средства сокрытия преступлений, использование которых может кардинальным образом изменить ситуацию в негативную для субъекта оперативно-разыскной деятельности сторону. В сложившейся ситуации традиционные возможности преодоления противодействия расследованию могут быть неэффективными. Поэтому эффективное раскрытие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий невозможно без систематической разработки и внедрения новых тактических приемов и методов борьбы с данным видом преступной деятельности.

СПИСОК ЛИТЕРАТУРЫ

1. Фалеев М. Бандерлоги. Главный следователь МВД: каждое двенадцатое расследованное преступление – мошенничество // Российская газета. 2018. 9 апр. Федеральный выпуск № 75(7538). URL: https://rg.ru/2018/04/09/romanov-kazhdoe-dvenadcatoe-rassledovannoe-prestuplenie-moshennichestvo.html (дата обращения 15.01.2020).
2. Белкин Р.С. Криминалистика. Противодействие расследованию и пути его преодоления криминалистическими и оперативно-розыскными средствами и методами / Т.В. Аверьянова, Р.С. Белкин, Ю.Г. Корухов, Е.Р. Россинская // Криминалистика. М.: Норма: ИНФРА-М. М., 2002. С. 694.
3. Солодовник В.В., Тишкина Н.В. Понятие и способы маскировки преступления // Мир юридической науки. 2015. № 7. С. 71-76.
4. В Омске возбудили дело против гражданина, который продавал SIM-карты без регистрации. URL: http://kvnews.ru/news-feed/109912 (дата обращения 24.01.2019г.).
5. Колычева А.Н., Васюков В.Ф. Расследование преступлений с использованием компьютерной информации из сети Интернет: учеб. пособие / под ред. А. Г. Волеводза. М.: Проспект, 2020. 200 с.
6. Васюков В.Ф., Гаврилов Б.Я., Кузнецов А.А. Способы получения доказательств и информации в связи с обнаружением (возможностью обнаружения) электронных носителей: учеб. пособие. М.: Проспект, 2017. 160 с.

Поступила в редакцию 24.12.2019

Поддубный Илья Васильевич, адъюнкт 1-го курса кафедры оперативно-разыскной деятельности ОВД
Орловский юридический институт МВД России им. В.В. Лукьянова
302027, Россия, г. Орел, ул. Игнатова, 2
E-mail: ilyuha.poddubniy@yandex.ru

I.V. Poddubnyi

ON THE ISSUE OF THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES BY THE DEFENDANTS IN ORDER TO HIDE THE THEFT FROM THE BANK ACCOUNTS OF CITIZENS

DOI: 10.35634/2412-9593-2020-30-3-424-430

The article substantiates the relevance of the study of theft from Bank accounts of citizens committed using information and communication technologies. The main information and communication technologies and techniques used by criminals to disguise criminal activity are analyzed and briefly characterized. The author reveals the term "cybercrime", which reflects the main features of this phenomenon. Based on the analysis of official statistics, a significant increase in crimes in this category is exposed. Various points of view are given on the terminology concerning the concealment of the crime, as well as the masking of criminal activity by the persons involved. The main methods and techniques of masking intruders on the Internet, such as the use of virtual private networks that encrypt the transmitted data and allow you to substitute the IP address of computer devices, proxy servers, which when connected becomes an intermediary for the subscriber's access to the Internet. Attention is paid to the use of socks protocols, which allow data exchange using

special protocols. Separately, we study the problems of disclosure of theft from Bank cards, which use electronic money services (Visa, QIWI, Wallet, WebMoney, Yandex Money,

Keywords: concealment, disguise, theft, anonymity, "Internet", information technology.

Received 24.12.2019

Poddubnyi I.V., Associate of the 1st year of the Department of ORD ATS
Oryol law Institute of the Ministry of internal Affairs of Russia named after V.V. Lukyanov
Ignatova st., 2, Orel, Russia, 302027
E-mail: ilyuha.poddubniy@yandex.ru