КИБЕРПРЕСТУПНОСТЬ В СФЕРЕ КАРШЕРИНГА КАК НОВАЯ УГРОЗА СОВРЕМЕННОСТИ

Молчанова Виктория Андреевна

Цель: *выработка характеристики киберпреступности в сфере каршеринга, анализ данного вида преступления и формирование мер по противодействию киберпреступности в области каршеринговых услуг.*

Методология: *аналитический, сравнительно-правовой, формально-юридический методы, синтез.*

Выводы: *в результате проведенного исследования автор делает вывод, что каршеринг как относительно новый вид услуг становится новой нишей киберпреступности и нуждается в правовом регулировании: определении общих положений о каршеринге, его месте в транспортной инфраструктуре и стандартизации оказания услуг в данной сфере, в том числе определении мер защиты персональных данных и способов идентификации пользователей.*

Научная и практическая значимость: *по итогам исследования автор выявляет такую нишу киберпреступности, как киберпреступность в сфере каршеринга, формулирует ее понятие, признаки, дает подробную классификацию, описывает разработанные им меры по предупреждению возможных проявлений киберпреступности в сфере каршеринга в будущем, что может быть использовано для развития науки и совершенствования законодательства.*

Ключевые слова: *киберпреступность, каршеринг, предупредительные меры, личность киберпреступника, причины киберпреступности в каршеринге, криминология.*

Введение

Преступления в области киберпространства в XXI в. уже не редкость и мало у кого вызывают удивление. В феврале 2019 г. Генеральная прокуратура Российской Федерации сообщила, что количество киберпреступлений в России за шесть лет выросло почти в 16 раз – до 174 тысяч, из них расследовано около 43 тысяч *(См.: МВД в 2018 году было зарегистрировано // URL: https://www.novayagazeta.ru/news/2019/03/03/149695-mvd-v-2018-godu-bylo-zaregistrirovano-bolee-206-tysyach-kiberprestupleniy (дата обращения: 01.11.2019))*. Статистика в данной сфере является достаточно условной и не отражает полную картину происходящего, так как многие преступления данной категории либо не фиксируются, либо квалифицируются по другим составам правонарушений.

Исследуемая в данной работе разновидность киберпреступлений в сфере каршеринга мало разработана, в связи с чем не имеет достаточного массива информации и статистики для изучения, однако это не делает данную тему менее актуальной. Напротив, в настоящее время в связи с внедрением каршеринга в транспортную систему городов по всему миру преступность в данной области растет и вызывает опасения у современного сообщества.

Для начала стоит разобраться, что же из себя представляет каршеринг, с чем связано появление криминогенности в сфере каршеринга и какие уязвимые места можно выявить в данном виде транспортных услуг. Итак, каршеринг – это сервис краткосрочной аренды автомобиля с поминутной или почасовой оплатой. В систему московского каршеринга входят следующие операторы: «Делимобиль», Car5, YouDrive, BelkaCar, Яндекс. Драйв, др. В настоящее время стоимость аренды автомобиля варьируется в среднем от 8 до 11 руб. за минуту езды, в эту сумму входят затраты на

DOI 10.31085/2310-8681-2020-4-208-148-154

бензин, парковку и др. Для аренды автомобиля необходимо зарегистрироваться на сайте или в мобильном приложении каршеринговой компании. Для регистрации обычно необходимы фотография пользователя, копии паспорта и водительских прав, а также для оплаты услуг – сведения о банковской карте.

В России первые каршеринг-сервисы появились в 2013 г. В Москве начала работу компания AnyTime, а в Санкт-Петербурге – Street Car. Однако о возможности аренды автомобиля на несколько минут в нашей стране еще никто не знал, и активное развитие рынка каршеринга пришлось на 2015 г., когда был осуществлен запуск нового оператора московского каршеринга «Делимобиль», который стал активно сотрудничать с мэрией Москвы, получив для каршеринга льготные условия и тем самым пробив дорогу развитию новому для страны транспортному бизнесу. После этого на рынке каршеринговых услуг начали появляться новые игроки, что было связано с появлением спроса на новый вид транспортных услуг. Уже в 2016 г. свою работу начали такие операторы, как Car5 и BelkaCar. С 2017 г. в базах автопарков каршеринговых сервисов стали появляться автомобили премиального класса, что так же вызвало активный интерес со стороны пользователей.

Доступность данного вида транспортной услуги для широкого круга пользователей, простота в его использовании, удобство и его новизна привлекли большое количество клиентов, что и стало новой платформой для развития деятельности злоумышленников. Уже в 2017 г. СМИ начали «бить тревогу» по поводу появления новой угрозы – преступлений в области каршеринговых услуг. Публичный резонанс эта история приобрела не сразу, а с накоплением негласной статистики преступлений и покушений на их совершение. С каждым годом криминогенность обстановки в транспортной сфере услуг набирает все новые обороты. Однако этого еще недостаточно, чтобы выработать устойчивую статистику по данному вопросу и сформировать эффективные предупредительные меры.

Киберпреступность – это область преступлений, которая на данный период времени остается малоизученной и плохо поддается какой-либо аналитике. Большой интерес к данной проблеме проявляет современное научное сообщество, в том числе и криминологическое, о чем свидетельствует большое число публикаций, посвященных киберпреступности. Но во всех таких публикациях нет одного – сведений о более-менее реальном состоянии данного вида преступлений, так как получить такие сведения из общедоступных источников сбора эмпирической информации невозможно. Такими сведениями не располагают даже сотрудники специализированных оперативных подразделений правоохранительных органов, так как особый механизм совершения киберпреступлений относит их к числу не просто высоколатентных, а сверхвысоколатентных [1, с. 44–47].

Киберпреступления в сфере каршеринга можно определить как совокупность преступлений, совершаемых в сфере информационных технологий посредством использования интерактивных платформ операторов каршеринговых услуг.

Данную категорию преступлений можно охарактеризовать следующими общими признаками:

– высокая латентность;

– стремительный рост;

– удаленность преступника от преступления;

– анонимность преступления;

– анонимность преступника;

– доступность совершения преступления любым слоям населения;

– ощущение безнаказанности;

– кализионность правового регулирования;

– использование Интернета и других компьютерных сетей.

К разновидностям киберпреступлений в сфере каршеринга можно отнести следующие:

– создание фальшивых аккаунтов/взлом аккаунтов пользователей для аренды транспортных средств за чужой счет;

– взлом аккаунтов пользователей/создание фальшивых аккаунтов с дальнейшей их продажей третьим лицам;

– регистрация фальшивых аккаунтов/взлом аккаунтов пользователей для дальнейшего угона транспортного средства;

– кража персональных данных пользователей посредством взлома аккаунтов/сетевой платформы сервиса.

Следует дать краткую характеристику каждому выделенному виду киберпреступления в сфере каршеринга.

Создание фальшивых аккаунтов в приложениях операторов каршеринговых услуг сейчас является довольно распространенным явлением, так как защита приложений от такого рода мошенничества является ненадежной. Результаты проведенного опроса показали, что 60% респондентов считают систему приложений сервисов каршеринга уязвимой при регистрации аккаунтов. Дистанционность сотрудничества компаний с клиентами вызывает затрудненность идентификации насто-

ящего пользователя транспортным средством по договору краткосрочной аренды. К регистрации аккаунтов по персональным данным других лиц, полученных чаще всего незаконным путем, а также к взлому уже существующих аккаунтов прибегают для пользования каршерингом за счет третьих лиц (т.е. списание средств за поездку производится со счета лица, чьи данные указаны в мобильном приложении, а также списание денежных средств за нарушение ПДД). Кроме безвозмездности оказания услуг каршеринга злоумышленники могут преследовать и такую цель, как сохранение анонимности личности настоящего пользователя аккаунта. Связана данная потребность может быть со следующими факторами:

– отказ сервиса в предоставлении автомобиля для аренды;

– отсутствие прав на управление транспортным средством;

– недостижение 18-летнего возраста;

– занесение пользователя каршеринга в «черный список» оператора.

Взлом аккаунтов пользователей или создание фальшивых аккаунтов с дальнейшей их продажей третьим лицам является разновидностью киберпреступления коммерческой направленности. Подталкивает злоумышленников на совершение такого преступления имеющийся спрос среди потенциальных пользователей каршеринга, связанный с наличием определенных правил и запретов каршеринговых сервисов, предотвращающих доступ к услуге отдельных категорий лиц. Покупатели таких аккаунтов никак не застрахованы от проблем, которые в дальнейшем возникают в период их эксплуатации. Чаще всего при покупке аккаунта пользователя настоящий владелец замечает постороннюю активность в собственном аккаунте, а именно списание денежных средств и получение уведомлений об использовании транспортных средств каршеринговых сервисов. В дальнейшем владелец блокирует банковский счет и аккаунт в приложении, оставляя покупателя данного аккаунта «с рук» ни с чем. Многие такие пользователи даже не задумываются о происхождении продаваемых аккаунтов в сети и считают это вполне обычной практикой. Так, по результатам проведенного нами опроса 5,3% респондентов пользовались сторонним аккаунтом в сервисе каршеринга.

Угон транспортных средств каршеринговых сервисов в настоящее время набирает обороты. Злоумышленники используют различные методы для угона автомобилей, начиная от таких примитивных, как угон транспортного средства по месту его расположения, так и более изощренные – угон каршеринговых авто посредством регистрации фальшивых аккаунтов или взлома аккаунтов пользователей, в результате чего вычислить настоящего злоумышленника становится гораздо сложнее. Так, в 2012 г. из-за действий мошенников был вынужден прекратить свою деятельность американский стартап HiGear, который специализировался на каршеринге класса люкс. HiGear стал жертвой криминальной группы, которая за короткий срок угнала четыре автомобиля общей стоимостью $400 тыс. Мошенники использовали украденные водительские удостоверения и кредитные карты при регистрации аккаунтов *(См. Мошенники осваивают каршеринг: технологии и медиа: Газета РБК // URL: https://www.rbc.ru/newspaper/2017/09/07/59aec3869a7947b18eb23374 (дата обращения: 01.11.2019))*.

Многих пользователей услугами каршеринга в настоящее время волнует и такая проблема, как кража их персональных данных посредством взлома аккаунтов/сетевой платформы сервиса. Результаты проведенного нами опроса показали, что 40% респондентов считают использование каршеринга через приложения небезопасным. Были опрошенные, которые заявляли, что и сами становились жертвами злоумышленников, утратив доступ к своим аккаунтам в связи с компьютерным взломом. При этом треть пострадавших, сталкивались с этой проблемой не единожды. Все пострадавшие не получили должной поддержки от служб безопасности сервисов, а некоторые заявили об утечке своих персональных данных. Украденные персональные данные пользователей сервисов каршеринга находят различное применение в руках киберпреступников (списание средств с банковского счета, использование паспортных и водительских данных в своих целях). В связи с наличием угрозы такого характера 85,3% опрошенных видят острую необходимость в усовершенствовании системы безопасности приложений каршеринга от злоумышленников.

Каждая категория преступлений возникает неспроста и обусловлена характерными причинами их совершения. Изучив специфику киберпреступлений в сфере каршеринга, можно выделить причины социального, экономического, правового, организационного и технического характера.

Социальные причины:

– повсеместная и масштабная компьютеризация всех сфер общества (в том числе транспортной сферы);

– ненадежность мер безопасности каршеринговых услуг (возможность обойти систему защи-

ты персональных данных и персонализации аккаунтов) – посредством предоставления ложных данных с целью использования транспортного средства и перекладывания преступником персональной ответственности на владельцев аккаунтов;

– доступность и открытость услуг (способность использования непрофессиональным субъектом).

Экономические причины: быстрый и относительно безопасный способ получения выгоды (оплата услуг пользования транспортным средством за счет средств владельца аккаунта, оплата штрафов за нарушение ПДД владельцем аккаунта).

Правовые причины:

– несовершенство законодательства в области уголовной, административной ответственности (отсутствие составов преступлений, характерных для киберпреступлений в области каршеринга, иных приложений);

– высокая естественная латентность (латентность киберпреступлений составляет более 99%);

– отсутствие единых стандартов безопасности компьютерных программ (в т.ч. приложений).

Организационные причины:

– неполная квалификация преступлений в данной области (преступления в сфере компьютерной информации претендуют лишь на дополнительную квалификацию к основным киберпреступлениям – кражам (ст. 158 УК РФ), мошенничествам (ст. 159.6 УК РФ). Но в практической деятельности правоохранительных органов киберпреступления, как правило, квалифицируются только по основному составу;

– нехватка квалифицированных кадров правоохранительных органов, занимающихся расследованием киберпреступлений.

Технические причины:

– отсутствие надежных способов идентификации пользователя при каждом использовании услуг каршеринговых сервисов;

– ненадежность системы защиты электронных хранилищ персональных данных пользователей каршеринга.

Для выработки эффективных мер предупреждения киберпреступлений в сфере каршеринга необходимо не только понимать природу данного вида преступления, возможные механизмы махинаций и причины их совершения, но так же и определить категорию лиц, потенциально входящих в группу киберпреступников в данной области. Под личностью киберпреступника в криминологической науке понимается совокупность социально-демографических, нравственно-психологических и уголовно-правовых свойств личности, определяющих преступное поведение индивида, выражающееся в совершении киберпреступлений *(См.: Личность киберпреступника – криминология // URL: https://studme.org/155128/pravo/lichnost_kiberprestupnika (дата обращения: 01.11.2019)).*

По возрастным характеристикам наиболее криминально активными в киберпреступности являются возрастные группы 18–24 лет (39,6%) и 25–29 лет (30,6%). На возрастную группу 50 лет и старше приходится около 3% преступников от общего числа осужденных киберпреступников, что, видимо, связано с меньшей «компьютеризацией» лиц старшего поколения *(См.: Личность киберпреступника – криминология // URL: https://studme.org/155128/pravo/lichnost_kiberprestupnika (дата обращения: 01.11.2019)).*

Киберпреступников в изучаемой области можно классифицировать по различным основаниям, одним из которых является уровень профессиональности киберпреступника.

Первая категория киберпреступников относится к хакерам, специализирующимся на совершении отдельных категорий киберпреступлений, обладающих «профессиональными» техническими знаниями, необходимыми для совершения преступлений данного рода. Встретить данную категорию киберпреступников можно при взломе аккаунтов пользователей сервисов каршеринга с целью продажи данных аккаунтов, личного использования или кражи персональных данных пользователей с дальнейшим их использованием в различных целях.

Ко второй категории киберпреступников в зависимости от уровня профессиональной подготовки можно отнести среднестатистических пользователей сети Интернет, не обладающих какими-либо специальными знаниями в области киберпространства. К ним относятся лица, занимающиеся созданием фальшивых аккаунтов приложений сервисов каршеринга, то есть осуществляющих ввод в систему персональных данных других лиц или сведений с использованием поддельных документов с целью продажи таких аккаунтов или личного использования.

Также потенциальных киберпреступников в сфере каршеринга можно подразделить в зависимости от используемой среды преступления:

– киберпреступники, осуществляющие деятельность только в рамках киберпространства (создание фальшивых аккаунтов/взлом аккаунтов пользователей с их дальнейшей продажей третьим

лицам, кража персональных данных пользователей посредством взлома аккаунтов/сетевой платформы сервиса);

– киберпреступники, осуществляющие деятельность в киберпространстве в сочетании с преступными действиями в реальной жизни (создание фальшивых аккаунтов/взлом аккаунтов пользователей для аренды транспортных средств за чужой счет, регистрация фальшивых аккаунтов/взлом аккаунтов пользователей для дальнейшего угона транспортного средства).

Существенным криминогенным фактором психологического характера, присущим киберпространству, является возможность сохранения полной анонимности пользователя устройства или Сети (за исключением технической информации о подключении к Сети, способы сокрытия которой также существуют). Анонимность позволяет не только не быть идентифицированным в определенный момент времени, но также, как следствие, предоставлять о себе ложную информацию, вступать в социальное взаимодействие, представляясь другим лицом. Очевидно, что в условиях анонимности любой человек ощущает возможность безнаказанно совершать поступки отрицательного характера [2, с. 87–94]. Посредством анонимности киберпреступника и достигается высокий уровень латентности преступлений данной категории. Однако, сверхлатентными чаще всего являются преступления в сфере каршеринга при их совершении только в рамках киберпространства, то есть в данном случае злоумышленник не обличает себя. При совершении преступления в сфере каршеринга смешанных способом (в среде киберпространства с дальнейшим выходом в реальную среду) преступник повышает риск обнаружения самого себя. Однако по сравнению с рядовыми категориями преступлений в данной области (кража, угон) злоумышленник имеет бóльшую степень защищенности.

Также психологических фактором, характеризующим исследуемый вид киберпреступников, выступает фактор отстраненности от совершения данного вида преступления с последующей возможностью перекладывания ответственности на владельцев аккаунтов сервисов каршеринга за совершенные правонарушения. Примерами могут служить случаи взлома аккаунтов пользователей каршеринговых сервисов и использование их при аренде транспортным средств с дальнейшим их угоном или нарушением ПДД.

Таким образом, можно сделать вывод, что личность киберпреступника в сфере каршеринга обладает общими характерными чертами для киберпреступника в целом, однако имеет важные специфические особенности, обусловленные спецификой преступлений с области услуг каршеринга.

В связи с образовавшейся тенденцией появления и роста киберпреступности в сфере каршеринга необходимо выработать эффективные меры предупреждения преступлений в данной области. На данный момент времени официальная статистика по данной категории преступлений отсутствует, но сведения из источников средств массовой информации и результаты проведенного нами опроса свидетельствуют о наличии данного рода проблемы в обществе и необходимости с ней бороться уже на раннем этапе, пока киберпреступность в исследуемой области не приняла глобальные масштабы. Согласно опросу 50,5% респондентов встречались с информацией о случаях мошенничества в сфере каршеринга с использованием компьютерных технологий и Интернета или же сами становились жертвами данного вида преступности. Подавляющее большинство (85%) опрошенных убеждены в необходимости усовершенствования системы безопасности сервисов каршеринга для предупреждения преступлений в данной области.

Каршеринговые компании, сталкиваясь с угрозами безопасности своих сервисов, стараются бороться с данной проблемой собственными силами, локально предотвращая совершение преступлений или уже их последствия. Например, при подделке аккаунтов в мобильных приложениях и предоставлении ненастоящих персональных данных аккаунт пользователя может быть заблокирован, при каждой новой установке приложения на смартфон система требует заново загрузить фото паспорта, фото водительского удостоверения и дополнительно снимок, на котором изображено лицо и рядом развернутый паспорт.

Однако для эффективного предупреждения киберпреступлений в сфере каршеринга необходимо принять комплекс мер по различным направлениям деятельности. В первую очередь необходимо ввести правовое регулирование услуг каршеринга на федеральном уровне, а именно определить общие положения о каршеринге, его месте в транспортной инфраструктуре и стандартизировать оказание услуг в данной сфере, в том числе определить меры защиты персональных данных и способы идентификации пользователей.

Для создания рабочего механизма идентификации пользователей возможно внедрение следующих альтернативных друг другу механизмом.

Работа первого механизма основывается на установлении системы Face ID (сканера объемно-пространственной формы лица человека) для сличения реального пользователя автотранспортного средства и личности владельца аккаунта сервиса каршеринга внутри самих транспортных средств, предоставляемых операторами.

Второй возможный механизм идентификации пользователя каршеринга заключается в модернизации прошивки мобильных приложений с появлением функции обязательного фотографирования пользователя перед каждым использованием автомобиля. При этом пользователь сможет сделать фотографию только в онлайн режиме с исключением возможности загрузки фото из галереи мобильного устройства с целью предотвращения подлога. Автоматизированная программа будет сличать отправленное на сервер фото с ранее прикрепленным фото владельца аккаунта. В случае возникновения проблем при идентификации пользователя в связи с независящими от него обстоятельствами такое фото будет отправлено на ручную обработку оператора сервиса.

В каждой из представленных выше технологий есть как плюсы, так и минусы. К плюсам технологии Face ID, установленной внутри транспортного средства, относятся высокая точность идентификации лица, минимизация подлога (датчик может отслеживать личность водителя в течении всей поездки). Минусом такой технологии является ее дороговизна для операторов каршеринга, которым будет необходимо установить такие датчики в каждом автомобиле.

Сильной стороной модернизации прошивки мобильных приложений каршеринга выступает относительная бюджетность данного решения, однако минусом может стать заторможенность процесса обработки данных.

При внедрении таких мер защиты при идентификации личности необходимо учитывать фактор конкуренции каршеринговых компаний на рынке, так как при усложнении условий пользования каршерингом клиенты будут пользоваться услугами компаний с более простыми способами идентификации личности, что вытиснит конкурентов с более сильной системой защиты с рынка услуг. В связи с чем необходимо повсеместное установление единых способов идентификации пользователей каршеринга. Также это позволит не оставлять возможность для использования злоумышленниками компаний с более уязвимой системой защиты.

Для надежной защиты персональных данных возможно внедрение хранения информации посредством распределенной системы блокчейн, которая смогла зарекомендовать себя во многих областях хранения и использования информации.

Также в целях расследования преступлений в области киберпространства и их предотвращения необходима подготовка квалифицированных кадров правоохранительных органов всех уровней, чтобы добиться высокого уровня раскрываемости киберпреступлений, а также их предотвращения не только государственного масштаба, но и совершенных в отношении простых граждан. Для этого необходимо создать комплекс образовательных программ, на стыке гуманитарных и технических (информационных) наук с целью выпуска специалистов, способных в полной мере противостоять преступным проявлениям в киберпространстве.

Исследуемая тема в настоящее время приобретает архиактуальность, что непосредственно связано со стремительным развитием информационных технологий и внедрением каршеринга в транспортную логистику каждого современного города. Преступность также реагирует на изменения в обществе и моментально подстраивается под новые тенденции. К сожалению, такого же эффекта не достигается правовой системой и правоохранительными органами, для изменения которых необходимо время. В этом нет ничего удивительного, ведь только опытным путем можно установить все потенциально уязвимые места системы, каковой и стала индустрия каршеринговых услуг. Однако часто бывает, что ответная реакция на преступные проявления становится чрезмерно заторможенной, что и приводит к развитию негативных последствий для человека и общества в крупных масштабах. С целью предотвращения данного упущения мной было проведено исследование, в результате которого удалось выявить такую отдельную нишу киберпреступности, как киберпреступность в сфере каршеринга, обозначить ее понятие, признаки, виды с их характеристикой, разработать меры по предупреждению возможных проявлений преступности в дальнейшем, а также провести социологический опрос с целью выявления вовлеченности фокусной группы в обозначенную проблематику и определения окраски отношения респондентов к отдельным компонентам исследуемой области. Результаты опроса способствовали проведению объективного анализа состояния киберпреступности в сфере каршеринга в настоящий период времени и как следствие выработке мер реагирования на криминогенные проявления в данной области.

Литература

1. *Чекунов И.Г., Шумов Р.Н.* Современное состояние киберпреступности в Российской Федерации // Российский следователь. 2016. № 10. С. 44–47.

2. *Косенков А.Н., Черный Г.А.* Общая характеристика психологии киберпреступника // Всероссийский криминологический журнал. 2012. С. 87–94.

References

1. *Chekunov I.G., Shumov R.N.* Sovremennoe sostoyanie kiberprestupnosti v Rossiiskoi Federatsii [Modern condition of cybercrime in the Russian Federation]. Rossiiskii sledovatel' [Russian Investigator], 2016, no. 10, pp. 44–47. (In Russian)

2. *Kosenkov A.N., Chernyi G.A.* Obshchaya kharakteristika psikhologii kiberprestupnika [General characteristics of a cybercriminal's personality]. *Vserossiiskii kriminologicheskii zhurnal [Russian Journal of Criminology],* 2012, pp. 87–94. (In Russian, abstract in English)