Однако, по нашему мнению, невозможно будет детально урегулировать эту область отношений, ведь ввиду сложности подобных дел необходимо будет рассматривать каждый случай индивидуально в аспекте человеческого вклада и связи конечного результата (произведения) с конкретным лицом.

СПИСОК ЛИТЕРАТУРЫ

1. Artificial intelligence / Science Daily [Электронный ресурс]. Режим доступа: https://www.sciencedaily.com/terms/artificial_intelligence.htm (дата обращения: 03.03.2020).
2. Obvious. Nike designed with AI [Электронный ресурс]. Режим доступа: https://obvious-art.com (дата обращения: 03.03.2020).
3. Christie's sells AI-created artwork painted using algorithm for $432,000 [Электронный ресурс]. Режим доступа: https://www.dezeen.com/2018/10/29/christies-ai-artwork-obvious-portrait-edmond-de-belamy-design (дата обращения: 03.03.2020).
4. Гражданский кодекс Российской Федерации: часть четвертая: от 18.12.2006 № 230-ФЗ (ред. от 18.07.2019) // Собрание законодательства Российской Федерации. 2006. № 52 (ч. I). Ст. 5496.
5. Постановление Пленума Верховного Суда Российской Федерации от 23.04.2019 № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Бюллетень Верховного Суда Российской Федерации. 2019. № 7.
6. A philosopher argues that an AI can't be an artist [Электронный ресурс]. Режим доступа: https://www.technologyreview.com/s/612913/a-philosopher-argues-that-an-ai-can-never-be-an-artist (дата обращения: 05.03.2020).
7. Мохат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: дис. д-ра юрид. наук. М.: РГАИС. 2018.
8. Томаров И. Е. Творчество нейросетей сквозь PRISMA авторского права [Электронный ресурс]. Режим доступа: https://zakon.ru/blog/2016/6/30/tvorchestvo_nejrosetej_skvoz_prisma_avtorskogo_prava (дата обращения: 15.03.2020).
9. Лаптев В. А. Понятие искусственного интеллекта и юридическая ответственность за его работу // Право. Журнал Высшей школы экономики. 2019. № 2.
10. Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации» // Собрание законодательства Российской Федерации. 2019. № 41. Ст. 5700.
11. Синельникова В. Н., Ревинский О. В. Права на результаты искусственного интеллекта // Копирайт. 2017. № 4.
12. Гражданский кодекс РСФСР: утв. Верховным Советом РСФСР 11.06.1964 (утратил силу) // Ведомости Верховного Совета РСФСР. 1964. № 24. Ст. 407.
13. Артений Л. С. Искусственный интеллект в авторском праве // Вестник науки и образования. 2019. № 7 (61). Ч. 1.

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК СПОСОБ СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ

Д. А. Михайлова,
студентка ИГиП ТюмГУ,
направление «Юриспруденция»,
dariya.mihailova@mail.ru
Научный руководитель:
Р. В. Минин,
доцент кафедры уголовного права
и процесса ИГиП ТюмГУ,
кандидат юридических наук, доцент

Цифровизация внедряется во все сферы нашей жизни: в социальные взаимоотношения, экономику, культуру и политику. Новые технологии заметно упрощают существование современного человека. XXI век сложно представить без быстрого обмена информацией. С одной стороны, это удобно, с другой — безопасно. Обезопасить хранение информации в сети Интернет, на серверах и в программных продуктах — это то, к чему

стремятся люди. Поэтому злоумышленникам приходится придумывать новые способы получения интересующих их сведений. Они воздействуют на человеческую психику, используя методы из психологии и социологии, так называемые техники «социальной инженерии».

«Социальная инженерия» — метод собирания информации о человеке, основанный на психологическом воздействии. Данный способ актуален именно сейчас, так как определенную часть информации о себе и своем имуществе люди хранят в коммуникационной сети Интернет, на российских и зарубежных серверах. Доступ к таким сведениям, как правило, имеет только лицо, которое их выгрузило. Идентификация для получе- ния доступа проходит через пароли, логины, кодовые слова и вопросы. Такая система призвана обеспечить безопасность информации, чтобы третьи лица не могли ей неправомерно завладеть. Когда злоумышленники не могут использовать вредоносные компьютерные программы для получения чужой информации, они применяют разные методы: рассылают сообщения якобы от банка; звонят и представляются работником организации, создают подложные веб-страницы, присылают специальные интернет-ссылки. С помощью этого они завладевают необходимой информацией, а далее реализуют свои преступные намерения. В таком случае у правоприменителя появляется ряд вопросов: как квалифицировать данное деяние? Есть ли тут обман или злоупотребление доверием? Это преступления против собственности или преступления в сфере компьютерной информации?

Проблема данного исследования заключается в вопросе: как правильно квалифицировать деяние, совершённое с использованием «социальной инженерии»?

Цели научной работы: определить, что входит в круг понятия «социальная инженерия»; составить план правильной квалификации с учетом всех особенностей; составить памятку для добросовестных граждан, чтобы они знали, как действовать, если в отношении них собираются совершить преступление.

Метод исследования: анализ и синтез учебных и научных работ и сложившейся судебной практики; социальный эксперимент в форме опроса людей для учета распространенности данного способа совершения преступлений.

Актуальность выбранной темы обусловлена расширением понятия «социальная инженерия», из чего закономерно вытекают проблемы ее правильной квалификации правоприменителем. А граждане не всегда могут себя обезопасить, так как новые техники «социальной инженерии» рассчитаны на втирание в доверие.

Под термином «социальная инженерия» мы понимаем совокупность способов воздействия на поведение человека. Манипуляция происходит на чувствах и эмоциях человека, его страхах. При этом социальная инженерия включает в себя множество различных техник воздействия. Мы рассмотрим четыре самые популярные техники: фишинг, претексинг, «дорожное яблоко» и плечевой серфинг.

Фишинг (англ. fishing — рыбная ловля) представляет собой комплекс методов по получению конфиденциальной пользовательской информации (например, логин, пароль, верификационные коды, доступ к электронной почте, интернет-банкам и т. д.) [1; 25]. Самым распространенным в фишинге является рассылка через электронную почту писем, которые внешне напоминают письма от банков или компаний, которыми пользуется лицо. В социальном опросе, который мы провели для исследования проблемы, 54% отвечающих указали, что они переходят по ссылкам, указанным в электронных письмах или сообщениях. 16% не помнят, переходили они по ссылкам или нет. Только 30% не обращают внимания на такие сообщения.

В таких письмах получателя просят срочно перейти по указанной ссылке, иначе случится что-то ужасное (например, заблокируют счет). При переходе потерпевший попадает на «липовый» сайт, который с точностью скопирован с настоящего, не замечания изменения в адресной ссылке (например, sberdank.ru: не все могут заметить изменившуюся «b» на «d»). На таких сайтах люди оставляют свои личные данные, номера карт, кодовые слова, секретные коды, пароли и логины.

В данной ситуации встает вопрос о квалификации деяния. Уголовный кодекс Российской Федерации (далее — УК РФ) предусматривает ответственность за кражу (ст. 158 УК РФ), мошенничество (ст. 159 УК РФ), мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ) [2]. Обращаясь к диспозициям указанных

норм, невозможно дать деянию верную оценку. Здесь не обойтись без Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 [3]. В п. 21 Постановления Пленума сказано, что завладение чужим имуществом путем распространения ложной информации в сети Интернет, например с помощью создания поддельных сайтов, квалифицируется по ст. 159 УК РФ, а не по ст. 159.6 УК РФ. При этом в том же пункте указано, что независимо от способа получения данных об учетной записи пользователя и дальнейшего хищения имущества деяние квалифицируется как кража, если не было оказано воздействия на телекоммуни- кационную сеть. В приговоре Куйбышевского районного суда г. Омска от 11 июня 2019 года судья переквали- фицировал деяние виновного с пунктов «а», «в» ч. 3 ст. 159.6 УК РФ на п. «г» ч. 3 ст. 158 УК РФ [4]. Виновный — работник банка — имел доступ к счету потерпевшей в силу своего служебного положения. Потерпевшая проси- ла перевести все деньги, имеющиеся на счету у покойного супруга, на ее счет по завещанию. Подсудимый из имеющихся 20 тыс. рублей перевел клиентке только 10 тыс. рублей, заявив, что это вся сумма. Остальные 10 тыс. рублей он перевел себе на карту. Первоначальная квалификация деяния была по ст. 159.6 УК РФ. Во время судебного разбирательства судья, ссылаясь на п. 21 Постановления Пленума Верховного Суда от 30 но- ября 2017 года № 48, не согласился с указанной статьей. В своем обосновании переквалификации он указал, что изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться воздействием на программное обеспечение серверов, компьютеры или информационные сети.

Путаница в правоприменительной практике возникает из-за большого массива схожих по диспозиции норм. Для их правильного толкования необходимо обращаться к действующим постановлениям Пленума Верховного Суда.

Одной из техник «социальной инженерии» является ***претексинг***. При претексинге злоумышленник представляется другим лицом, например сотрудником банка. При этом самое интересное в том, что звонящий знает персональные данные потерпевшего. Это могут быть не только общедоступные данные: фамилия, имя и отчество, — но и кодовые слова, серия и номер паспорта, место его регистрации. Откуда они могут быть у преступника? Временами происходят разные скандалы, связанные с утечкой информации из банков и крупных организаций. В крупных компаниях работает огромное количество людей. Сотрудники, как правило, имеют доступ к информации о клиенте, его счетах, паспортных данных, кодовых словах. Такая информация активно продается на «черном рынке» [5]. При претексинге злоумышленники пользуются шоковой ситуацией, в которой оказывается гражданин: например, говорят, что банковский счет будет заблокирован через 15 минут из-за подозрительной транзакции. Потерпевшего вводят в заблуждение тем, что о нем уже знают персональную информацию, которой должен владеть только представитель организации. Поэтому обманутые граждане сообщают секретные коды из СМС и всё, что попросят, лишь бы не было никаких негативных последствий. В 2016 году было популярно звонить и представляться родственником, прося материальной помощи. И опять злоумышленники знали, какие отношения между людьми, могли назвать потерпевшего по имени, давили на близкую родственную связь. Такие действия следует квалифицировать как мошенничество по ст. 159 УК РФ, так как виновный обманом заставляет потерпевшего выдать информацию о себе, а после, с помощью получен- ных данных, совершает хищения имущества.

Проведенный социальный опрос показал, что с 20% людей связывались лица, которые пытались настойчиво вынудить их конфиденциальную информацию. При этом 30% опрошенных не помнят, чтобы с ними случалось что-то похожее. Один из респондентов ответил, что при проведении социального опроса у него пытались узнать его ФИО, место жительства, финансовое положение. Лица, которые не обращают внимания на подозрительные звонки, могут также не помнить, какие данные о себе они сообщили злоумышленникам. Это создает благоприятную почву для совершения преступлений.

Еще один метод получения информации о человеке — так называемое ***«дорожное яблоко»***. Суть данной техники заключается в том, что на улице или в общественном месте лежат диски или флеш-карты с интригующей надписью. Такая надпись вызывает у людей интерес. Ничего не подозревающий гражданин поднимает

электронный носитель информации и вставляет в свой компьютер. На таком диске обычно содержится вирусная программа, которая обходит антивирусную защиту компьютера. Цель программы — получить удаленный доступ к сведениям на устройстве. Например, такая ситуация: работник корпорации находит неизвестную флеш-карту в коридоре фирмы. Ему хочется узнать собственника карты памяти, и, чтобы это сделать, он вставляет ее в свой рабочий компьютер. Как выясняется, никаких видимых файлов на флеш-карте нет. Сотруд- ник забывает про нее, а через два дня со счетов корпорации пропадают все денежные средства. Схема такая: злоумышленники через вставленную карту памяти получили доступ к устройству сотрудника, через общую сеть фирмы они смогли выйти к компьютеру бухгалтера, составили от имени бухгалтера платежный документ и вывели деньги [6].

Опрос показал, что 30% респондентов взяли бы с собой заинтересовавший их диск и посмотрели его содержимое на своем персональном компьютере или принесли его на учебу или работу.

Квалификация в такой ситуации тоже вызывает много вопросов. В п. 20 Постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 указано, что вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации признаётся целенаправленное воздействие программных средств на серверы, компьютеры, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него [3]. В том же пункте постановления сказано: если виновный неправомерно получил доступ к компьютерной информации, то деяние подлежит дополнительной квалификации по соответствующим частям статей 272, 273 и 274.1 УК РФ. В указанных частях предусмотрены обязательные последствия: уничтожение, блокирование, модификация или копирование информации.

Что из этого подходит для техники «дорожное яблоко»? В Методических рекомендациях, утвержденных Генеральной прокуратурой Российской Федерации от 30 мая 2014 года, под модификацией понимается изменение компьютерной информации или ее параметров [7]. Когда виновные лица вносят данные о переводе денег на счет, который им подконтролен, они модифицируют существующие сведения на компьютере. Квалификация в данном случае должна быть по ч. 1 ст. 159.6 УК РФ при отсутствии квалифицирующих признаков по ч. 2 ст. 273 УК РФ (при отсутствии других квалифицирующих признаков).

Техника ***«плечевой серфинг»*** представляет собой получение лицом информации, которой гражданин пользуется прямо при нем. Например, в общественном транспорте человек через свой телефон заходит в онлайн-банк. Сидящий рядом смотрит на экран телефона и получает информацию о пароле, логине входа, может увидеть количество денежных средств на счетах. Далее такая информация используется для доступа к карте потерпевшего и для перевода денег на подконтрольные счета.

Проведенный опрос показал, что 80% людей считают, что их конфиденциальную информацию в мобильном телефоне или на компьютере могли видеть разные лица. 80% респондентов указали, что сами видели персональные сведения у другого человека в телефоне, когда тот об этом не знал. Про ситуации, когда кто-то открыто заглядывает в их мобильное устройство, опрошенные люди ответили следующим образом: 50% убрали бы свой телефон в карман, чтобы незнакомец ничего не увидел; 20% отвернулись бы в другую сторону; 20% продолжили бы сидеть, как и раньше, — их не волнует, что может увидеть рядом сидящий человек; 10% попросили бы его отвернуться.

Когда лицо намеренно собирает информацию о людях, чтобы в дальнейшем с ее помощью завладеть их имуществом, то это должно быть квалифицированно по соответствующим частям ст. 158 УК РФ, так как ли- цо не оказывает воздействия на программное обеспечение. Такой вывод содержится в п. 21 Постановления Пленума Верховного Суда от 30 ноября 2017 года № 48.

Статья 137 УК РФ предусматривает ответственность за незаконное собирание и распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия. Статья 138 УК РФ устанавливает уголовную ответственность за нарушение тайны переписки, телефонных пере- говоров, почтовых, телеграфных или иных сообщений граждан [2]. «Социальная инженерия» включает в

себя незаконное собирание информации о личной жизни потерпевшего, а также нарушение тайны переписки или иных сообщений. Вопрос о квалификации решается следующим образом: статьи 137 и 138 УК РФ — это способ техник «социальной инженерии», соответственно способ совершения кражи или мошенничества. Санкция за нарушение неприкосновенности частной жизни и нарушение тайны сообщений граждан меньше, чем за кражу или мошенничество. Поэтому дополнительной квалификации по ст. 137 УК РФ и ст. 138 УК РФ деяние не требует.

Вышеуказанные техники «социальной инженерии» совершаются только с прямым умыслом и корыстной целью. Виновное лицо желает завладеть чужим имуществом и распоряжаться им как своей собственностью.

Сегодня жизнь человека сложно представить без технических средств, коммуникационных сетей. Наличие гаджетов значительно упрощает существование: удобные переводы денежных средств через онлайн-банки, хранение информации о нас в собственных телефонах, быстрые бесконтактные системы оплаты. Чем больше человек доверяет свою жизнь компьютерным программам, тем более ему надо быть внимательным. Для этого мы разработали памятку для граждан, которая поможет не попасться на удочку злоумышленников (Приложение 1).

Техники социальной инженерии постоянно модифицируются, подстраиваются под мировые изменения. Новые методы усложняют уголовно-правовую квалификацию деяний. Правоприменители не всегда имеют возможность разобраться во всех нюансах конкретного преступления и дать ему правильную оценку. С этой целью мы разработали таблицу, в которой указана техника социальной инженерии и ее квалификация (Приложение 2).

СПИСОК ЛИТЕРАТУРЫ

1. Бахтеев Д. В. О некоторых современных способах совершения мошенничества в отношении имущества физических лиц // Российское право: Образование. Практика. Наука. 2016. № 3 (93) [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/o-nekotoryh-sovremennyh-sposobah-sovershеniya-moshennichestva-v-otnoshenii-imuschestva-fizicheskih-lits (дата обращения: 16.03.2020).

2. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ: по сост. на 18.02.2020 // Собрание законодательства Российской Федерации. 1996. № 25. Ст. 2954.

3. Постановление Пленума Верховного Суда Российской Федерации от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Бюллетень Верховного Суда Российской Федерации. 2018. № 2.

4. Приговор Куйбышевского районного суд города Омска от 11.06.2019 по делу № 1-220/2019 / СудАкт [Электронный ресурс]. Режим доступа: https://sudact.ru/ (дата обращения: 12.03.2020).

5. Солдатских В. Клиенты Сбербанка попали на черный рынок / Коммерсантъ [Электронный ресурс]. Режим доступа: https://www.kommersant.ru/doc/4111863 (дата обращения 12.03.2020).

6. Мазаев А. Думаете не дадите свои данные? / Privacy Policy [Электронный ресурс]. Режим доступа: https://lambda-it.ru/post/dumaete-ne-dadite-svoi-dannye (дата обращения: 12.03.2020).

7. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утвержденные Генеральной прокуратурой 30.05.2014 / Гарант.ру [Электронный ресурс]. Режим доступа: https://www.garant.ru/products/ipo/prime/doc/70542118/#review (дата обращения: 12.03.2020).

Приложение 1

ПАМЯТКА О РАЗНЫХ ТЕХНИКАХ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ	
Техника	**Как обезопасить себя**
Фишинг — распространение посред-	1. Не переходите сразу по указанной ссылке.

ством электронных писем ложных интернет-ссылок, выглядящих как ссылки на официальные сайты	2. Обратите внимание на адресную строку: прочитайте ее и убедитесь, что слово в строке соответствует оригинальному названию сайта (например, www.sberdank.ru — буква b изменена на d). 3. Позвоните в организацию, от которой Вам пришло письмо, и спросите, делали ли они такую рассылку. Найдите официальную почту организации и отправьте им полученное письмо для подтверждения его оригинальности. 4. Зайдите самостоятельно на сайт организации и обратитесь к указанному в рассылке разделу.
Претексинг — злоумышленник представляется сотрудником организации и с помощью этого получает нужную ему информацию	Если Вам звонит сотрудник банка и сообщает информацию, которая касается конкретно Вас: 1. Попросите его представиться: назвать ФИО, место работы, должность. 2. Спросите, откуда у него информация о Ваших персональных данных. (Много вопросов могут сбить злоумышленника с толку.) 3. Если Вам говорят, что надо срочно выполнить действия по инструкции, то зайдите на официальный сайт компании, найдите их номер и самостоятельно им позвоните. 4. Злоумышленники работают на запугивании — для них выгодно торопливать Вас и говорить, что через 15 минут уже всё пропало. Не поддавайтесь панике.
Дорожное яблоко — злоумышленники получают доступ к компьютерной информации через оставленные на улице диски и флеш-карты	Если Вы увидели на улице брошенный диск или флеш-карту: 1. Пройдите мимо. Для обеспечения безопасности других, если Вы не видели, кто оставил носитель информации, выбросите его. 2. Помните, с большой долей вероятности — там вирус, который обеспечит злоумышленникам доступ к Вашему компьютеру или ноутбуку.
Плечевой серфинг — злоумышленник получает ту информацию, которую лицо само демонстрирует в общественном месте (путем наблюдения)	Если вокруг Вас есть люди: 1. Обращайте внимание, смотрят ли они в Ваш телефон. Если да, не ведите важных переписок, не вводите свои личные данные для входа в аккаунт. 2. Попросите человека, который заглядывает к Вам в телефон (компьютер), отвернуться от Вас, или отвернитесь сами.

Приложение 2

ТАБЛИЦА ДЛЯ КВАЛИФИКАЦИИ	
Техника	**Квалификация**
Фишинг — распространение посредством электронных писем ложных интернет-ссылок, выглядящих как ссылки на официальные сайты	**Часть 1 статьи 158 УК РФ** (если нет квалифицирующих признаков) Объект: общественные отношения по охране права собственности; предмет: чужое имущество. Объективная сторона: деяние — тайное хищение чужого имущества, последствия — ущерб собственника или иного владельца; причинно-следственная связь; способ — создание подложных интернет-сайтов. Субъект: вменяемое физическое лицо, достигшее 14-летнего возраста. Субъективная сторона: прямой умысел; корыстная цель. См. п. 21 ПП ВС РФ от 30.11.2017 № 48

Претексинг — злоумышленник представляется сотрудником организации и с помощью этого получает нужную ему информацию	**Часть 1 статьи 159 УК РФ** (если нет квалифицирующих признаков) Объект: общественные отношения по охране права собственности; предмет: чужое имущество или право на чужое имущество. Объективная сторона: деяние — хищение чужого имущества, последствия — ущерб собственника или иного владельца; причинно-следственная связь; способ — обман или злоупотребление доверием (виновный выдает себя за сотрудника организации, которым на самом деле не является). Субъект: вменяемое физическое лицо, достигшее 16-летнего возраста. Субъективная сторона: прямой умысел; корыстная цель
Дорожное яблоко — злоумышленники получают доступ к компьютерной информации через оставленные на улице диски и флеш-карты	**Часть 1 статьи 159.6 УК РФ** (если нет квалифицирующих признаков) Объект: общественные отношения по охране права собственности; предмет: чужое имущество или право на чужое имущество. Объективная сторона: деяние — хищение чужого имущества, последствия — ущерб собственника или иного владельца; причинно-следственная связь; способ — вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Субъект: вменяемое физическое лицо, достигшее 16-летнего возраста. Субъективная сторона: прямой умысел; корыстная цель. **Часть 2 статьи 273 УК РФ** (если нет других квалифицирующих признаков) Объект: общественные отношения по охране компьютерной информации. Объективная сторона: деяние — создание и распространение вредоносных программ. Преступление окончено с момента создания компилированной вредоносной программы. Если виновное лицо не создавало вредоносной программы, то с момента распространения. Субъект: вменяемое физическое лицо, достигшее 16-летнего возраста. Субъективная сторона: прямой умысел и корыстная заинтересованность. См. п. 20 ПП ВС РФ от 30.11.2017 № 48
Плечевой серфинг — злоумышленник получает ту информацию, которую лицо само демонстрирует в общественном месте (путем наблюдения)	**Часть 1 статьи 158 УКРФ** (если нет квалифицирующих признаков) Объект: общественные отношения по охране права собственности; предмет: чужое имущество. Объективная сторона: деяние — тайное хищение чужого имущества, последствия — ущерб собственника или иного владельца; причинно-следственная связь; способ — собирание информации о потерпевшем с помощью наблюдательности. Субъект: вменяемое физическое лицо, достигшее 14-летнего возраста. Субъективная сторона: прямой умысел; корыстная цель. См. п. 21 ПП ВС РФ от 30.11.2017 № 48