УДК 343.791

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ

Е.А. Тарапанова, кандидат философских наук, доцент кафедры ИУ10 «Защита информации»
Л.Я. Добкач, студент кафедры ИУ8 «Информационная безопасность»
Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), Москва (Россия)

Ключевые слова: информационная безопасность; информационная безопасность личности; киберпреступность; преступления в сфере компьютерной информации; фишинг.

Аннотация: На развитие нашей страны оказывают влияние такие общемировые процессы, как интеграция и унификация информационных отношений. Формирование и развитие информационного общества должно сопровождаться соответствующим совершенствованием системы государственных гарантий конституционных прав человека и гражданина в информационной сфере.

В качестве одной из мер осуществления указанных прав выступает создание и обеспечение должного уровня информационной безопасности личности. Принятие новой Доктрины информационной безопасности Российской Федерации ставит интересы личности во главу нормативного регулирования в данной сфере, однако институт информационной безопасности личности по-прежнему недостаточно регламентирован действующим законодательством. Статья посвящена проблемам правового обеспечения информационной безопасности личности в условиях глобального информационного общества.

В частности, проанализировано состояние современной киберпреступности в России. Отмечается, что цель подавляющего большинства таких преступлений – посягательство на право собственности. Рассмотрены основные проблемы квалификации мошенничества в сфере компьютерной информации. В настоящее время в судебной практике мошенничество в сфере компьютерной информации рассматривается как форма хищения. Кроме того, проанализированы актуальные проблемы негативного воздействия глобального информационного пространства на личность, это воздействие особенно вредно для подрастающего поколения. В статье рассмотрены основные угрозы, которые представляют современные информационные технологии для уязвимой психики детей.

Проводится анализ состояния действующего законодательства Российской Федерации по вопросу обеспечения информационной безопасности личности. В заключение даны предложения, направленные на совершенствование правового обеспечения информационной безопасности личности.

ВВЕДЕНИЕ

Проблема информационной безопасности личности имеет большую значимость в условиях глобального информационного общества. Среди большого объема различной информации, с которой человек сталкивается каждый день, есть как полезная, так и вредная информация (или не содержащая в себе какого-либо потенциала вообще). Человек, не обладающий в достаточной степени развитым критическим мышлением, не способен адекватно оценивать современный мощный информационный поток с точки зрения его достоверности, полезности или вредности, актуальности и т. д., что отрицательно влияет не только на реализацию интересов человека в обществе, но и в конечном итоге на жизнь общества в целом.

На законодательном уровне понятия «вредная информация» пока не существует, частичная легитимация данного понятия произошла лишь благодаря вступлению в силу Федерального закона от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [1]. Таким образом, законодательно признано наличие вредной информации для детей, но общих норм о вредной информации в отечественном законодательстве пока нет. Согласно ст. 1 Федерального закона от 24.07.1998 № 124-ФЗ «Об основных гарантиях прав ребенка в Российской Федерации», дети – лица до 18 лет (совершеннолетия). Это далеко не самая обширная возрастная группа, но одна из наиболее уязвимых для воздействия вредной информации в силу особенностей психики и отсутствия необходимого жизненного опыта и знаний, так как «способ классификации воспринимаемого у каждого из нас тесно связан с нашим предварительным жизненным опытом» [2, с. 185].

В Доктрине информационной безопасности 2016 года, которая является основой для формирования государственной политики в области обеспечения информационной безопасности нашей страны, отмечается «нарастающее информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей». В последние годы в органы МВД поступает немало заявлений от родственников людей, которые попали под влияние различных деструктивных объединений – сект, так называемых «групп роста», «групп смерти» и прочих [3]. Деятельность секты, в отличие от обычной религиозной организации, имеет разрушительный и экстремистский характер, может быть связана с принуждением, насильственным воспитанием; зачастую деятельность секты нацелена на разрушение семьи, доведение до самоубийства и т. д. [4]. На законодательном уровне понятий «секта» или «деструктивное объединение» не существует. Большинство таких организаций, с точки зрения действующего российского законодательства, ничего не нарушает. Кроме того, сами пострадавшие, в силу разных причин и обстоятельств, не всегда обращаются в полицию. Поэтому привлечь к ответственности лидеров деструктивных объединений и их подельников очень сложно, целесообразно уделять соответствующее внимание превентивной работе. При этом особенно важны соответствующие превентивные меры среди подростков

и молодежи [5]. С одной стороны, люди попадают в различные деструктивные объединения добровольно. Но, с другой стороны, происходит подавление воли человека, смена его жизненных ценностей и ориентиров в интересах (как правило, финансовых и политических) лидеров таких групп. При этом в большинстве случаев представители различных деструктивных объединений ведут активную пропаганду, чтобы привлечь новых сторонников, с помощью Всемирной сети – социальных сетей и мессенджеров (мобильных приложений WhatsApp, Telegram, Viber и др.), и листовок и объявлений с соответствующей информацией и т. д.

Вследствие развития информационно-телекоммуникационных технологий Интернет стал для многих основным источником информации, он заменяет людям телевидение, журналы, газеты и во многом иные способы коммуникации с родственниками и друзьями – общение происходит преимущественно через мессенджеры и социальные сети (особенно у молодежи). В настоящее время «цифровые технологии для молодого поколения являются естественной, родной средой, в которой подростку намного проще найти для общения виртуального собеседника, чем познакомиться с реальным человеком в действительности» [6]. Кроме того, информационно-телекоммуникационные технологии развиваются интенсивно, что приводит к тому, что далеко не все многочисленные пользователи Интернета готовы противостоять этой достаточно агрессивной информационной среде.

Цель работы – исследование правовых аспектов информационной безопасности личности с учетом последних законодательных изменений.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ

В настоящее время государство принимает активное участие в регулировании интернет-пространства, при этом большое внимание уделяется проблеме размещения запрещенной информации на различных интернет-ресурсах. На основании анализа судебной практики можно сделать вывод о том, что в последние 5 лет прослеживается тенденция к увеличению роста числа исков об ограничении доступа к сайтам в сети Интернет. В частности, число заблокированных судами интернет-ресурсов составляет 24 203 (по состоянию на 13.08.2018) из 106 328 [7].

Постановление Правительства РФ от 27.10.2018 № 1279 «Об утверждении Правил идентификации пользователей информационно-телекоммуникационной сети «Интернет» организатором сервиса обмена мгновенными сообщениями» вступило в силу 06.05.2019. Теперь операторы мобильной связи должны фиксировать в своих базах, какими приложениями пользуются при переписке их клиенты, и присвоить каждому абоненту специальный идентификационный код. Согласно утвержденным правилам, администраторы мессенджеров обязаны проверять всех новых пользователей своих сервисов по номерам телефонов, а предоставлять им необходимую информацию должны операторы сотовой связи. На эту проверку отводится максимально 20 минут. Если сим-карта зарегистрирована на другого человека, пользователю могут отказать в регистрации [8; 9].

Следует отметить, что дети в силу возрастных особенностей психики быстро воспринимают как полезную, так и вредную информацию, при этом последствия влияния вредной информации на несовершеннолетних пользователей Интернета могут быть очень негативными [10]. Особую актуальность начиная с 2015 года приобрела проблема доведения до самоубийства путем вовлечения в так называемые группы смерти. Посредством сети Интернет лидеры деструктивных объединений организовали опасные для жизни игры, предлагали «увлекательные квесты» (например, внезапно пересечь дорогу перед приближающимися транспортными средствами, проехать, зацепившись за электропоезд, – так называемый «зацепинг», и т. п.), которые содержали в себе явный или скрытый призыв рисковать жизнью, в том числе призыв к самоубийству. В июне 2017 года в России впервые введена уголовная ответственность за доведение до самоубийства путем создания так называемых «групп смерти» в сети Интернет. Так, в ст. 110 Уголовного кодекса Российской Федерации «Доведение до самоубийства» теперь предусмотрена ответственность за все виды преступных действий по созданию и организации «групп смерти». Тогда же были включены в УК РФ и новые составы преступлений: склонение к совершению самоубийства или содействие совершению самоубийства (ст. 110.1 УК РФ); организация деятельности, направленной на побуждение к совершению самоубийства (ст. 110.2 УК РФ); вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего (ст. 151.2 УК РФ).

Деструктивные объединения могут пропагандировать религиозный экстремизм и терроризм, вербовать сторонников, что в итоге может привести к гораздо большим жертвам и потерям. Экстремизм и терроризм представляют собой явные угрозы для национальной безопасности Российской Федерации. Однозначного ответа, можно ли не поддаться пропаганде, не существует, многое зависит от каждого конкретного человека, особенностей его психики, уровня образования и воспитания, предварительного жизненного опыта, социума и множества других факторов. Уровень развитости той или иной личности определяется характером общественных отношений, в которых личность участвует. На основании вышеизложенного очевидно, что необходима нейтрализация и профилактика подобного деструктивного информационно-психологического воздействия, которое может не только принести значительный вред психическому здоровью граждан, но и способствовать дестабилизации социально-политической обстановки в целом.

Киберпреступников в первую очередь интересует не жизнь намеченных жертв, а их финансовые активы. Примерно 70 % их атак – это хищение денежных средств [11]. При этом киберпреступность причиняет огромный вред правам и законным интересам личности, обществу и государству [12]. Более того, ущерб от подобных преступлений приобретает все больший масштаб. Согласно отчету Генеральной прокуратуры РФ, за 2017 год количество преступлений в сфере информационно-телекоммуникационных технологий выросло на 37 %, из них 4,4 % приходится на Россию, т. е. это почти каждое 20-е преступление. За первое полугодие 2018 года количество преступлений по ст. 273 УК РФ выросло еще на 3,4 % и в 7 раз возросло количество мошеннических действий, совершенных с использованием электронных

средств платежа (ст. 159.3 УК РФ). Между тем за указанный период количество раскрытых преступлений стало меньше на 19,6 %, а количество нераскрытых преступлений увеличилось на 30,5 %. Эксперты утверждают, что такая тенденция сохранится и в будущем [13]. Таким образом, происходит активная криминализация киберпространства, поэтому стать жертвами киберпреступлений в настоящее время могут практически все пользователи программно-технических устройств, в том числе обычные держатели банковских карт и владельцы мобильных телефонов. Мощный и постоянно увеличивающийся функциональный потенциал современных вредоносных компьютерных программ делает возможным их применение в качестве орудий или средств совершения многих из известных действующему уголовному законодательству преступлений. Использование вредоносных компьютерных программ в корыстных целях делает преступную деятельность сверхдоходной и безопасной, так как киберсреда обеспечивает злоумышленникам скрытность преступных действий и при этом предоставляет практически свободный доступ к значительным материальным ресурсам [14].

В отечественном уголовном законодательстве киберпреступления представлены в ряде глав Уголовного кодекса РФ и в первую очередь – в главе 28 УК РФ «Преступления в сфере компьютерной информации» (ст. 272–274.1 УК РФ). Помимо ст. 272–274.1 УК РФ, уголовная ответственность за совершение преступлений непосредственно с использованием информационных технологий предусмотрена, в частности, в ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации», в ст. 159.3 УК РФ «Мошенничество с использованием платежных карт».

Фишинг – это вид мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам, паролям, данным лицевых счетов и банковских карт; в последние годы в сети Интернет он приобрел наибольшую популярность [15]. Данный вид мошенничества закрепленного в российском законодательстве определения не имеет. При фишинге непосредственный контакт между преступником и жертвой отсутствует. Основу фишинга составляют рассылка sms-рассылок, использование различного вредоносного программного обеспечения (скачивается при переходе по ссылке в адресованном жертве sms-сообщении), поддельных сайтов, создание компьютерных сетей (ботнетов), соединяющих незаметно для их владельцев большое количество компьютеров, зараженных программами-роботами, осуществляющими в интересах владельца ботнета нужные ему действия, например подбор паролей, рассылку рекламных сообщений, атаки на другие компьютеры.

Криптовалюта представляет собой новую революционную реалию не только в сфере информационных технологий, но и в экономике, при этом криптовалюта, как правило, похищается также посредством фишинга – с использованием фишинговых сайтов [16; 17].

Кроме того, все большее распространение получает голосовой фишинг. Например, злоумышленник звонит клиенту банка, представившись сотрудником финансовой организации, и под разными предлогами пытается получить реквизиты его банковской карты (номер, срок действия, CVR-код) в целях последующего осуществления мошеннических операций в Интернете. Как правило, такие звонки преступники реализуют через IP-телефонию. С помощью SIP-протокола звонки можно осуществлять посредством компьютера, установив соответствующую программу; через сети Wi-Fi или 3G/4G с помощью SIP-программ для планшетов и мобильных телефонов; используя специальный стационарный SIP-телефон, который включаются в роутер; через обычный телефон, подключив его к VoIP-шлюзу, а сам шлюз – к роутеру. Преступники также могут звонить с номера, очень похожего на номер колл-центра конкретной финансовой организации. Звонки также могут поступать с номеров 8-800, которые операторы IP-телефонии могут сдать в аренду на срок от одного дня.

Согласно данным ЦБ РФ, за 2018 год общий объем несанкционированных операций по выпущенным российскими банками платежным картам составил 1,4 млрд руб., что на 44 % выше показателя 2017 года – 961 млн руб. По данным регулятора, число выявленных несанкционированных транзакций по картам за год выросло почти на треть, до 417 тыс., а средняя сумма одной такой операции составила 3,32 тыс. руб. (на 9,6 % больше, чем в 2017 году). Также ЦБ РФ отмечается, что преступники для хищения денежных средств с платежных карт все активнее используют переводы через Интернет и мобильные устройства [18].

В 2017 году Верховный суд Российской Федерации в Постановлении № 48 от 30.11.2017 «О судебной практике по делам о мошенничестве, присвоении и растрате» (далее – Постановление Пленума ВС РФ № 48), подробно разъяснил правовые аспекты «мошенничества в сфере компьютерной информации» (ст. 159.6 УК РФ). Согласно этому Постановлению, фишинг следует квалифицировать как кражу, а не как мошенничество. Тем не менее квалификация фишинга по УК РФ представляет большую сложность.

Раскрываемость таких преступлений осложнена тем, что, во-первых, жертва электронной кражи узнает о пропаже денежных средств не сразу. Чем больше проходит времени с момента совершения такого преступления до обращения потерпевшего в правоохранительные органы, тем меньше шансов раскрыть преступление. Во-вторых, как правило, сайт-двойник существует недолго – максимум сутки. Кроме того, выявление подобных преступлений на стадии подготовки практически невозможно.

Следует отметить, что мошенники-фишеры в своей преступной деятельности ориентируются на человеческий фактор, то есть на беспечность и невнимательность потенциальных жертв, а также на эмоции, вызванные стрессовой ситуацией (например, звонок мнимого сотрудника банка, уведомляющий клиента о списывании всех денег с его банковской карты). Крупные организации стараются предупреждать своих клиентов об угрозе фишинговых атак: размещают на своих сайтах соответствующую информацию, сопровождают свои сообщения какими-либо доказательствами их подлинности и т. д. В настоящее время не существует гарантированной защиты от фишинга программными или программно-техническими средствами, поэтому необходимо быть осторожными, внимательно перепроверять сообщения, указанные в них гиперссылки и сайты, на которые предлагается перейти [19].

Близок к фишингу и подбор пароля, защищающего личные сведения владельца электронного носителя информации, взлом аккаунтов жертвы в социальных сетях и, что может привести к гораздо более серьезным последствиям, – учетных записей на различных порталах, в частности на портале государственных услуг, где указаны персональные данные граждан Российской Федерации, позволяющие им получать различные услуги, например, записаться на прием к врачу, поставить на учет и снять с учета автотранспортное средство и т. д. Следует отметить, что пользователи часто не придают должного внимания выбору надежного пароля, используя в качестве пароля самые примитивные комбинации: например, пароль может полностью совпадать с логином, состоять из даты рождения пользователя, из его имени и т. д. Некоторые пользователи после завершения сеанса работы на компьютере в общественном месте зачастую просто забывают выйти из почты, могут оставить записанные логин и пароль на видном месте.

Как правило, для защиты данных используются методы идентификации, аутентификации и авторизации. Идентификация заключается в присвоении уникального имени (номера, логина) пользователю, аутентификация – процесс проверки соответствия предъявляемых данных связанному с ними идентификатору, в случае успеха осуществляется авторизация пользователя в системе, разрешение войти на свою страницу. В большинстве случаев люди (как пользователи, так и разработчики) ограничиваются реализацией однофакторной аутентификации, обычно основанной только на принципе «то, что ты знаешь», то есть реализацией непосредственно парольной защиты. Мультифакторная аутентификация в целом и двухфакторная аутентификация в частности, использующая также принципы «то, что ты имеешь» и «то, чем ты являешься», распространены несколько меньше и во многих случаях сводятся все равно лишь к введению пароля.

Потенциально уязвимое место – пароль – становится целью злоумышленников. На то, чтобы определить его посредством перебора всех возможных вариантов, обычно тратится довольно много времени, в соответствии с формулой безопасности Андерсона

$$4{,}32 \cdot 10^4 \cdot k \cdot \frac{M}{P} \le A^l,$$

прямо зависящей от мощности алфавита A, количества попыток подбора пароля k в минуту, времени действия пароля M (в месяцах), обратно пропорционально вероятности подбора пароля P и экспоненциально его длине l [20]. Чтобы не тратить большое количество времени, преступники прибегают к уже рассмотренному выше методу социальной инженерии. В этом случае они крадут не финансовые активы жертвы, а ее аутентификационные данные. Иногда достаточно определить, что жертва считает для себя важным (чей-нибудь день рождения, чье-нибудь имя), или же она вообще не беспокоится о должной сложности пароля (123456, qwerty и их аналоги тому примеры). В остальных же случаях злоумышленник может достичь своей цели с помощью поддельных сайтов или управляемой беседы, направленной на выяснение пароля или же пользуясь невнимательностью и беспечностью жертвы. Основной метод защиты в данном случае аналогичен, как и при столкновении с фишерами: нужно быть внимательным, тщательно анализировать поступающую информацию и принимать взвешенные решения. При этом следует отметить, что формирование критического мышления требует от личности определенных усилий [21, с. 93].

Кроме того, нельзя не упомянуть и о тесной связи киберпреступности с самым опасным на сегодняшний день видом преступности – терроризмом. Террористические организации пользуются услугами профессиональных специалистов в сфере информационных технологий. Цель террористических организаций – нанести максимальный ущерб противнику, совершить теракты с большим количеством человеческих жертв и кибератаки на жизненно важные системы и военные объекты.

ВЫВОДЫ

В целях нейтрализации и профилактики деструктивного информационно-психологического воздействия на личность особенно важны соответствующие превентивные меры среди подростков и молодежи. Представляется целесообразным формировать и развивать у учащихся критичность мышления в рамках учебного процесса в средних и высших учебных заведениях. Личность, обладающая критичным мышлением, сможет более эффективно противостоять угрозам современной информационной среды.

Необходим действенный законодательный механизм защиты информационных прав и свобод и его постоянное совершенствование: профилактика преступлений и повышение процента их раскрываемости.

СПИСОК ЛИТЕРАТУРЫ

1. Куликова С.А. К вопросу о классификации вредной информации в российском законодательстве // Информационное право. 2015. № 4. С. 22–29.
2. Годфруа Ж. Что такое психология. Т. 1. М.: Мир, 1992. 496 с.
3. «Бог Кузя» и участники секты его имени вышли на свободу // РАПСИ. Российское агентство правовой и судебной информации. URL: rapsinews.ru/judicial_news/20190408/297497758.html.
4. Сибата Сэйги. Религиозные объединения в России и Японии: развитие законодательства в сравнительной перспективе // Конституционное и муниципальное право. 2018. № 4. С. 72–76.
5. Шерникова Д.А. Проблемы правового регулирования профилактики терроризма и экстремизма и их решение органами местного самоуправления // Муниципальная служба: правовые вопросы. 2018. № 4. С. 26–30.
6. Бураева Л.А., Дадова З.И. О проблемах негативного влияния глобального информационного пространства на процесс становления системы ценностей молодежи // Социально-политические науки. 2018. № 5. С. 270–272.
7. Омелин В.Н., Горовой В.В. Анализ судебной практики по блокировке интернет-групп в мессенджерах и страниц в социальных сетях // Уголовно-исполнительная система: право, экономика, управление. 2019. № 1. С. 8–11.

8. КонсультантПлюс: Новости для юриста с 6 по 9 ноября 2018 года из информационного банка «Юридическая пресса» // Консультант-Плюс: справочно-правовая система. URL: consultant.ru.
9. Колосова И.Ю. Новая обязанность оператора связи – идентификация пользователей // Услуги связи: бухгалтерский учет и налогообложение. 2019. № 1. С. 16–20.
10. Бородин К.В. Правовая защита несовершеннолетних от информации, приносящей вред их здоровью и развитию, распространяющейся в сети Интернет // Актуальные проблемы российского права. 2016. № 7. С. 68–74.
11. Кондрашин М. Security by design как основа // Банковское обозрение. 2018. № 11. С. 69–72.
12. Основные направления развития финансового рынка Российской Федерации на период 2019–2021 годов. М.: ЦБ РФ, 2019. 64 с.
13. О преступлениях, совершаемых с использованием современных информационно-коммуникационных технологий // Генеральная прокуратура Российской Федерации.
URL: genproc.gov.ru/smi/news/genproc/news-1431104.
14. Зубова Е., Тронин А. Киберпреступлений становится все больше, однако их раскрываемость уменьшается // Адвокатская газета. Орган Федеральной палаты адвокатов РФ. 2018. 13 ноября.
URL: advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/.
15. Григорян Г.Р. Об объекте мошенничества в сфере компьютерной информации // Российская юстиция. 2018. № 5. С. 29–31.
16. Тарапанова Е.А., Иванников П.В. К вопросу об организационно-правовом регулировании криптовалют и их реализация на базе отечественных стандартов информационной безопасности // Наукоемкие технологии. 2018. Т. 19. № 11. С. 58–64.
17. Сидоренко Э.Л. Криптовалюта как предмет хищения: проблемы квалификации // Мировой судья. 2018. № 6. С. 18–24.
18. Обзор несанкционированных переводов денежных средств за 2018 год. М.: ЦБ РФ, 2019. 31 с.
URL: cbr.ru/Content/Document/File/62930/gubzi_18.pdf.
19. Хачатурова С.С., Жихарева Ю.П. Осторожно, фишинг! // Международный журнал прикладных и фундаментальных исследований. 2016. № 4-4. С. 793–795.
20. Барбасова П.М., Зернов М.И. Система для смены паролей // Вычислительные сети. Теория и практика. 2010. № 1. С. 25–27.
21. Холодный Ю.И., Тарапанова Е.А. Информационно-психологическая безопасность, лженаука и критическое мышление // Социально-политические науки. 2018. № 5. С. 89–93.

REFERENCES

1. Kulikova S.A. Major Types of Harmful Information in the Russian Legislation: a Step to Classification. *Informatsionnoe pravo*, 2015, no. 4, pp. 22–29.
2. Godfrua Zh. *Chto takoe psikhologiya* [What is the psychology]. Moscow, Mir Publ., 1992. Vol. 1, 496 p.
3. “God Kuzya” and members of the sect of his name were released. *RAPSI. Rossiyskoe agentstvo pravovoy i sudebnoy informatsii*.
URL: rapsinews.ru/judicial_news/20190408/297497758.html.
4. Sibata Seygi. Religious associations in Russia and Japan: development of legislation in the comparative prospect. *Konstitutsionnoe i munitsipalnoe pravo*, 2018, no. 4, pp. 72–76.
5. Shernikova D.A. Issues of the Legal Regulation of Terrorism and Extremism Prevention and Their Solution by Local Self-Government Authorities. *Munitsipalnaya sluzhba: pravovye voprosy*, 2018, no. 4, pp. 26–30.
6. Buraeva L.A., Dadova Z.I. On the problems of the negative influence of the global information space on the process of youth value system formation. *Sotsialno-politicheskie nauki*, 2018, no. 5, pp. 270–272.
7. Omelin V.N., Gorovoy V.V. An Analysis of the Judicial Practice of Blocking Internet Groups in Messengers and Pages in Social Networks. *Ugolovno-ispolnitelnaya sistema: pravo, ekonomika, upravlenie*, 2019, no. 1, pp. 8–11.
8. ConsultantPlus: News for a lawyer from 6 to 9 November 2018 from the information bank “Legal Press”. *Konsultant-Plyus: spravochno-pravovaya sistema*.
URL: consultant.ru.
9. Kolosova I.Yu. New duty of the operator – identification of users. *Uslugi svyazi: bukhgalterskiy uchet i nalogo-oblozhenie*, 2019, no. 1, pp. 16–20.
10. Borodin K.V. Legal Protection of Minors from Harmful Information Spread via the Internet and Causing Harm to their Health and Development. *Aktualnye problemy rossiyskogo prava*, 2016, no. 7, pp. 68–74.
11. Kondrashin M. Security by design as a basis. *Bankovskoe obozrenie*, 2018, no. 11, pp. 69–72.
12. *Osnovnye napravleniya razvitiya finansovogo rynka Rossiyskoy Federatsii na period 2019–2021 godov* [Main directions of development of the financial market of the Russian Federation for the period of 2019–2021]. Moscow, TsB RF Publ., 2019. 64 p.
13. About crimes committed with the use of modern information and communication technologies. *Generalnaya prokuratura Rossiyskoy Federatsii*.
URL: genproc.gov.ru/smi/news/genproc/news-1431104.
14. Zubova E., Tronin A. Cybercrime is becoming more and more, but their detection is decreasing. *Advokatskaya gazeta. Organ Federalnoy palaty advokatov RF*, 2018, 23 November.
URL: advgazeta.ru/obzory-i-analitika/kiberprestupleniy-stanovitsya-vse-bolshe-odnako-ikh-raskryvaemost-umenshaetsya/.
15. Grigoryan G.R. About the object of fraud in the field of computer information. *Rossiyskaya yustitsiya*, 2018, no. 5, pp. 29–31.
16. Tarapanova E.A., Ivannikov P.V. Legal regulation of crypto-currencies and their implementation on the basis of national information security standards. *Naukoemkie tekhnologii*, 2018, vol. 19, no. 11, pp. 58–64.
17. Sidorenko E.L. Cryptocurrency as a Subject of Embezzlement: Qualification Issues. *Mirovoy sudya*, 2018, no. 6, pp. 18–24.
18. *Obzor nesanktsionirovannykh perevodov denezhnykh sredstv za 2018 god* [Review of unauthorized money

transfers for 2018]. Moscow, TsB RF Publ., 2019. 31 p. URL: cbr.ru/Content/Document/File/62930/gubzi_18.pdf.
19. Khachaturova S.S., Zhikhareva Yu.P. Beware of phishing! *Mezhdunarodnyy zhurnal prikladnykh i fundamentalnykh issledovaniy*, 2016, no. 4-4, pp. 793–795.
20. Barbasova P.M., Zernov M.I. Password change system. *Vychislitelnye seti. Teoriya i praktika*, 2010, no. 1, pp. 25–27.
21. Kholodnyy Yu.I., Tarapanova E.A. Information-psychological security, pseudoscience and critical thinking. *Sotsialno-politicheskie nauki*, 2018, no. 5, pp. 89–93.

INFORMATION SECURITY OF A PERSON

E.A. Tarapanova, PhD (Philosophy), assistant professor of Chair IU10 "Information protection"
L.Ya. Dobkach, student of Chair IU8 "Information security"
Bauman Moscow State Technical University (National Research University), Moscow (Russia)

Keywords: information security; information security of a person; cybercrime; computer crime; fishing.

Abstract: Such global processes as integration and unification of information relations influence the effective development of our country. The formation and development of information society must be accompanied by the appropriate improvement of the system of state guarantees of constitutional rights of a person and a citizen in the information sphere.

One of the measures necessary to ensure the execution of these rights is the creation and maintenance of the necessary level of information security of a person. The adoption of a new Doctrine of information security of the Russian Federation puts the interests of a person at the head of legal regulation in this sphere; however, the institute of personal information security still lacks the sufficient regulation in the current legislation. The paper deals with the problems of legal support of the information security of a person in the conditions of the global information society.

In particular, the authors analyzed the state of modern cybercrimes in Russia. They note that the aim of the great majority of such crimes is the entrenchment on the property right. The authors considered the main problems of classification of fraud in the cyber realm. Currently, in litigation practice, the fraud in the sphere of the cyber realm is considered as a form of kidnapping. Moreover, the authors analyzed the topical issues of the negative influence of global information space on a person; this influence is especially harmful for the younger generation. The paper considers the main threats, which the modern information technologies constitute for the vulnerable psychics of children.

The authors analyzed the state of the current legislation of the Russian Federation on the issue of providing personal information security. In conclusion, the authors give the suggestions aimed at the improvement of legal support of the information security of a person.