Марина Валериевна ЕГОРОЧКИНА,
ORCID 0009-0007-4050-9492
Краснодарский университет МВД России (г. Краснодар)
адъюнкт
mariegorochkina@yandex.ru

Научный руководитель:
Константин Викторович ОБРАЖИЕВ, доктор юридических наук, профессор, профессор кафедры уголовного права и криминологии Краснодарского университета МВД России

Научная статья
УДК 343.713:004(44)

УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ВЫМОГАТЕЛЬСТВО В ЦИФРОВОМ ПРОСТРАНСТВЕ ПО ЗАРУБЕЖНОМУ ЗАКОНОДАТЕЛЬСТВУ

КЛЮЧЕВЫЕ СЛОВА. Вымогательство, шантаж, искусственный интеллект, дипфейк, секс-вымогательство, отягчающие обстоятельства, уголовное законодательство Франции.

АННОТАЦИЯ. ***Введение.*** *В статье представлены результаты уголовно-правового анализа законодательства Французской Республики, предусматривающего ответственность за вымогательство, шантаж и сопряженные с ними преступления. Особое внимание уделяется способам совершения этих преступлений в случаях использования технологий искусственного интеллекта, программ-вымогателей и дипфейков. Целью проведенного автором исследования было формулирование выводов о целесообразности внедрения положительного опыта французского уголовного законодательства в России. Автор считает необходимым продолжать исследования в данной области, поскольку достижения правовой системы Франции по квалификации таких деяний, как вымогательство и шантаж, отвечают современным вызовам, связанным с противодействием преступности.* ***Методы.*** *В ходе исследования применялись методы анализа и синтеза, общенаучный диалектический метод познания окружающей действительности, сравнительно-правовой, формально-юридический и логический методы.* ***Результаты.*** *Механизм совершения вымогательства за последнее время претерпел значительные изменения. С развитием технологий искусственного интеллекта, компьютеризацией и цифровизацией практически всех сфер общественной жизни способы совершения противоправных деяний данного вида эволюционировали, что требует скорейшего реагирования со стороны законодателя в целях обеспечения защиты прав и свобод граждан. Подход уголовного законодательства Французской Республики к решению проблем квалификации вымогательства и шантажа, совершенных с использованием технологии искусственного интеллекта, по мнению автора статьи, отвечает современным потребностям противодействия преступности.*

ВВЕДЕНИЕ

Искусственный интеллект выводит на принципиально новый уровень развития абсолютно все сферы деятельности человека: медицину, искусство, промышленность, правоприменение и т.д. Его возможности доступны даже самым обычным пользователям сети Интернет, в том числе лицам, чьи намерения выходят за пределы, установленные законом. Такой инструмент в руках злоумышленника – крайне опасное высокотехнологичное оружие, противодействие которому требует от сотрудников правоохранительных органов специализированных знаний, умений и навыков.

Использование искусственного интеллекта (далее – ИИ) в противоправных целях порождает новые способы совершения преступлений различных видов. Интеграция прогрессивных возможностей компьютерных технологий в механизм преступной деятельности требует безотлагательных мер реагирования со стороны государства для защиты общества от вредоносного использования высоких технологий. Отмеченная тенденция затронула и такое традиционное преступление, как вымогательство. В цифровую эпоху оно приобрело новые формы. «Зарубежный опыт показывает, – отмечает А.Г. Уфалов, – что развитие искусственного интеллекта выводит совершение вымо-

Marina V. EGOROCHKINA,
ORCID 0009-0007-4050-9492
Krasnodar University of the Ministry
of Interior of Russia (Krasnodar, Russia)
Adjunct
mariegorochkina@yandex.ru

Scientific supervisor:
Konstantin V. OBRAZHIEV, Doctor of Law, Professor,
Professor of the Department of Criminal Law and Criminology
of the Krasnodar University of the Ministry of the Interior of Russia

CRIMINAL LIABILITY FOR EXTORTION IN THE DIGITAL SPACE UNDER FOREIGN LEGISLATION

KEYWORDS. Extortion, blackmail, artificial intelligence, deepfake, sextortion, aggravating circumstances, French criminal law.

ANNOTATION. ***Introduction.*** *The article presents the results of the criminal-legal analysis of the legislation of the French Republic, providing for liability for extortion, blackmail and related crimes. Particular attention is paid to the methods of committing these crimes in cases of using artificial intelligence technologies, ransomware and deepfakes. The purpose of the study was to formulate conclusions on the advisability of introducing the positive experience of French criminal legislation in Russia. The author believes it is necessary to continue research in this area, since the achievements of the French legal system in qualifying such acts as extortion and blackmail meet modern challenges associated with combating crime.* ***Methods.*** *The study used methods of analysis and synthesis, the general scientific dialectical method of cognition of reality, comparative legal, formal legal and logical methods.* ***Results.*** *The mechanism of extortion has recently undergone significant changes. With the development of artificial intelligence technologies, computerization and digitalization of almost all spheres of public life, the methods of committing illegal acts of this type have evolved, which requires a prompt response from the legislator in order to ensure the protection of the rights and freedoms of citizens. The approach of the criminal legislation of the French Republic to solving the problems of qualifying extortion and blackmail committed using artificial intelligence technology, according to the author of the article, meets the modern needs of combating crime.*

гательства в мире на новый уровень. В различных обществах и странах, где всё записывается, … данные, относящиеся к лицам или голосам людей, как правило, продаются в Интернете. В результате развитие ИИ заставляет исследователей, законодателя реагировать на новые вызовы»[1].

МЕТОДЫ

В ходе исследования, результаты которого представлены в настоящей статье, применялся общенаучный диалектический метод познания окружающей действительности. Он был необходим для полного отражения мер, принимаемых для противодействия совершению вымогательства в цифровой среде. Кроме того, использованы общенаучные методы анализа и синтеза, которые позволили детально изучить дифференциацию действий, связанных с вымогательством и шантажом, совершаемыми в цифровом пространстве. Из числа частнонаучных методов были востребованы формально-юридический и логический методы. Для исследования законодательства Французской Республики применялся сравнительно-правовой метод.

РЕЗУЛЬТАТЫ

В поисках эффективных уголовно-правовых инструментов противодействия вымогательству целесообразно обратиться к опыту зарубежных государств с развитой цифровой средой, которые первыми столкнулись с новыми проявлениями данного вида преступности. Особый интерес в этом плане представляет уголовное законодательство Французской Республики, которое довольно гибко реагирует на актуальные криминальные угрозы, связанные с вымогательством.

Согласно ст. 312-1 Уголовного кодекса Французской Республики (далее УК Франции), под вымогательством понимается акт получения путем насилия, угрозы насилия или принуждения либо подписи, обязательства или отказа от обязательства, либо секретной информации, либо денежных средств, ценных бумаг, материальных ценностей или любого иного имущества. Санкция за совершение данного преступления предусматривает семь лет лишения свободы и штраф в размере 100 тысяч евро. Это преступление относится к категории средней тяжести как по французскому законодательству[2], так и по российскому.

Интересно отметить, что во Франции законодательно закреплено освобождение виновного от наказания за попытку совершения вымогательства в составе организованной группы, если он уведомил административный или судебный орган и

[1] Уфалов А.Г. Проблемы совершенствования уголовно-правового регулирования ответственности за вымогательство и шантаж: Дисс. … канд. юрид. наук. Саратов, 2003. 170 с.
[2] Уголовный кодекс Франции // Legifrance. Droit national en vigueur. Codes: Code pénal // URL: https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006070719/2024-09-30/.

это позволило предотвратить совершение преступления и выявить, при необходимости, других исполнителей или соучастников (п. 1 ст. 312-6-1 УК Франции).

В уголовном законе Франции закреплены следующие отягчающие обстоятельства вымогательства:

- если оно сопровождается насилием, которое приводит к полной нетрудоспособности потерпевшего на срок до восьми дней (п. 1 ст. 312-2);
- если посягательство совершено во вред лицу с особой уязвимостью, которая может быть обусловлена возрастом, болезнью, физическим или психологическим недостатком, состоянием беременности, что очевидно или известно виновному лицу (п. 2 ст. 312-2);
- когда вымогательство совершено тем, кто намеренно скрывает свое лицо полностью или частично, чтобы не быть опознанным (п. 3 ст. 312-2);
- когда вымогательство совершается в учебных заведениях или учреждениях образования, а также при входе или выходе учащихся, или в непосредственной близости от них, на прилегающей территории этих учреждений (п. 4 ст. 312-2);
- если вымогательству предшествует, сопровождает его или следует за ним насилие, приводящее к полной нетрудоспособности на срок более восьми дней (ст. 312-3);
- в случае, когда вымогательство связано с применением или угрозой применения оружия, или осуществляется лицом, имеющим при себе оружие, на которое требуется разрешение или ношение которого запрещено (ст. 312-5);
- осуществление вымогательства в составе организованной группы (п. 1 ст. 312-6);
- если вымогательству предшествует, сопровождает его или следует за ним насилие, приводящее к увечью или стойкой инвалидности (п. 2 ст. 312-6);
- если ему предшествует, сопровождает его или следует за ним насилие, повлекшее смерть, пытки или варварские действия (ст. 312-7).

Санкции по перечисленным квалифицированным составам преступлений варьируются от десяти лет лишения свободы до пожизненного заключения, а размер штрафа может достигать 150 тысяч евро. Это подчеркивает, что государство видит высокую степень общественной опасности таких деяний и необходимость защиты от подобного рода посягательств наиболее уязвимых потерпевших [1, с. 208; 2, с. 93].

Существенное отличие понятия вымогательства, используемого во Франции, от закрепленного в российском уголовном законодательстве подчеркивает А.Р. Адельханян. Он указывает на то, что, согласно французскому представлению о вымогательстве, субъект преступления, применяя насилие, может требовать немедленной передачи имущества, а высказываемые им угрозы могут быть реализованы незамедлительно. С точки зрения Уголовного кодекса Российской Федерации (далее – УК РФ) такие преступные деяния выходят за рамки вымогательства и квалифицируются как разбой или грабеж[1].

Возвращаясь к вопросу о новых механизмах совершения преступлений рассматриваемого вида, следует обратить внимание на противоправные действия, осуществляемые посредством использования так называемых программ-вымогателей, в основе которых лежит вредоносное программное обеспечение – компьютерный вирус, блокирующий работу компьютера до тех пор, пока пользователь не выполнит требования злоумышленника, как правило, заключающееся в переводе денежных средств, криптовалюты и т.д. [3, с. 4].

В течение последнего десятилетия во Франции программы-вымогатели широко используются для шантажа, когда хакер утверждает, что у него есть компрометирующие потенциальную жертву видеозаписи или изображения. Стратегия вымогателя, играющего на страхе жертвы, состоит в рассылке повторяющихся электронных писем, содержащих информацию о наличии у него неблагоприятных сведений об адресате, с целью заставить его поверить в то, что компьютер и доступ к веб-камере были взломаны, а изображения, на которых он находится в деликатном положении, скачаны и сохранены злоумышленником. Далее, как правило, вымогатель выдвигает требования о передаче денежных средств (чаще всего в биткойнах), угрожая разослать эти изображения по адресам из списка личных контактов потерпевшего и/или разместить их в сети Интернет [4, с. 942]. Впоследствии выясняется, что для совершения вымогательства пароли были взломаны или найдены в базах данных в даркнете (скрытом сегменте Интернета) [5, с. 93]. Лица, утверждающие, что у них есть видеозаписи или иные компрометирующие изображения жертвы шантажа, часто предлагают адресату перейти по ссылке, чтобы убедиться, что это действительно так. На самом деле потерпевший получает файл с заархивированным контентом. В случае распаковки такого архива на устройство автоматически устанавливается программа-вымогатель, и далее начинается реализация описанной выше схемы преступления [6, с. 251-252].

Данные, опубликованные на официальном сайте газеты «Le Figaro» в разделе «Общество»[2], свидетельствуют о росте во Франции числа случаев вымогательства и шантажа, совершаемых с использованием угроз, носящих сексуальный характер, в целях получения материальной выгоды. Для описания подобных случаев применяется термин секс-вымогательство. Проблема секс-вымогательства, осуществляемого с использованием информационно-коммуникационных технологий, включая искусственный интеллект, становится всё более актуальной, особенно для несовершеннолетних. Во Франции законодатель активно реагирует на этот вызов [7, с. 187]. Так, в 2020 году в уголовный закон были внесены изменения, которые ужесточили наказания за

[1] Адельханян А.Р. Имущественные преступления и проступки по Уголовному кодексу Франции (уголовно-правовой и сравнительный анализ): Дисс. … канд. юрид. наук. М., 2007. 150 с.
[2] Le Figaro // URL: https://www.lefigaro.fr/actualite-france/cyberattaques-le-risque-s-accroit-avec-les-tensions-geopolitiques-20240705.

сексуальное насилие и шантаж, совершаемые в отношении несовершеннолетних. В 2021 году установлена ответственность за требования со стороны совершеннолетнего лица, обращенные к несовершеннолетнему, о распространении или передаче изображений, видеозаписей или других материалов порнографического характера с этим несовершеннолетним (ст. 227-23-1 УК Франции). Следует обратить внимание на то, что возраст потерпевшего и совершение преступления в организованной группе признаются отягчающими обстоятельствами[1].

Вместе с тем необходимо иметь в виду, что вымогательство может быть сопряжено с другими преступлениями. Это осложняет деятельность правоохранительных органов по его выявлению и раскрытию.

В последнее время во Франции активно развиваются правовые средства, позволяющие сдерживать распространение вымогательства и шантажа и привлекать виновных к уголовной ответственности. Рассматривая вопрос сопряженности преступлений, необходимо подчеркнуть, что во французском законодательстве вымогательство и шантаж – преступления разных видов, ответственность за них предусмотрена разными нормами. Под шантажом понимается акт, направленный на получение путем использования угрозы раскрытием или вменением в вину фактов, способных причинить ущерб чести и достоинству, либо подписи, обязательства или отказа от обязательства, либо конфиденциальной информации, либо денежных средств, ценностей или любого имущества (ст. 312-10 УК Франции). В то же время ст. 132-16 УК Франции устанавливает, что вымогательство и шантаж являются однородными преступными деяниями, и при совершении одного из них, а затем другого возникают основания для признания рецидива. Такой подход оправдан, поскольку вымогательство и шантаж имеют общую цель: заставить потерпевшего дать преступнику то, чего он требует [8, с. 74]. Необходимо заметить, что, по сути дела, с точки зрения российского уголовного права шантаж – это разновидность вымогательства.

В данном контексте социальные сети представляют собой идеальную среду для выдвижения требований с корыстной целью под угрозой разоблачения, обвинения, клеветы и т.д. [9, с. 295]. Французское уголовное законодательство предоставляет пользователям социальных сетей, столкнувшимся с шантажом, возможности эффективно защищать себя. Во-первых, за совершение шантажа предусмотрено строгое наказание в виде пяти лет лишения свободы и штрафа в размере 75 тысяч евро. Для сравнения: санкция статьи российского уголовного закона, закрепляющей ответственность за совершение аналогичного деяния, предусматривает лишение свободы на срок до четырех лет и штраф в размере до 80 тысяч рублей. Во-вторых, шантажист не может оправдать свои действия, ссылаясь на истинность фактов, которые он угрожает раскрыть, даже если они изобличают потерпевшего в противоправной деятельности. В-третьих, попытка шантажа сама по себе наказуема, поскольку считается оконченным преступлением, таким образом, даже если потерпевший не поддался угрозам, шантажист всё равно должен быть наказан. Норма, закрепленная ст. 312-9 УК Франции, определяет, что покушение на вымогательство и шантаж наказывается так же, как и оконченные преступления. Формулирование усеченного состава в данном случае демонстрирует сходство позиций французского и российского законодателей.

Возвращаясь к вопросу о квалификации действий секс-вымогателей и шантажистов в сети Интернет, необходимо рассмотреть, какие объекты преступного посягательства подлежат дополнительной защите с точки зрения законодательства Франции. За реализацию преступного умысла, выражающегося в распространении в сети видео, созданного или скачанного для использования в качестве инструмента давления на жертву, виновные могут быть привлечены к ответственности по совокупности по ст. 226-1 УК Франции за посягательство на неприкосновенность частной жизни, за которое установлено наказание в виде лишения свободы на срок до одного года и штрафа в размере до 45 тысяч евро.

В то же время за производство, импорт, хранение, демонстрацию, предложение, аренду или продажу технических средств, предназначенных для удаленного прослушивания разговоров и позволяющих совершать преступления, связанные с посягательством на частную жизнь другого лица, предусмотрена уголовная ответственность по ст. 226-3 УК Франции. Это подчеркивает важность защиты конституционных прав частных лиц, особенно в контексте развития современных технологий и расширения возможностей распространения информации через Интернет. Впрочем, с учетом того, что в большинстве случаев хакеры, совершающие вымогательство и шантаж, проживают в других странах и обладают большой технической поддержкой, вероятность того, что они будут привлечены к уголовной ответственности французскими правоохранительными органами, невелика. М. Массе пишет, что во Франции в качестве профилактической меры предлагается настраивать оповещения с указанием имени и фамилии, чтобы попытаться идентифицировать публикуемый в Интернете контент, персонализируя пользователя[2]. Поскольку преступления рассматриваемого вида наносят серьезный вред психическому и эмоциональному состоянию молодых людей, ключевую роль в предотвращении подобного рода случаев играют образовательные программы и пропагандистские кампании по повышению осведомленности.

[1] Le Bot C. Convention de lanzarote: la luttecontrel'exploitation et les abussexuels sur mineurs // Village de la Justice. 17.08.2022 // URL: https://www.village-justice.com/articles/convention-lanzarote-outils-juridiques-lutte-contre-exploitation-les-abus,42288.html.

[2] Masse M. «Sextorsion»: Sexe, chantage, paranoia, quell recours? // Village de la Justice. 02.07.2020 // URL: https://www.village-justice.com/articles/sextorsion-sexe-chantage-paranoia,35578.html.

Государственная власть реализует во Франции ряд уголовно-правовых мер в сфере подавления методик синтеза изображения или голоса с помощью технологии искусственного интеллекта, то есть дипфейков, и защиты несовершеннолетних от их воздействия. Дипфейки, создаваемые искусственным интеллектом, имеют целью подделку аудио- и видеоконтента с использованием физических, морфологических признаков, жестов и языка человека [10, с. 114]. В течение нескольких лет общество сталкивается с развитием этой новой творческой техники, особенно в журналистской и юмористической сферах, а также, как отмечают В.Г. Иванов и Я.Р. Игнатовский, в контексте половых преступлений, вымогательства и шантажа [11, с. 380-381].

Одной из уголовно-правовых мер борьбы с дипфейками является ст. 226-8-1 УК Франции, предусматривающая ответственность за публикацию без согласия лица монтажа сексуального характера, выполненного с его речью или изображением. Закрепленная в этой статье норма соответствует целям борьбы с шантажом сексуального характера и защиты людей, ставших жертвами порнодипфейков (среди них, по данным ассоциации «Deeptrace», 99% – женщины).

Использование искусственного интеллекта для монтажа изначально реальных фотографий или видео с целью запугивания потерпевших порождает еще одну форму секс-вымогательства. В 2024 г. в ст. 226-8 УК Франции были внесены изменения, устанавливающие уголовную ответственность в целях защиты личной информации и прав на слова или изображение человека в контексте использования алгоритмически созданного контента. С введением в действие данной нормы использование изображения или речи лица без его согласия признается преступлением, наказание за которое может ужесточаться в случае его совершения посредством публичных онлайн-сервисов.

В рамках уголовной политики Франции, направленной на противодействие преступлениям, совершаемым с использованием технологий, позволяющих нейросетям собирать в Интернете фотографии и видеозаписи, чтобы создавать на их основе дипфейки, в том числе порнографического характера, был принят закон, который существенно изменил содержание ст. 226-8 УК Франции. Во-первых, часть первая дополнена положением о том, что уголовная ответственность наступает за доведение до сведения общественности или третьей стороны любым способом визуального или звукового контента, созданного с помощью алгоритмической обработки и представляющего изображение или слова лица без его согласия, если не очевидно, что контент создан алгоритмически, или если об этом прямо не упоминается. Во-вторых, за публикацию монтажа или контента, созданного с помощью алгоритмической обработки, если эти действия осуществлялись с использованием услуги публичного онлайн-общения, установлено более суровое наказание в виде двух лет лишения свободы и штрафа в размере 45 тысяч евро[1].

Рассматривая развитие российской уголовной политики в отношении вымогательства, осуществляемого в цифровом пространстве, следует отметить, что в сентябре 2024 г. в Государственную Думу Российской Федерации был внесен законопроект, предусматривающий установление уголовной ответственности за совершение преступлений с использованием технологий подмены личности, то есть за мошеннические дипфейки[2].

Однако, несмотря на принимаемые законодателями меры по противодействию вымогательству, всё больше несовершеннолетних и женщин становятся жертвами криминального воздействия лиц, использующих дипфейки сексуального характера для осуществления своих преступных целей. К сожалению, киберпреступникам удается скрываться посредством маскировки IP-адресов и шифрования данных, что затрудняет их обнаружение и определение местонахождения. Такие возможности им предоставляет технология виртуальной частной сети (VPN), позволяющая обеспечить сетевое соединение поверх чьей-либо другой сети. С развитием искусственного интеллекта увеличивается объем сгенерированного с его помощью контента, который может быть использован для совершения противоправных деяний, в том числе вымогательства [12, с. 18; 13, с. 138].

Таким образом, вышеизложенное подтверждает потребность в разработке новых уголовно-правовых средств защиты граждан от вымогательства, осуществляемого в цифровом пространстве, а также мер виктимологической профилактики такого рода преступлений, что должно способствовать снижению степени рисков, связанных с публикацией личных данных в сети Интернет [14, с. 68; 15, с. 550].

В работе французского исследователя А. Релле описаны способы защиты несовершеннолетних от угроз рассматриваемого нами вида, разработанные для родителей. Не следует делиться фотографиями своих детей в социальных сетях, чтобы избежать завладения злоумышленниками их изображениями; необходимо устанавливать родительский контроль за контактами детей в Интернете, чтобы ограничить круг людей, которые могут с ними общаться. Полезно обсуждать с детьми опасности, связанные с использованием социальных сетей, повышать их осведомленность о потенциальных рисках, чтобы они не чувствовали себя беззащитным в случае возникновения неприятностей[3].

[1] Artigouha I., Parizet M. Les premiers pas de l'encadrement legal des deepfakes // Mesinfos. Affiches Parisiennes. 04.04.2024 // URL: https://mesinfos.fr/75000-paris/les-premiers-pas-de-l-encadrement-legal-des-deepfakes-196705.html.
[2] Законопроект № 718538-8 «О внесении изменений в Уголовный кодекс Российской Федерации» // Система обеспечения законодательной деятельности: сайт // URL: https://sozd.duma.gov.ru/bill/718538-8 (дата обращения: 30.09.2024).
[3] Relle A. Une nouvelle forme de «sextorsion», quand l'utilisation de l'ia detruit les mineurs // Village de la Justice. 20.12.2023 // URL: https://www.village-justice.com/articles/sextorsion-quand-utilisation-detruit-les-mineurs,48054.html.

Вместе с тем есть аналогичные рекомендации для несовершеннолетних: накрывать (закрывать) камеру компьютера, планшета и телефона; не общаться с незнакомыми людьми; переводить свои аккаунты в приватный режим. В случае совершения преступления следует незамедлительно обратиться в полицию и заблокировать пользователя в сети Интернет. И главное – никогда не платить деньги киберпреступникам [13].

Криминальные возможности лиц, совершающих противоправные деяния с помощью технологии искусственного интеллекта, весьма разнообразны [16, с. 118]. Эта технология способствует автоматизации и персонализации атаки, облегчает моделирование реалистичных сценариев, тем самым усиливая воздействие, оказываемое посягательством на частную жизнь, честь и достоинство людей, а также их репутацию.

При отсутствии согласия лица использование записей сказанных им в частном или конфиденциальном порядке слов или его изображений, например приватных фотографий, является преступлением. Следовательно, на этом основании можно привлечь к ответственности любое лицо, которое записывает подобные слова или изображения и выкладывает их в социальную сеть (ст. 226-1 УК Франции).

Как отмечает М. Пасотти, французское уголовное право предлагает несколько механизмов, позволяющих защитить личность и репутацию в Интернете. Однако эта защита должна основываться на индивидуальном подходе к квалификации содеянного, учитывающем все обстоятельства рассматриваемого события[1].

Помимо имущественного и морального ущерба, наносимого потерпевшему, как отмечает Г. Хаас, вымогательство может иметь гораздо более серьезные последствия. Случаи шантажа, осуществленного посредством веб-камеры, разрушили жизни многих потерпевших, а некоторых довели до самоубийства. Предотвращение такого рода посягательств начинается с защиты учетных записей в социальных сетях. Доступ к контактам друзей или подписчиков жертвы создает фундамент для реализации угроз киберпреступников. То же самое касается любого контента (фотографий и видеозаписей, например), опубликованного через аккаунт, к которому открыт свободный доступ[2].

Итак, проведенный нами анализ норм французского уголовного закона, предусматривающих ответственность за шантаж и вымогательство, позволил сделать вывод о том, что совершению таких преступлений способствует угроза раскрытия конфиденциальной информации и/или публикации сведений, компрометирующих жертву (супружеская измена, сексуальная ориентация, судимость, болезнь и т.д.), независимо от того, являются ли они реальными или вымышленными. Угроза может быть заявлена в письменной или устной форме, она достаточно конкретна для того, чтобы определить, чего хочет добиться преступник. Г. Хаас пишет, что законодательство Франции позволяет дифференцировать действия виновных лиц, связанные с вымогательством. Французский уголовный кодекс устанавливает более жесткие санкции для некоторых видов таких преступлений, включая увеличенные сроки лишения свободы и повышенные размеры штрафов[3].

ЗАКЛЮЧЕНИЕ

Резюмируя изложенное, отметим, что французский опыт уголовно-правового противодействия вымогательству в цифровом пространстве может быть использован при разработке мер, направленных на совершенствование российского уголовного законодательства, в частности, при дифференциации уголовной ответственности за вымогательство и криминализации новых общественно опасных деяний, фактически представляющих собой способы вымогательства.

Так, например, в настоящее время диспозиция ст. 163 УК РФ не охватывает такие способы совершения вымогательства, как использование программ-вымогателей и зачастую сопутствующие ему угрозы в виде блокирования или уничтожения компьютерной информации, а также применение возможностей искусственного интеллекта, в том числе для создания дипфейков. Конструкция статей УК Франции об ответственности за вымогательство и шантаж помогает квалифицировать применение такого рода способов и угроз как преступление. Сопряженная квалификация требуется для восстановления социальной справедливости, ущерб которой был нанесен в связи с нарушением других охраняемых законом прав и свобод.

Стоит обратить внимание на то обстоятельство, что во Франции закреплены более строгие санкции за совершение вымогательства и шантажа, чем в России. Это подчеркивает жесткость уголовно-правовой политики в отношении нарушения прав и свобод граждан при совершении преступлений изучаемого нами вида. Вопрос о целесообразности ужесточения санкций в УК РФ требует дополнительных исследований, его разрешение не входило в нашу задачу при подготовке данной статьи.

При этом подчеркнем, что в деятельности по совершенствованию российского уголовного законодательства следует обратить внимание на положительный опыт противодействия вымогательству во Франции. Например, считаем целесообразным внести изменения в ст. 163 УК РФ, а именно расширить перечень способов и угроз, образующих состав преступления. ■

[1] Pasotti M. Chantage et delits de presse au moyen des réseaux sociaux: défendre son e-reputation grace au droit penal? // Village de la Justice. 28.12.2009 // URL: https://www.village-justice.com/articles/Chantage-delits-presse-moyen,7171.html.

[2] Haas G. Cyberharcelement, fraude sentimentale: que faire face au chantage affectif? // Village de la Justice. 21.04.2022 // URL: https://www.village-justice.com/articles/cyberharcelement-fraude-sentimentale-que-faire-face-chantage-affectif,42390.html.

[3] Там же.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Мулюков Ф.Б., Ибрагимов А.Г. Санкции и наказания за преступления против личности по уголовному кодексу Франции // Ученые записки Казанского университета. Серия: Гуманитарные науки. 2020. № 2. С. 201-213.
2. Цой Л.В. Уголовное законодательство России и зарубежных стран об ответственности за вымогательство // Алтайский вестник государственной и муниципальной службы. 2017. № 17. С. 92-94.
3. Гоголь А.С., Маслова М.А. Основные виды компьютерных угроз // Научный результат. Информационные технологии. 2020. Т. 5. № 3. С. 3-9.
4. Стяжкина С.А. Вопросы квалификации кибервымогательства // Вестник Удмуртского университета. 2022. Т. 32. Вып. 5. С. 941-947.
5. Жмуров Д.В. Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1 (27). С. 89-98.
6. Шевко Н.Р., Казанцев С.Я., Турутина Е.Э. Анализ киберпреступности в период пандемии // Вестник Московского университета МВД России. 2023. № 2. С. 250-252.
7. Демидович В.А. Анализ уголовного законодательства Франции, Англии и Испании об ответственности за развратные действия // Вестник Костромского государственного университета. 2021. Т. 27. № 4. С. 186-191.
8. Рыбин И.В. Сравнительно-правовой анализ предмета вымогательства в уголовном законодательстве Франции и России // Закон и право. 2020. № 9. С. 73-75.
9. Чурсина А.Д. Кибервымогательство и угрозы в социальных сетях // Вестник Московского университета МВД России. 2022. № 5. С. 294-296.
10. Добробаба М.Б. Дипфейки как угроза правам человека // Lex russica. 2022. Т. 75. № 11. С. 112-119.
11. Иванов В.Г., Игнатовский Я.Р. Deepfakes: перспективы применения в политике и угрозы для личности и национальной безопасности // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2020. № 4. С. 379-385.
12. Дворянкин О.А. Даркнет – темная сторона Интернета или неужели так все плохо? // Национальная ассоциация ученых. 2021. № 71-1. С. 14-20.
13. Усманов Р.А. Характеристика преступной деятельности, осуществляемой в сети Интернет посредством сервисов-анонимайзеров // Юридическая наука и правоохранительная практика. 2018. № 4 (46). С. 135-141.
14. Желудков М.А. Обоснование необходимости адаптации деятельности правоохранительных органов к условиям цифровой трансформации преступной среды // Lex russica. 2021. № 4 (173). С. 63-70.
15. Алексеева А.П. Профилактика правонарушений в России: законодательные основы и перспективы реализации // Преступность, уголовная политика, уголовный закон: Сборник научных трудов. Саратов: Саратовская государственная юридическая академия, 2013. С. 549-551.
16. Sukhodolov A.P., Bychkov A.V., Bychkova A.M. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects // Journal of Siberian Federal University. Humanities and Social Sciences. 2020. Vol. 13. No. 1. P. 116-122.

REFERENCES

1. Mulyukov F.B., Ibragimov A.G. Sanktsii i nakazaniya za prestupleniya protiv lichnosti po ugolovnomu kodeksu Frantsii // Uchenyye zapiski Kazanskogo universiteta. Seriya: Gumanitarnyye nauki. 2020. № 2. S. 201-213.
2. Tsoy L.V. Ugolovnoye zakonodatel'stvo Rossii i zarubezhnykh stran ob otvetstvennosti za vymogatel'stvo // Altayskiy vestnik gosudarstvennoy i munitsipal'noy sluzhby. 2017. № 17. S. 92-94.
3. Gogol' A.S., Maslova M.A. Osnovnyye vidy komp'yuternykh ugroz // Nauchnyy rezul'tat. Informatsionnyye tekhnologii. 2020. T. 5. № 3. S. 3-9.
4. Styazhkina S.A. Voprosy kvalifikatsii kibervymogatel'stva // Vestnik Udmurtskogo universiteta. 2022. T. 32. Vyp. 5. S. 941-947.
5. Zhmurov D.V. Darknet kak uskol'zayushchaya sfera pravovogo regulirovaniya // Sibirskiye ugolovno-protsessual'nyye i kriminalisticheskiye chteniya. 2020. № 1 (27). S. 89-98.
6. Shevko N.R., Kazantsev S.Ya., Turutina Ye.E. Analiz kiberprestupnosti v period pandemii // Vestnik Moskovskogo universiteta MVD Rossii. 2023. № 2. S. 250-252.
7. Demidovich V.A. Analiz ugolovnogo zakonodatel'stva Frantsii, Anglii i Ispanii ob otvetstvennosti za razvratnyye deystviya // Vestnik Kostromskogo gosudarstvennogo universiteta. 2021. T. 27. № 4. S. 186-191.
8. Rybin I.V. Sravnitel'no-pravovoy analiz predmeta vymogatel'stva v ugolovnom zakonodatel'stve Frantsii i Rossii // Zakon i pravo. 2020. № 9. S. 73-75.
9. Chursina A.D. Kibervymogatel'stvo i ugrozy v sotsial'nykh setyakh // Vestnik Moskovskogo universiteta MVD Rossii. 2022. № 5. S. 294-296.
10. Dobrobaba M.B. Dipfeyki kak ugroza pravam cheloveka // Lex russica. 2022. T. 75. № 11. S. 112-119.
11. Ivanov V.G., Ignatovskiy Ya.R. Deepfakes: perspektivy primeneniya v politike i ugrozy dlya lichnosti i natsional'noy bezopasnosti // Vestnik Rossiyskogo universiteta druzhby narodov. Seriya: Gosudarstvennoye i munitsipal'noye upravleniye. 2020. № 4. S. 379-385.
12. Dvoryankin O.A. Darknet – temnaya storona Interneta ili neuzheli tak vse plokho? // Natsional'naya assotsiatsiya uchenykh. 2021. № 71-1. C. 14-20.

13. Usmanov R.A. Kharakteristika prestupnoy deyatel'nosti, osushchestvlyayemoy v seti Internet posredstvom servisov-anonimayzerov // Yuridicheskaya nauka i pravookhranitel'naya praktika. 2018. № 4 (46). S. 135-141.

14. Zheludkov M.A. Obosnovaniye neobkhodimosti adaptatsii deyatel'nosti pravookhranitel'nykh organov k usloviyam tsifrovoy transformatsii prestupnoy sredy // Lex russica. 2021. № 4 (173). S. 63-70.

15. Alekseyeva A.P. Profilaktika pravonarusheniy v Rossii: zakonodatel'nyye osnovy i perspektivy realizatsii // Prestupnost', ugolovnaya politika, ugolovnyy zakon: Sbornik nauchnykh trudov. Saratov: Saratovskaya gosudarstvennaya yuridicheskaya akademiya, 2013. S. 549-551.

16. Sukhodolov A.P., Bychkov A.V., Bychkova A.M. Criminal Policy for Crimes Committed Using Artificial Intelligence Technologies: State, Problems, Prospects // Journal of Siberian Federal University. Humanities and Social Sciences. 2020. Vol. 13. No. 1. P. 116-122.

ССЫЛКА ДЛЯ ЦИТИРОВАНИЯ

Егорочкина М.В. Уголовная ответственность за вымогательство в цифровом пространстве по зарубежному законодательству // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2024. № 4 (78). С. 31-38.