*Научная статья*
*Научная специальность*
*12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»*

УДК 316.422.42
DOI https://doi.org/10.26516/2071-8136.2022.2.105

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОЙ РОССИИ В ПЕРИОД ПАНДЕМИИ COVID-19

**© Островских Ж. В.[1], Хохлова О. М.[2], Рожкова А. К.[3], 2022**
[1] Иркутский государственный университет, г. Иркутск, Россия
[2] Восточно-Сибирский филиал Российского государственного университета правосудия, г. Иркутск, Россия
[3] Байкальский государственный университет, г. Иркутск, Россия

Исследуется как одна из важных составляющих системы национальной безопасности современной России информационная безопасность, которая, как показала пандемия COVID-19, имеет высокую социальную значимость на различных уровнях, включая национальный. Анализ интенсивно развивающегося законодательства в сфере информационных технологий и защиты информации и неоднородной практики его применения позволил выделить разночтения и, как следствие, обозначить потребность унификации подходов. Рассмотрены приоритетные направления развития информационного общества в современной России, понятие информационной безопасности, виды и методы реализации угроз информационной безопасности, а также предложены некоторые способы защиты информационных ресурсов.

*Ключевые слова*: информация, информационная безопасность, национальная безопасность, средства массовой информации, система национальной безопасности, пандемия COVID-19.

# INFORMATION SECURITY IN THE NATIONAL SECURITY SYSTEM OF MODERN RUSSIA DURING THE PANDEMIC COVID-19

**© Ostrovskikh Zh. V.[1], Khokhlova O. M.[2], Rozhkova A. K.[3], 2022**
[1] Irkutsk State University, Irkutsk, Russian Federation
[2] East-Siberian Branch of Russian State University of Justice, Irkutsk, Russian Federation
[3] Baikal State University, Irkutsk, Russian Federation

The authors study information security as one of the important components of the national security system of modern Russia, and which, as shown by the COVID-19 pandemic, has a high social significance and a priority need to protect information resources at various levels, including national. The analysis of the intensively developing legislation in the field of information technology and information protection, and the heterogeneous practice of its application, made it possible to identify discrepancies, and, as a result, to identify the need for unification of approaches. The priority directions of the development of the information society in modern Russia, the concept of information security, types and methods of implementing threats to information security are considered, and some ways of protecting information resources are proposed.

*Keywords*: information, information security, national security, mass media, national security system, pandemic COVID-19.

## Введение

Пандемия коронавируса COVID-19, оказавшая сильнейшее воздействие на все социальные и экономические процессы, в том числе их массовый переход в онлайн, ярко продемонстрировала необходимость осуществления эффективной защиты информационного пространства. Несомненно, что ограничительные меры, введенные в целях борьбы с коронавирусом, существенно ускорили цифровизацию и активный рост IT-технологий, но вместе с тем положительный технологический эффект послужил триггером значительного увеличения киберпреступлений, так как интерес преступности всего мира, особенно ее организованных форм, переместился в виртуальное пространство [6, с. 205–209].

В России наблюдается крайне неблагоприятная устойчивая тенденция роста преступлений, совершаемых с использованием информационно-телекоммуникационных и цифровых технологий или в сфере компьютерной информации. Если исходить из анализа статистических данных МВД РФ, с 2014 г. их количество увеличилось почти в 50 раз – с 11 тыс. (0,5 % в общей структуре преступности) до 517,7 тыс. в 2021 г. (удельный вес – до 25 %, или каждое четвертое преступление), при этом их раскрываемость остается крайне низкой (22,9 %)[1].

В новой редакции Указа Президента РФ «О Стратегии национальной безопасности Россий-

[1] Состояние преступности // Министерство внутренних дел Российской Федерации. URL: https://мвд.рф/folder/101762 (дата обращения: 12.04.2012)

ской Федерации» от 2 июня 2021 г.[1], в сравнении с прошлой редакцией документа, проблема обеспечения информационной безопасности, которой теперь посвящен целый раздел, стала рассматриваться в качестве глобальной, требующей комплексных решений, а также в качестве национального интереса и национального приоритета.

Таким образом, обеспечение информационной безопасности, переосмысление ее роли и места в системе национальной безопасности России обозначились как одна из приоритетных задач в модернизации российской государственности, предопределившая во многом содержание и динамику внутриполитических процессов, специфику самоидентификации страны, определение ее роли и места в трансформирующемся мировом сообществе.

**Материалы и методы исследования**

Эмпирическую базу составили данные, содержащиеся в исследовательских отчетах компаний – производителей средств информационной безопасности Check Point, Ivanti, Sophos, а также официальная статистика, представленная Федеральной службой государственной статистики, МВД и Минцифры России.

В методологическую основу легли категории и принципы диалектики, определяющие требования объективности, всеобщей связи и системности в познании любых социально-правовых явлений. Отсутствие однозначных доктринальных позиций, постоянно меняющееся и развивающееся законодательство в сфере информационных технологий и защиты информации, неоднородная практика его применения позволили выделить разночтения и, как следствие, обозначить потребность в унификации подходов.

В нашем исследовании базируемся на категории «личность», интегрирующей категории «человек», «гражданин», поскольку именно личность в глобальном информационном обществе способна выступать и субъектом, и объектом информационных правоотношений, представлять законодательно закрепленные интересы информационной сферы, обладая при этом высокой степенью самостоятельности и автономности.

**Обзор литературы**

За теоретическую основу взяты актуальные публикации российских и иностранных исследователей.

Как в уголовно-правовой и криминологической, так и экономической, и других научных сферах ученые дискутируют по поводу развивающихся информационных отношений, их глобализации в мировом пространстве, что требует пересмотра и изменения законодательно-правовой модели этих отношений в плане оказания услуг и защиты информационного поля.

Ряд отечественных ученых внесли значительный вклад в развитие этого направления, среди них отметим Г. Т. Артамонова, В. М. Глушкова, В. Л. Иноземцева, К. К. Колина, Н. Н. Моисеева, А. И. Ракитова, А. В. Соколова, А. Д. Урсула, Е. С. Устиновича и других [16, с. 165]. И особенно выделим российского *экономиста, социолога и политического деятеля* В. Л. Иноземцева, переводившего на русский язык работы Д. Белла [12, с. 20].

**Результаты исследования**

Информационные отношения, становление современного информационного общества, защита информационного поля, информационная безопасность стали выступать предметом исследования в юридической науке сравнительно недавно.

Основоположником концепции информационного (постиндустриального) общества был американский социолог и публицист Д. Белл, опубликовавший в 1973 г. свой знаменитый научный труд «Грядущее постиндустриальное общество. Опыт социального прогнозирования» [2, с. 18], где описывал угрозы, связанные с развитием информационных технологий: «при помощи совершенной аппаратуры… сбор правительственными и коммерческими учреждениями банков данных» [11, с. 19], что заметно пропагандируется и демонстрируется в последнее время.

В современном обществе уделяется пристальное внимание сфере развития информационных отношений, технологий и защиты информации, что позволило охарактеризовать информационную безопасность в целом как одну из наиболее значимых в системе национальной безопасности, поскольку именно этот вид безопасности связан практически со всеми другими ее видами.

В Концепции формирования информационного общества в России[2] (далее – Концепция) говорится, что осознаны предпосылки и реальные пути формирования и развития информационного общества в России. Этот процесс имеет глобальный характер, неизбежно вхождение

[1] О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 2 июля 2021 г. № 400 // Собр. законодательства РФ. 2021. № 27. Ст. 5351.

[2] Концепция формирования информационного общества в России. Одобрена решением Государственной комиссии по информатизации при Государственном комитете Российской Федерации по связи и информатизации от 28 мая 1999 г. № 32 // КонсультантПлюс : справочная правовая система.

нашей страны в мировое информационное сообщество, поскольку в каждой стране процесс формирования и развития информационного общества проходит, базируясь на сложившихся социально-экономических, политических и культурных условиях. Принятая Концепция явилась отправной точкой для дальнейшего формирования правовых основ современного информационного общества, определила основы информационной безопасности России.

В Указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[1] (далее – Стратегия), отмечается, что информационным признается общество, «в котором информация и уровень ее применения и доступности кардинальным образом влияют на экономические и социокультурные условия жизни граждан». Основным критерием информационного общества признается влияние информации на уровень жизни граждан. В Стратегии уделено пристальное внимание интересам отдельной личности в информационной сфере, при котором обеспечиваются государственные интересы в целом, а также защита российских граждан. В качестве приоритетного направления развития информационного общества в нашей стране выбрано формирование информационного пространства с учетом потребностей граждан в получении качественных и достоверных сведений. Отмечается, что признаками информационного общества в современной России являются всеобщая доступность и активное распространение мобильных устройств, сетей связи и беспроводных информационных технологий, обеспечение системы предоставления государственных и муниципальных услуг в электронной форме для улучшения жизни и удобства граждан, определены меры для развития информационного общества в дальнейшем, учитывая цели и задачи внутренней и внешней политики страны в сфере применения информационных и коммуникационных технологий.

Нам импонируют выводы Е. С. Устиновича, который полагает, что создание информационного общества в России выступает своеобразной платформой для решения задач высокого уровня: модернизации экономики и общественных отношений, соблюдения конституционных прав граждан в информационной сфере, высвобождения информационных ресурсов для личностного развития человека [20, с. 73].

А. С. Бородин, рассматривая признаки информационного общества, к сложившимся характерным чертам предлагает отнести информационную экономику, высокий уровень информационных потребностей членов общества, фактическое и качественное их удовлетворение, высокую информационную культуру, свободный доступ каждого к информации, ограниченный лишь информационной безопасностью самой личности, общественных групп и общества в целом [4, с. 21].

Данные Мониторинга развития информационного общества, проводимого Федеральной службой государственной статистики с 2010 по 2021 г. включительно, свидетельствуют о том, что в Российской Федерации наблюдается положительная динамика развития информатизации общества. Значительно увеличились за указанный период объемы инвестиций на оборудование для информационных и коммуникационных технологий, затраты на научные исследования и разработки, использование информационно-коммуникационных технологий в деятельности органов государственной власти, что ярко демонстрирует положительные сдвиги. Вместе с тем Россия до сих пор находится в группе со средним уровнем развития информационно-коммуникационных технологий, существенно отставая от наиболее развитых в этой сфере стран, таких как Соединенные Штаты Америки, Нидерланды, Сингапур, Финляндия, Швеция, при этом уровень проникновения Интернета в нашей стране достаточно высок и составляет 72,8 %[2].

В современной науке имеются различные классификации видов безопасности. В соответствии с объектом защиты выделяют безопасность личности, общества и государства. Исходя из содержания сфер жизни общества, подлежащих защите, определяют следующие виды безопасности: экономическую, военную, экологическую, социальную, информационную, демографическую, интеллектуальную, культурную безопасность и ряд других. Среди перечисленных видов безопасности информационная безопасность, на наш взгляд, занимает особое положение, поскольку информационная составляющая находит почетное место в структуре всех видов безопасности без исключения.

Роль информации в современном российском обществе имеет стремительную тенденцию к росту, а необходимость в информационных ресурсах и информационных технологиях в

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента РФ от 9 мая 2017 г. № 203 // Собр. законодательства РФ. 2017. № 20. Ст. 2901.

[2] Федеральная служба государственной статистики. URL: https://gks.ru/free_doc/new_site/business/it/ikt21/index.html (дата обращения: 05.02.2022).

эпоху информатизации современного общества выдвигает информационную безопасность на первый план, делая приоритетной по всем показателям, что еще более отчетливо нам продемонстрировал период пандемии.

Современное развитие информационного общества в России свидетельствует о повышенном к нему внимании, поскольку постоянно совершенствуется нормативно-правовая база, принимаются государственные программы, направленные на его развитие.

В имеющихся нормативных законодательных актах под информационной безопасностью Российской Федерации принято понимать «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет государства, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации»[1].

Безопасность выступает в качестве основной потребности, представляет собой ведущую цель как отдельного человека, так и общества в целом.

Американский психолог-гуманист А. Маслоу выделял потребность в безопасности и защите (Safetysecurity need) в качестве ведущей потребности, которая способна мотивировать человека установить разумный порядок, структуру и прогнозируемость своего окружения, и считал неистребимым желание жить лучше [15, с. 34].

Со времен Древнего мира проблема безопасности считается особым социальным феноменом, укрепившим в наши дни свои позиции и расширившимся с возрастанием количества угроз и опасностей в обществе. К исследователям, уделявшим пристальное внимание этим вопросам, отнесем Платона, Аристотеля, Дж. Локка, Т. Гоббса, Ж. Ж. Руссо и других ученых.

Определение понятия «безопасность» до сих пор является достаточно дискуссионным, не имеющим четкой трактовки. Отдельные ученые, рассматривающие дефиницию безопасности, в качестве ее основы выделяют «состояние защищенности», анализируя понятие, закрепленное в Законе РФ от 5 марта 1992 г. № 2446-1 «О безопасности»[2], утратившем силу с 29 декабря 2010 г. Действующий Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»[3] понятие «безопасность» также не раскрывает в полной мере, поэтому и имеется множество его авторских толкований, что зачастую приводит к его пониманию в различных значениях и контекстах, порой явно спорных, противоречивых или не согласующихся с современными реалиями.

Отметим, что в праве понятия входят в формулировки законов, соответственно, от их точности, приемлемости и логической корректности зависит толкование самой сути закона, включая его дальнейшее исполнение, что накладывает определенные требования к дефиниции правового понятия, необходимости его смысловой однозначности, унифицированности употребления во всех нормативных правовых актах.

Поэтому попытаемся проанализировать имеющиеся в современной научной теории основные подходы к трактовке понятия «безопасность». Определяя теоретико-методологические подходы к толкованию данного понятия, А. А. Гриценко считает, что безопасность не может быть сведена к защищенности, а в новых условиях отождествляется с предотвращением, управлением и развитием; поэтому, говоря об этом, мы ведем речь не о самой безопасности, а о ее обеспечении [5, с. 88].

М. Ю. Зеленков считает, что определение безопасности через понятие «защищенность» охватывает не все опасные состояния, а лишь некоторые. Кроме того, «безопасность как состояние сохранности, надежности предполагает поддержание определенного баланса между негативным воздействием на субъект окружающей его среды и его способностью преодолеть это воздействие либо собственными ресурсами, либо при помощи соответствующих, специально для этого созданных органов или механизмов» [10, с. 11].

Ряд других исследователей этой проблемы: И. В. Демин [7, с. 29–30], Е. С. Недосекова [17, с. 28], А. А. Смирнов [19, с. 19] – рассматривают безопасность в ее традиционной трактовке, которая предложена в Законе РФ № 2446-1 «О безопасности», указанном выше, как «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». При этом, анализируя ревизионистские подходы к определению понятия «безопасность», А. А. Смирнов указывает, что часто критикуется «состояние защищенности» как статичное и пассивное явление, которое не соответствует сущности самой безопасности,

[1] Об утверждении Доктрины информационной безопасности РФ : указ Президента РФ от 5 дек. 2016 г. № 646 // Собр. законодательства РФ. 2016. № 50. Ст. 7074.

[2] О безопасности : закон РФ от 5 марта 1992 г. № 2446-1-ФЗ (Утратил силу).

[3] О безопасности : федер. закон от 28 дек. 2010 г. № 390-ФЗ // Собр. законодательства РФ. 2011. № 1. Ст. 2.

что «речь идет о безопасности, где под состоянием защищенности подразумевается комплекс условий, как внутренних, так и внешних, обеспечивающих защиту объекта от негативного воздействия угроз, а достижение этого состояния предполагает активную деятельность со стороны государства и других субъектов обеспечения безопасности» [19, с. 17]. Он связывает понятие «состояние защищенности» с динамикой уровня безопасности, «выступающей метасостоянием объектов безопасности, допускающей изменения их основных параметров, но только в строго установленных границах, вход за которые приводит к состоянию незащищенности (опасности)» [Там же, с. 18]. Автор доказывает, что традиционное определение безопасности хотя и имеет недостатки, но все-таки является оптимальной дефиницией. Согласимся с исследователем и отметим, что такая формулировка включена в большинство нормативных правовых актов сферы безопасности, например в Федеральный закон «О пожарной безопасности»[1], в Указ Президента РФ «О Стратегии национальной безопасности Российской Федерации»[2] (далее – Стратегия национальной безопасности). Трактовка «безопасности», указанная в вышеперечисленных документах, охватывает все объекты безопасности, включая интересы личности, общества и государства, учитывает возможность наступления внутренних и внешних угроз. На наш взгляд, она является наиболее оптимальной для сферы безопасности в целом и способна выступать основой характеристики различных видов безопасности.

На наш взгляд, информационная безопасность – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан и государства. Следовательно, под информационной безопасностью понимается защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб субъектам информационных отношений, включая владельцев и пользователей информации и поддерживающей инфраструктуры.

Выделим два базовых принципа информационной безопасности, обеспечивающей:

– целостность данных, предполагающих защиту от сбоев, приводящих к потере информации и неавторизованного создания или уничтожения данных;

– конфиденциальность информации и одновременно ее доступность для всех авторизованных пользователей.

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности. Правильный с методологической точки зрения подход к проблемам информационной безопасности начинается с выявления субъектов информационных отношений, с учета их интересов, связанных с использованием информационных систем.

Угрозы информационной безопасности – обратная сторона использования информационных технологий, а защита информации в современном информационном обществе имеет существенное значение, поскольку новая информационная инфраструктура способна создать новые опасности.

На наш взгляд, обеспечить достижение информационной безопасности способен только комплексный подход, сочетающий в себе четыре уровня: законодательный, административный, процедурный и программно-технический. Нормативные правовые акты имеют ограничивающую направленность, в них не предусматривается ответственность государственных органов за нарушение информационной безопасности: лицензирование и сертификация не смогут обеспечить полную защиту от всевозможных угроз [21, с. 78].

В условиях жизнедеятельности современного общества обеспечение национальной безопасности прочно закреплено как значимое и приоритетное направление развития государственной политики нашей страны, что зарегламентировано и в ряде нормативных правовых актов. Национальная безопасность представляет собой систему взаимосвязанных элементов, в которую входят социально-политические и правовые институты, учреждения и организации, совокупность принципов, положений, форм, методов и средств, предотвращающих или не допускающих возникающие опасности, вызовы и угрозы.

Субъектами безопасности выступают как отдельные граждане, так и общество в целом, активно участвующие в преодолении угроз национальной безопасности государственными органами, в свою очередь, государство предоставляет необходимую правовую и социальную защиту, гарантированную национальным законодательством и нормами международного права. В Стратегии национальной безопасности существует положение, в котором отмечается,

[1] О пожарной безопасности : федер. закон от 21 дек. 1994 г. № 69-ФЗ // Собр. законодательства РФ. 1994. № 35. Ст. 3649.

[2] О Стратегии национальной безопасности Российской Федерации : указ Президента РФ от 31 дек. 2015 г. № 683 // Собр. законодательства РФ. 2016. № 1. Ст. 212. (Утратил силу).

что национальная безопасность включает в себя все виды безопасности, предусмотренные Конституцией РФ[1] и законодательством Российской Федерации: государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую, а также безопасность личности[2].

Делая выводы, отметим, что информационная безопасность законодательно отнесена к виду национальной безопасности [1, с. 23].

Место информационной безопасности в системе национальной безопасности в отечественной науке определяется через различные подходы, требующие всесторонней оценки и глубокого анализа.

Информационную безопасность рассматривают в качестве равноценного и равнозначного вида национальной безопасности [14, с. 45]. А. А. Марков – представитель данного подхода – отмечает, что статус роли информационной безопасности как главенствующей преждевременный, возможен в случае, если информационное общество в России будет построено и станет составной частью глобального информационного общества [Там же, с. 47].

Информационной безопасности принадлежит первоочередное место в системе национальной безопасности, поскольку через информационную среду реализуются всевозможные угрозы национальной безопасности, предъявляемые России в различных сферах деятельности [3, с. 8]. Ряд исследователей предлагают рассматривать информационную безопасность как самостоятельный наднациональный вид всеобщей безопасности, обеспечивающий прогрессивное развитие не только информационной среды, но и общества в целом, а не как один из видов национальной безопасности.

В современных реалиях информационная безопасность может выступать как основной элемент системы национальной безопасности, а может и как самостоятельный вид безопасности, и даже быть преобладающим элементом всех сфер безопасности. В последнем случае информационная безопасность подразумевается уже в более широком смысле, поскольку встает на защиту всей информационной инфраструктуры, информационно-коммуникационных технологий от неправомерных воздействий ее функционирования, защиту информации от несанкционированного доступа, негативных информационных воздействий на психоэмоциональное состояние личности, обеспечение доступа к информации при условии соблюдения требований, предусмотренных законодательством Российской Федерации.

Попытаемся оценить роль информационной составляющей в разных видах национальной безопасности. В российском обществе информационно-коммуникационные технологии являются неотъемлемой частью управленческих систем государственной деятельности, обеспечения правопорядка, обороны и безопасности государства, различных отраслей экономики при осуществлении взаимодействия ее субъектов, поэтому своевременная, достоверная и полная информация при принятии управленческих решений является ее наивысшим преимуществом.

По мнению И. В. Овсяниковой, информационный ресурс является доминантным фактором развития не только производственной сферы, но и экономической системы в целом [18, с. 3]. Отметим при этом, что индекс конкурентоспособности экономики государств (по данным Всемирного экономического форума) имеет высокий уровень корреляции с индексом развития в странах информационно-коммуникационных технологий[3].

Стоит отметить и негативные последствия заявленной проблемы: незаконное использование коммерческой информации, шпионаж, хакерство, похищение персональных данных и другие. Необходимо учитывать и государственную и общественную безопасность при манипулировании сознанием населения с помощью предоставления недостоверной информации, формировании искаженного представления о процессах и явлениях современного общества. Перечисленные факторы негативно влияют на устойчивое развитие России, создавая атмосферу напряженности, политической нестабильности, провоцируют социально-экономические, национальные и другие конфликты.

Т. В. Закупень отмечает значимую роль информационной составляющей в сфере военной безопасности, говоря об уровне развития информационных технологий, на которых основываются современные системы разведки, радиоэлектронной борьбы, управления войсками и высокоточным оружием, что существенно влияет на исход вооруженных конфликтов [9, с. 28].

[1] Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // КонсультантПлюс : справочная правовая система.

[2] О Стратегии национальной безопасности РФ : указ Президента РФ от 2 июля 2021 г. № 400 // Собр. законодательства РФ. 2021. № 27. Ст. 5351.

[3] Об утверждении Стратегии развития отрасли информационных технологий в РФ на 2014–2020 годы и на перспективу до 2025 года : распоряжение Правительства РФ от 1 нояб. 2013 г. № 2036-р // Собр. законодательства РФ. 2013. № 46. Ст. 5954.

Говоря о проблемах продовольственной безопасности в нашей стране, В. В. Кожевников отмечает, что угрозой обеспечения продовольственной безопасности выступает создание искусственных конкурентных преимуществ зарубежной продукции, формируемых за счет различных мер государственной поддержки производства пищевых продуктов зарубежных стран [13, с. 59], при формировании продовольственного спроса населения информационная составляющая играет главенствующую роль.

Рассмотрим информационную безопасность, ее особенности, угрозы и криминальные риски в период пандемии COVID-19, которые приобрели массовый и более изощренный характер.

Разнообразие преступлений, совершенных с использованием Интернета и информационных технологий или в сфере компьютерной информации, уходит далеко за рамки определенного Генеральной прокуратурой РФ и МВД РФ перечня видов преступлений[1], а, учитывая их высокую латентность, оценить точное число угроз информационной безопасности не представляется возможным. Так, большинство кибератак не предается огласке из-за репутационных рисков, в связи с чем даже организации, занимающиеся расследованием инцидентов и анализом действий хакерских групп, могут подсчитать лишь их приблизительное количество.

По оценке Интерпола, за период пандемии COVID-19 киберпреступность показала значительный сдвиг целей противоправного воздействия от частных лиц и малых предприятий к крупным корпорациям, правительствам и критической инфраструктуре[2]. В период пандемии чаще всего подвергались кибератакам госучреждения и медицинские организации. Учреждения здравоохранения являются легкой жертвой для киберпреступников, поэтому вопросу обеспечения информационной безопасности медицинских учреждений необходимо уделить особое внимание, проанализировать все потенциальные риски и выработать способы их предотвращения, потому что последствия попыток дестабилизировать медицинскую инфраструктуру могут быть необратимы.

Так, по данным Positive Technologies[3], в 2021 г. на госучреждения пришлось 16 % атак, на медицинские учреждения – 11 %, промышленные компании – 10 %, научные и образовательные учреждения – 9 %, IT-компании – 7 %. В основном злоумышленники охотились за персональными и учетными данными и информацией, составляющей коммерческую тайну, а также увеличилось количество атак с использованием программ-вымогателей, количество атак на частных лиц оставалось на высоком уровне (14 %), в основном они были связаны с социальной инженерией (88 %). При этом активно эксплуатировались актуальные темы и социально значимые события: популярными темами фишинга в 2021 г. были собственно пандемия COVID-19 и вакцинация, премьеры фильмов и сериалов, корпоративные рассылки, инвестиции. Уже в начале 2022 г. российские граждане столкнулись с фишинговыми атаками, при которых преступники обещают помочь сохранить денежные накопления в случае отключения России от системы международных переводов SWIFT или предлагают заработать на арбитражной торговле.

В отношении самих видов угроз ничего нового придумано не было: все те методы атак, встречающиеся сейчас (вредоносные программы, хакинг, фишинг, спам, ботнеты, социальная инженерия, эксплуатации веб-уязвимостей и т. п.), и раньше давали о себе знать, а сейчас, в связи с переходом на удаленную работу, с появлением новых сервисов для работы с личных ноутбуков и рабочих станций внутри корпоративного периметра, произошло перераспределение акцентов в части того, как эффективнее атаковать. Как отмечается в докладе Европола, в условиях введенного режима самоизоляции современные киберпреступники действуют в рамках наработанной годами практики, однако с учетом специфики общественного интереса к теме коронавируса[4].

Ущерб от преступлений, совершаемых с использованием информационно-телекоммуникационных и цифровых технологий, является колоссальным. По оценкам Всемирного экономического форума, потери мировой экономики от кибератак составили в 2021 г. 2,5 трлн долл.

[1] Показатели статистической отчетности формируются в соответствии с Перечнем № 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 29 декабря 2021 г. № 790/11/1.

[2] Interpol. URL: https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19 (дата обращения: 04.08.2020).

[3] Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2021/ (дата обращения: 19.04.2022).

[4] Pandemic profiteering: how criminals exploit the COVID-19 crisis. URL: https://www.europol.europa.eu/pandemic-profiteeringhow-criminals-exploit-covid-19-crisis (дата обращения: 04.04.2020).

США, а к 2022 г. они могут достичь 8 трлн[1]. Так, например, по данным экспертов Check Point, за период с ноября 2020 г. по ноябрь 2021 г. лишь с помощью ботнета Phorpiex злоумышленникам удалось перехватить 969 транзакций и вследствие подмены адресов криптовалютных кошельков похитить около 500 тыс. долл. США[2]. Согласно исследовательскому отчету Ivanti, только за первое полугодие 2021 г. средняя сумма выплат распространителям программ-вымогателей составила 570 тыс. долл. США, максимальная выплаченная сумма – 40 млн долл. США[3], а средняя стоимость устранения последствий атаки программы-вымогателя, исходя из опроса компании Sophos, равняется 1,85 млн долл. США[4].

Таким образом, обеспечение информационной безопасности стало одной из ключевых задач как государства, так и любой организации (предприятия) и частных лиц, поскольку пандемия открыла новые возможности, позволившие организованной преступности получить дополнительное финансирование и существенно расширить вариативность атак с помощью фишинга и социальной инженерии, этому способствовал вынужденный переход большинства организаций на удаленный режим работы.

Выстраивая комплексную безопасность, представителям бизнеса необходимо учитывать, что изменилась сама парадигма: сейчас частью инфосистемы стало множество других устройств, которые пользователи умудряются подключить к корпоративным ресурсам. Дистанционный формат работы расширил границы взаимодействия организации со своими сотрудниками, защита данных конкретного человека, даже с личного устройства, стала приоритетом. Это звено в современных реалиях определяет уровень защиты всей организации. Адресные атаки на сотрудников могут превратиться из малой проблемы одного человека в большие инциденты для целой компании или корпорации. Рассматривая вопрос обеспечения информационной безопасности в компаниях, не лишним будет вспомнить о Письме Федеральной службы по техническому и экспортному контролю от 20 марта 2020 г. № 240/84/389[5], в котором сформирован перечень рекомендаций по обеспечению безопасности при реализации дистанционного режима работы в части объектов критической информационной инфраструктуры. Документ адресован госорганам, госучреждениям, российским юридическим лицам и индивидуальным предпринимателям, которым на законном основании принадлежат информсистемы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и т. п., но будет полезен и любым субъектам предпринимательства.

Государством разработан комплекс мер обеспечения информационной безопасности, назовем лишь некоторые наиболее значимые из них, так как этот вопрос требует самостоятельного рассмотрения.

Постановлением Правительства РФ от 15 апреля 2014 г. № 313 «Об утверждении государственной программы Российской Федерации “Информационное общество”»[6] введена в действие и осуществляется указанная государственная программа, содержащая комплексные подпрограммы «Информационно-телекоммуникационная инфраструктура информационного общества и услуги, оказываемые на ее основе», «Информационное государство», «Информационная среда», «Безопасность в информационном обществе».

В рамках реализации указов Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[7] и от 21 июля 2020 г. № 474 «О национальных целях развития Российской Федерации на период до 2030 года»[8] Правительством РФ сформирована национальная программа «Цифровая экономика Российской Федерации», утвержденная протоколом заседания президиума Совета при Президенте

[1] Киберпреступность переросла в пандемию // Ведомости. URL: https://www.vedomosti.ru/forum/technologii_novoj_realnosti/columns/2020/12/02/849244-kiberprestupnost (дата обращения: 11.05.2022)

[2] Check Point. URL: https://research.checkpoint.com/2021/phorpiex-botnet-is-back-with-a-new-twizt-hijacking-hundreds-of-crypto-transactions/ (дата обращения: 22.01.2022).

[3] Ivanti. URL: https://www.ivanti.com/lp/security/reports/ransomware-spotlight-year-end-2021-report (дата обращения: 05.01.2022).

[4] Sophos. URL: https://assets.sophos.com/X24WTUEQ/at/k4qj qs-73jk9256hffhqsmf/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469 (дата обращения: 23.03.2022).

[5] Письмо ФСТЭК России от 20 марта 2020 г. № 240/84/389 // ФСТЭК России. URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/2059-pismo-fstek-rossii-ot-20-marta-2020-g-n-240-84-389 (дата обращения: 23.03.2022).

[6] Об утверждении государственной программы Российской Федерации «Информационное общество» : постановление Правительства РФ от 15 апр. 2015 г. № 313 (в редакции постановления от 31 марта 2021 г. № 504-19) // Собр. законодательства РФ. 2014. № 18. Ст. 2159.

[7] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : указ Президента РФ от 7 мая 2018 г. № 204 (с последующими изм. и доп. от 19 июля 2018 г., 21 июля 2020 г.) // Собр. законодательства РФ. 2018. № 20. Ст. 2817.

[8] О национальных целях и стратегических задачах развития Российской Федерации на период до 2030 года : указ Президента РФ от 21 июля 2020 г. № 474 // Собр. законодательства РФ. 2020. № 30. Ст. 4884.

РФ по стратегическому развитию и национальным проектам от 4 июня 2019 г. № 7. В ее состав входят федеральные проекты: «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление», «Искусственный интеллект», «Обеспечение доступа в Интернет за счет развития спутниковой связи», «Развитие кадрового потенциала ИТ-отрасли», «Цифровые услуги и сервисы онлайн». В ходе ее реализации в период пандемии принят комплекс стандартов информационной безопасности, минимизирующий риски и угрозы безопасного функционирования сетей связи общего пользования с целью обеспечения целостного, устойчивого и безопасного функционирования российского сегмента сети Интернет, разработаны дорожные карты развития «сквозных» цифровых технологий «Технологии беспроводной связи», «Технологии виртуальной и дополненной реальности», «Квантовые технологии», «Нейротехнологии и искусственный интеллект» и другие. Так же Минцифры России приступило к разработке «ГосДата.хаба» – проекта по созданию национального озера данных, объединяющего потоки обезличенных данных госорганов и значительно повышающего их информационную безопасность.

Тема обеспечения информационной безопасности и борьбы с киберпреступностью, которая в последние годы находится в числе ключевых глобальных рисков, особо набрала обороты в период распространения новой коронавирусной инфекции. И если ранее представители отрасли делали акцент на борьбу с кибератаками злоумышленников, то сейчас приоритет отдается именно защите информации и предотвращению возможных угроз. Поэтому необходимо переосмыслить подход к информационной безопасности и максимально сократить «площадь атаки», а уроки, полученные по обеспечению информационной безопасности в период пандемии, использовать и в постпандемический период.

**Обсуждения и заключения**

Делая выводы по рассматриваемой проблеме, отметим, что становление и развитие информационного общества в современной России предопределяют ряд положительных возможностей, но вместе с этим создают ряд негативных и деструктивных последствий, проявивших себя в различных сферах жизнедеятельности общества, особенно в период пандемии COVID-19.

Исследуя информационную безопасность в системе национальной безопасности современной России, резюмируем, что информационная сфера в современных реалиях представляет собой системообразующий фактор жизни общества, оказывает активное влияние на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность нашей страны существенным образом зависит от обеспечения информационной безопасности, а в перспективе с развитием информационно-технического прогресса ее роль будет развиваться и стремительно усиливаться.

Проблемы, возникающие при реализации информационной безопасности, способны постоянно усугубляться процессами проникновения во все сферы общества технических средств обработки и передачи данных. Периодически возникающие сбои в работе компьютерной сети, несомненно, наносят моральный ущерб работникам предприятий и администраторам. Технологии электронных платежей, безбумажный документооборот, перегруженность локальных сетей и другие сбои способны парализовать работу крупных корпораций, предприятий, банков, что может привести к значительным потерям. Защита информации – одна из самых острых проблем современного общества. Информационная сфера влияет на национальные интересы России, формируя стратегические и текущие задачи внутренней и внешней политики государства по обеспечению информационной безопасности страны.

Основные составляющие национальных интересов России в информационной сфере: защита информационных ресурсов от несанкционированного доступа и обеспечение безопасности информационных и телекоммуникационных систем.

Таким образом, информационная безопасность – важнейший компонент, гарантирующий результативное развитие современного информационного общества, входящий в систему национальной безопасности в качестве ее основного элемента. Информационная составляющая присутствует во всех видах безопасности, входящих в структуру национальной безопасности Российской Федерации (государственной, общественной, экономической и других), именно поэтому информационная безопасность, сущность которой заключается в защите от внутренних и внешних информационных угроз, приобретает определяющее значение в системе национальной безопасности нашей страны на современном этапе ее развития.

## СПИСОК ЛИТЕРАТУРЫ


1. Анохина С. Ю., Логинова Т. Д. Информационная безопасность как основной элемент системы национальной безопасности государства // Алтайский юридический вестник. 2016. № 4 (16). С. 20–32.

2. Белл Д. Грядущее постиндустриальное общество: опыт социального прогнозирования: пер. с английского / под ред. В. Л. Иноземцева. 2-е изд., испр. и доп. М. : Academia, 2004. 284 с.

3. Борисов А. Ю. Государственная политика в области информационной безопасности на современном этапе : дис. ... канд. полит. наук. М., 2006. 32 с.

4. Бородин А. С. Информационная безопасность в современной России: политологический анализ : дис. ... канд. полит. наук. СПб., 2009. 42 с.

5. Гриценко А. А. Теоретико-методологические подходы к определению понятия безопасности // Вестник НГУ. Серия: Философия. 2008. Т. 6. С. 87–88.

6. Грозин С. С., Островских Ж. В. Транснациональная организованная преступность в век высоких технологий: основные тенденции развития // Проблемы современного законодательства России и зарубежных стран : материалы IX Международной научно-практической конференции. (г. Иркутск, 16 октября 2020 г.) / отв. ред. А. М. Бычкова, С. И. Суслова. Т. 1. Иркутск : Иркутский институт (филиал) ВГУЮ (РПА Минюста России), 2020. С. 205–209.

7. Демин И. В. Сущность и содержание понятий «безопасность», «общественная безопасность» и «национальная безопасность» // Вестник Екатерининского института. 2009. № 1. С. 29–30.

8. Информационная безопасность России / Е. А. Ерофеев, Ю. С. Уфимцев [и др.]. М. : Издательство Экзамен, 2001. 206 с.

9. Закупень Т. В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. № 4 (110). С. 22–38.

10. Зеленков М. Ю. Теоретико-методологические проблемы теории национальной безопасности РФ. М. : Юридический институт МИИТа, 2013. 210 с.

11. Иванов В. Ф. Массовая коммуникация. Киев : Академия Украинской Прессы, 2013. 514 с.

12. Иноземцев В. Л. Современное постиндустриальное общество: природа, противоречие, перспективы : учебное пособие для студентов вузов. М. : Логос, 2000. 304 с.

13. Кожевников В. В. Конституция РФ и проблемы продовольственной безопасности // Вестник Омского университета. Право. 2015. № 3. С. 50–65.

14. Марков А. А. Некоторые аспекты информационной безопасности в контексте национальной безопасности // Вестник СПбГУ. 2011. Сер. 12. С. Вып. 1. С. 43–48.

15. Маслоу А. На подступах к психологии бытия / пер. О. Чистякова ; под ред. В. Данченко. М. : Рефл-бук, 1997. 134 с.

16. Мичурин А. Н. Исторические аспекты развития информационного общества в России и мире // Новая наука: проблемы и перспективы. 2016. № 6–3 (85). С. 160–176.

17. Недосекова Е. С. Проблемы правовой терминологии в сфере информационной безопасности // Информационные ресурсы России : научно-практический журнал. 2011. № 6. С. 20–34.

18. Овсяникова И. В. Воспроизводство информационных ресурсов в современной экономике России : автореф. дис. … канд. экон. наук. Орел, 2010. 202 с.

19. Смирнов А. А. Критический анализ ревизионистских подходов к определению понятия «безопасность» // Административное право и процесс. 2015. № 5. С. 16–28.

20. Устинович Е. С. Государственная политика в сфере информационных технологий : дис. … д-ра полит. наук. М., 2012. С. 73–74.

21. Хохлова О. М., Рожкова А. К., Хохлова А. В. Информационная безопасность в системе национальной безопасности современного российского общества // Инновационное развитие науки: фундаментальные и прикладные проблемы : монография. Петрозаводск : МЦНП «Новая наука», 2021. 197 с.


## REFERENCES


1. Anokhina S.Yu., Loginova T.D. Informacionnaya bezopasnost' kak osnovnoj element sistemy nacional'noj bezopasnosti gosudarstva [Information security as the main element of the national security system of the state]. *Altajskij yuridicheskij vestnik* [Altai Legal Bulletin], 2016, no. 4 (16), pp. 20-32. (in Russian)

2. Bell D. *Gryadushchee postindustrial'noe obshchestvo: opyt social'nogo prognozirovaniya: per. s anglijskogo. Pod red. V. L. Inozemceva. 2-e izd., ispr. i dop* [Coming post-industrial society: the experience of social forecasting: Per. from English. Ed. V.L. Inozemtseva. 2nd ed., rev. and additional]. Moscow, Academia Publ., 2004, 284 p. (in Russian)

3. Borisov A.Yu. *Gosudarstvennaya politika v oblasti informacionnoj bezopasnosti na sovremennom etape: dis. ... kand. polit. nauk* [State policy in the field of information security at the present stage. Cand. sci. diss.]. Moscow, 2006, 32 p. (in Russian)

4. Borodin A.S. *Informacionnaya bezopasnost' v sovremennoj Rossii: politologicheskij analiz: dis. ... kand. polit. nauk* [Information security in modern Russia: political analysis. Cand. sci. diss.]. Saint Petersburg, 2009, 42 p. (in Russian)

5. Gritsenko A.A. Teoretiko-metodologicheskie podhody k opredeleniyu ponyatiya bezopasnosti [Theoretical and methodological approaches to the definition of the concept of security]. *Vestnik NGU. Seriya Filosofiya* [Vestnik NGU. Ser: Philosophy]. 2008, vol. 6, pp. 87-88. (in Russian)

6. Grozin S.S., Ostrovskih Zh.V. *Transnacional'naya organizovannaya prestupnost' v vek vysokih tekhnologij: osnovnye tendencii razvitiya* [Problems of modern legislation of Russia and foreign countries: mater. IX International Scientific and Practical Conference (Irkutsk, October 16, 2020)] managing editor. A.M. Bychkova, S. I. Suslova. T. Vol. 1.] Irkutsk, Irkutsk Institute (branch) VGUYU (RPA of the Ministry of Justice of Russia), 2020, pp. 205-209. (in Russian)

7. Demin I.V. [The essence and content of the concepts of "security", "public security" and "national security"]. *Vestnik Ekaterininskogo instituta* [Bulletin of the Catherine Institute], 2009, no. 1, pp. 29-30. (in Russian)

8. Erofeev E.A., Ufimtsev Yu.S. et al. *Informacionnaya bezopasnost' Rossii* [Information security of Russia]. Moscow, Exam Publ., 2001, 206 p. (in Russian)

9. Zakupen T.V. Ponyatie i sushchnost' informacionnoj bezopasnosti i ee mesto v sisteme obespecheniya nacional'noj bezopasnosti RF [The concept and essence of information security and its place in the system of ensuring the national security of the Russian Federation]. *Informacionnye resursy Rossii* [Information resources of Russia]. 2009, no. 4 (110), pp. 22-38. (in Russian)

10. Zelenkov M.Yu. *Teoretiko-metodologicheskie problemy teorii nacional'noj bezopasnosti RF* [Theoretical and methodological problems of the theory of national security of the Russian Federation]. Moscow, Law Institute of MIIT Publ., 2013, 210 p. (in Russian)

11. Ivanov V.F. *Massovaya kommunikaciya* [Mass communication]. Kiev, Academy of Ukrainian Publ., 2013, 514 p. (in Russian)

12. Inozemtsev V.L. *Sovremennoe postindustrial'noe obshchestvo: priroda, protivorechie, perspektivy: ucheb. posobie dlya studentov vuzov* [Modern post-industrial society: nature, contradiction, prospects: textbook. allowance for university students]. Moscow, Logos Publ., 2000, 304 p. (in Russian)

13. Kozhevnikov V.V. The *Konstituciya RF i problemy prodovol'stvennoj bezopasnosti* [Constitution of the Russian Federation and the problems of food security]. *Vestnik Omskogo universiteta. Pravo* [Bulletin of the Omsk University], Right, 2015, no. 3, pp. 50-65. (in Russian)

14. Markov A.A. Nekotorye aspekty informacionnoj bezopasnosti v kontekste nacional'noj bezopasnosti [Some aspects of information security in the context of national security], *Vestnik SPbGU* [Bulletin of St. Petersburg State University]. 2011, Ser. 12. S. Iss. 1, pp. 43-48. (in Russian)

15. Maslow A. *Na podstupah k psihologii bytiya. Per. O. Chistyakova, pod red. V. Danchenko* [On the approaches to the psychology of being]. Moscow, Refl-book Publ., 1997, 134 p. (in Russian)

16. Michurin A.N. Istoricheskie aspekty razvitiya informacionnogo obshchestva v Rossii i mire [Historical aspects of the development of the information society in Russia and the world]. *Novaya nauka: problemy i perspektivy* [New science: problems and prospects], 2016, no. 6-3 (85), pp. 160-176. (in Russian)

17. Nedosekova E.S. Problemy pravovoj terminologii v sfere informacionnoj bezopasnosti [Problems of legal terminology in the field of information security]. *Informacionnye resursy Rossii: nauchno-prakticheskij zhurnal* [Information resources of Russia: a scientific and practical journal], 2011, no. 6, pp. 20-34. (in Russian)

18. Ovsyanikova I.V. *Vosproizvodstvo informacionnyh resursov v sovremennoj ekonomike Rossii: avtoref. dis. … kand. ekon. nauk* [Reproduction of information resources in the modern economy of Russia. Cand. sci. diss.]. Orel, 2010. 202 p. (in Russian)

19. Smirnov A.A. Kriticheskij analiz revizionistskih podhodov k opredeleniyu ponyatiya "bezopasnost'" [Critical analysis of revisionist approaches to the definition of the concept of "security"]. *Administrativnoe pravo i process* [Administrative law and process], 2015, no. 5, pp. 16-28. (in Russian)

20. Ustinovich E.S. *Gosudarstvennaya politika v sfere informacionnyh tekhnologij: dis. … d-ra polit. nauk* [State policy in the field of information technology. Cand. sci. diss.]. Moscow, 2012, pp. 73-74. (in Russian)

21. Khokhlova O.M., Rozhkova A.K., Khokhlova A.V. Informacionnaya bezopasnost' v sisteme nacional'noj bezopasnosti sovremennogo rossijskogo obshchestva [Information security in the national security system of modern Russian society]. *Innovacionnoe r azvitie nauki: fundamental'nye i prikladnye problemy: monografiya* [Innovative development of science: fundamental and applied problems]. Petrozavodsk, MTsNP "New Science" Publ., 2021, 197 p. (in Russian)

*Статья поступила в редакцию* 14.01.2022; *одобрена после рецензирования* 21.02.2022; *принята к публикации* 13.05.2022.

*Received on* 14.01.2022; *approved on* 21.02.2022; *accepted for publication on* 13.05.2022.

**Островских Жанна Владимировна** – кандидат юридических наук, доцент, доцент кафедры уголовного права, Юридический институт, Иркутский государственный университет (Россия, 664003, г. Иркутск, ул. Карла Маркса, 1), ORCID: 0000-0002-5663-6230, ResearcherID: ABE-1420–2021, e-mail: zh888@yandex.ru

**Ostrovskikh Zhanna Vladimirovna** – Candidate of Juridical Sciences, Associate Professor, Associate Professor of the Department of Criminal Law, Institute of Law, Irkutsk State University (1, K. Marx st., Irkutsk, 664003, Russian Federation), ORCID: 0000-0002-5663-6230, ResearcherID: ABE-1420-2021, e-mail: zh888@yandex.ru

**Хохлова Ольга Михайловна** – кандидат философских наук, доцент, доцент кафедры уголовного права, Восточно-Сибирский филиал Российского государственного университета правосудия (Россия, 664074, г. Иркутск, ул. Ивана Франко, 23-а), e-mail: chochlovaolga-17@mail.ru

**Khokhlova Olga Mikhailovna** – Candidate of Philosophy Sciences, Associate Professor, Associate Professor of the Department of Criminal Law, East Siberian branch of The Russian State University of Justice (23-a, Ivan Franko st., Irkutsk, 664074, Russian Federation), e-mail: chochlovaolga-17@mail.ru

**Рожкова Анна Константиновна** – преподаватель кафедры правового обеспечения национальной безопасности, Институт государства и права, Байкальский государственный университет (Россия, 664003, г. Иркутск, ул. Ленина, 11), ORCID: 0000-0003-1999-4212, ResearcherID: ABE-3810–2021, e-mail: rannette@mail.ru

**Rozhkova Anna Konstantinovna** – Lecturer, Department of Legal Support of National Security, Institute of State and Law, Baikal State University (11, Lenin st., Irkutsk, 664003, Russian Federation), ORCID: 0000-0003-1999-4212, ResearcherID: ABE-3810-2021, e-mail: rannette@mail.ru