МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.05.01 Правовое обеспечение национальной безопасности
(код и наименование направления подготовки, специальности)

Государственно-правовая
(направленность (профиль)/специализация)

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Правовая политика в сфере государственной безопасности»

Обучающийся С.В. Швагерус
(Инициалы Фамилия) (личная подпись)

Руководитель к.ю.н. К.П. Федякин
(ученая степень (при наличии) , ученое звание (при наличии) , Инициалы Фамилия)

Тольятти 2022

## Аннотация

Актуальность темы исследования обусловлена необходимостью более ясного легального определения категорий «государственная безопасность» и «общественная безопасность» и разработки комплекса мер для эффективного обеспечения государственной и общественной безопасности с учетом данной конкретизации рассматриваемых категорий.

Цель исследования - выявление особенностей механизма правовой политики в сфере государственной безопасности, анализ оснований и практики ответственности за совершение информационных правонарушений, а также формирование предложений по совершенствованию правового регулирования данной сферы правоотношений.

Для достижения данной цели были поставлены следующие задачи:

- рассмотреть понятие, сущность государственной безопасности
- раскрыть особенности обеспечения государственной безопасности посредством правовой политики
- привести понятие информационной безопасности, ее правовые основы
- обозначить правовую политику в сфере обеспечения информационной безопасности Российской Федерации

Объектом настоящего исследования являются общественные отношения, возникающие в сфере информационных правонарушений как угрозы национальной безопасности.

Предмет исследования – законодательство, регламентирующее национальную безопасность, а также правонарушения в сфере информационной безопасности, научные труды по данному вопросу и материалы правоприменительной практики.

Исследование состоит: из введения, основной части из двух глав, заключения, списка использованной в процессе работы литературы.

**Оглавление**

# Введение

Актуальность темы исследования. Одной из первостепенных государственных задач современности является обеспечение национальной безопасности, государственная и общественная безопасность являются неотъемлемыми и ключевыми составляющими системы национальной безопасности.

Постоянно растущая угроза национальной безопасности, а, как следствие, государственной и общественной безопасности определяет необходимость совершенствования системы их обеспечения на законодательном и практическом уровне.

Однако, вопрос соотношения и понятия данных категорий в юридической науке не столь однозначен, поскольку четкого научного подхода к вышеописанным категориям не выработано. Отсутствие легальных формулировок препятствует определению четкого соотношения между понятиями общественной, государственной и национальной безопасности.

Актуальность темы исследования обусловлена необходимостью более ясного легального определения категорий «государственная безопасность» и «общественная безопасность» и разработки комплекса мер для эффективного обеспечения государственной и общественной безопасности с учетом данной конкретизации рассматриваемых категорий.

Современное российское общество, развиваясь в сторону демократического рыночного государства, неизбежно стремится перейти от исключительно силовых к административно-правовым методам обеспечения информационной безопасности и информатизации. Информационная безопасность по своей сути является одной из форм проявления всеобщего стремления всех субъектов к стабильности и надежности. В данной сфере, концентрируются интересы всех субъектов хозяйствования от государства до отдельного гражданина.

С позиций национальной безопасности России именно информационная безопасность наиболее слабое звено. Она переживает трудный и противоречивый процесс трансформации в новое состояние, порождающий серьезные проблемы во всех сферах общества. Результаты развития связи и информатизации на современном этапе показали, что Россия пока не может преодолеть состояние незащищенности в области телекоммуникации. Россия все еще отстает от развитых стран по уровню информационной безопасности страны и общества, что значительно затрудняет ее современное состояние.

Указанные моменты обусловили необходимость нового концептуального подхода к проблемам обеспечения информационной безопасности в рамках государственной политики.

Теоретическая основа формирования правовых норм может базироваться на подходе, в рамках которого информационная безопасность представляется как социальное явление, в основе которого лежат интересы субъектов общественных отношений, каковыми являются человек, общество и государство.

Правонарушения, связанные с компьютерной информацией, получают все большее распространение во всем мире, и наша страна не является здесь исключением. Полагаем, что достаточно большое число таких деяний обусловлено развитием научно – технического прогресса, внедрения компьютерных технологий во все сферы жизнедеятельности, все большее число лиц использует электронные средства платежа, имеет к ним доступ с помощью различных приложений, работающих от сети Интернет. При этом, компьютерные технологии используются и на планшетах, смартфонах, множествах различных устройств, в классическом понимании к компьютерной технике не относящихся.

Следует с сожаление констатировать, что компьютерные технологии не только позволяют облегчить жизнь граждан, оптимизировать различные виды деятельности, но и активно используются преступниками в

криминальных целях. Появляются новые способы совершения преступлений, связанных с компьютерными технологиями, а также новые виды преступлений, посягающие на различные объекты, охраняемые уголовно – правовыми нормами. Несмотря на это, при практической реализации привлечения к ответственности за совершение информационных правонарушений, продолжают возникать различные проблемы, связанные как с определением признаков данного состава преступления, так и с отграничением его от смежных деяний, что, по нашему мнению, обусловлено несовершенством действующего законодательства. В некоторой степени это возможно объяснить тем фактом, что в целом в нашей стране отсутствует длительный накопленный опыт борьбы с различными правонарушениями в сфере информационных технологий, а также и тем фактом, что до настоящего времени информационное законодательство в целом в Российской Федерации находится в стадии своего развития.

Несмотря на проводимые исследования, все больше имеющие место в последние годы, разрешить имеющие проблемы в полной мере так и не удается, что находит свое проявление как в дискуссиях среди исследователей по рассматриваемым вопросам, до настоящего времени не пришедших к единому мнению по многим аспектам, так и в разнообразии судебной практики. Все это определяет востребованность и актуальность темы.

Степень научной разработанности темы. Вопросы обеспечения государственной и общественной безопасности являлись и являются предметом изучения ученых, таких как Р.Д. Сипок, А.Д. Градовский, Н.Я. Данилевский, К.Н. Леонтьев, П.Б. Струве и др. Однако, отмечая значительный накопленный опыт названных авторов применительно к теме исследования, необходимо признать потребность более детального рассмотрения вопросов, касающихся обеспечения государственной и общественной безопасности.

Степень научной разработанности темы исследования: в отечественной и зарубежной юридической науке к настоящему времени имеются

многочисленные исследования, которые посвящены общим проблемам, связанным с информационной безопасностью и её обеспечением.

Цель исследования выявление особенностей механизма правовой политики в сфере государственной безопасности, анализ оснований и практики ответственности за совершение информационных правонарушений, а также формирование предложений по совершенствованию правового регулирования данной сферы правоотношений.

Для достижения данной цели были поставлены следующие задачи:

- рассмотреть понятие, сущность государственной безопасности;
- раскрыть особенности обеспечения государственной безопасности посредством правовой политики;
- привести понятие информационной безопасности, ее правовые основы;
- обозначить правовую политику в сфере обеспечения информационной безопасности Российской Федерации.

Объектом настоящего исследования являются общественные отношения, возникающие в сфере информационных правонарушений как угрозы национальной безопасности.

Предмет исследования – законодательство, регламентирующее национальную безопасность, а также правонарушения в сфере информационной безопасности, научные труды по данному вопросу и материалы правоприменительной практики.

Методами исследования стали: диалектический метод научного познания социальных явлений; методы анализа и синтеза; исторический, сравнительно-правовой, формально-логический, системный, формально-юридический, сравнительно-правовой методы исследования. В целом, методологический аппарат, с помощью которого проводилось научное исследование поставленных вопросов, включает в себя несколько приемов научного анализа диалектического характера. В исследовании применялись и другие специальные методы: функциональный анализ правовых явлений, системно-структурный подход и др.

Теоретическую основу работы составили научные труды С.С. Аветисяна, В.В. Воробьева, А.А. Гребенькова, М.Ю. Дворецкого, А.М. Доронина, К.Н. Евдокимова, В.С. Зайцева, С.Н. Клокова А.П. Кузнецова, С.М. Паршина, В.П. Числина и др.

Нормативную базу исследования составили нормы уголовного законодательства, иных федеральных законов и нормативно – правовых актов в Российской Федерации.

Теоретическая значимость исследования заключается в выработке научных положений о конструкции информационных правонарушений как угрозы национальной безопасности, предложений по совершенствованию законодательства. Полученные результаты могут быть использованы в дальнейших научных исследованиях, при подготовке учебной и научной литературы, а также в учебном процессе.

Практическая значимость исследования заключается в возможности применения его теоретических выводов, предложений и рекомендаций в повышении эффективности правоприменительной деятельности, связанной с информационными правонарушениями как угрозы национальной безопасности.

Теоретическим и практическим значением обладают следующие направления осуществленного исследования:

- на основании обзора нормативных правовых актов защиты информации мы выделили четыре уровня правовой основы защиты информации;
- рассмотрели информационную безопасность в российской федерации как одну из составляющих национальной безопасности государства;
- показали ряд особенностей юридической ответственности за нарушения законодательства, регулирующего отношения в информационной сфере;

- на основании выявленных проблем уголовно-правовой ответственности за информационные преступления предложили пути совершенствования обеспечения информационной безопасности в структуре национальной безопасности.

Для достижения целей и задач исследования была определена следующая структура работы.

Исследование состоит: из введения, где поставлена цель исследования и задачи для ее достижения, а также определены актуальность и необходимость исследования; основной части из двух глав, где непосредственно раскрываются основные положения рассматриваемого вопроса; заключения, где подводится итог проделанной работе; списка использованной в процессе работы литературы.

# Глава 1 Государственная политика как средство обеспечения государственной безопасности

## 1.1 Понятие, сущность государственной безопасности

Государственная безопасность – важнейшая составляющая национальной безопасности, связанная с защитой государственного суверенитета и территориальной целостности, основ конституционного строя, правовой системы и системы управления.

В правовом государстве понятия «государственная безопасность» и «национальная безопасность» обычно употребляются как синонимы. В то же время государственная безопасность чаще относится к системам управления и институтам государства, обороне и государственной тайне, а национальная безопасность – к духовной, нравственной, экологической сторонам жизни нации.

Необходимо отметить, что широкое использование ключевых категорий «безопасность», «государственная безопасность», «национальная безопасность» в различных правовых и политических аспектах создает впечатление не только научно-практической значимости и актуальности соответствующих вопросов, но и одновременно их достаточной разработанности. Однако приходится констатировать, что четкого научно обоснованного подхода, как к содержанию, так и к соотношению этих понятий на сегодняшний день не выработано.

Отметим, прежде всего, что при рассмотрении вопросов безопасности личности, общества и государства в нормативных правовых актах и юридической литературе используются различные термины: «безопасность» в Законе Российской Федерации «О безопасности»; «национальная безопасность»; «государственная безопасность»; «безопасность страны» [2].

Ситуация усугубляется отсутствием легальных (нормативных) формулировок и определений, поскольку законодатель дает определение

понятия безопасность, не уточняя соотношения его с понятиями «государственная безопасность» и «национальная безопасность» и понимает под безопасностью состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, не уточняя при этом, о каком виде безопасности - национальной или государственной - идет речь, равно как и необходимо ли вообще проводить между ними различие.

В результате складывается парадоксальная ситуация, поскольку одни авторы, анализируя содержание понятия «безопасность», закрепленное в федеральном законодательстве, делают вывод, что речь идет о государственной безопасности, другие этому же понятию (определению) придают характер национальной безопасности. Во многом это объясняется стремлением законодателя увязать в предлагаемом определении интересы государства, личности, общества, в то время как эти интересы могут и расходиться.

В этой связи, обеспечение безопасности государства следует определять, как комплекс мероприятий, политической, экономической, социально-правовой и военной направленности, цель реализации которой состоит в защите существующего общественно-политического строя, неприкосновенности территории и обеспечении независимости государства от негативной деятельности иностранных государств, а также от противников существующего строя внутри страны.

Одной из явных дискуссионных тем является исследование вопроса о взаимозамещении определений «национальная безопасность» и «государственная безопасность». Если не углубляться в историографию проблемы, и признать, как данность наличие различных (порой диаметрально противоположных) позиций по указанному вопросу, то такое положение дел можно объяснить историческими особенностями развития российской государственности, где указанное соотношение устанавливала

наличествующая в нашей стране на данный момент времени ведущая политико-правовая сила.

В частности, в советскую эпоху, существовало официально признанное, но отличное от современного, объяснение термина «нация». Исходя из него употребление такого словосочетания, как «национальная безопасность» в контексте безопасности какого-то отдельно рассматриваемого этноса было невозможно. Подобный подход воспринимался бы как стремление в нашей многонациональной стране возвысить одну нацию над другими. Это не «вписывалось» в национальную политику Коммунистической партии, так как могло разрушить основу СССР– признание равноправия всех наций и народностей, проживающих в Советском Союзе. Поэтому общепринятым являлся термин «государственная безопасность», соответственно, понятие «национальная безопасность» популярностью не пользовалось [6].

И в современной науке, к сожалению, продолжают играть роль отголоски политических дискуссий постсоветской эпохи. Деиделогизация создала ситуацию, в которой понятие «государственная безопасность» «вышло из моды», так как воспринималось исключительно как охрана базовых ценностей социалистического строя.

Определенную ясность, как мы уже указывали, внесла Стратегия национальной безопасности 2015 года, в которой спор о возможности взаимозамены терминов «государственная» и «национальная» безопасность решен в пользу невозможности указанного действия.

Отождествлять понятия «национальная безопасность» и «государственная безопасность» невозможно.

Во-первых, это приведет к ограничению смысла понятия «национальная безопасность»; во-вторых, такое отождествление опасно, т.к. государство имеет объективную тенденцию к превращению в самодовлеющую силу, которая может выйти из- под контролем гражданского общества. Кроме того, использование понятия «государственная

безопасность» позволяет «проводить грань между «государственной» и «негосударственной» безопасностью». Другими словами, государственная безопасность является «высшим срезом» национальной безопасности, поэтому ее нельзя соотносить с другими видами безопасности.

Что касается научного оформления категории «государственная безопасность», то и здесь особое внимание следует обратить на XIX столетие. Традиционалистическая теория Н.М. Карамзина и М.М. Сперанского позволили сформировать первое в российской науке представление о безопасности государства, где государственная безопасность рассматривалась как национальная и включала в себя национальный интерес, национальный дух и идею.

Во второй половине XIX века появились теории, рассматривавшие безопасность как комплексное явление. А.Д. Градовский понимал безопасность через национальную идею; Н.Я. Данилевский и К.Н. Леонтьев рассматривали теорию безопасности через установление многонационального государства при активной политике отдельных национальностей; П.Б. Струве видел в содержании понятия безопасность степень реализации национальных интересов на международной арене. Новым подходом к пониманию государственной безопасности стали взгляды Б.Н. Чичерина, который представлял, как необходимость обеспечения государством общегражданских прав и свобод, в первую очередь политических и социальных.

В общем виде к началу XX века безопасность рассматривалась и как внешняя, то есть защита государственной независимости и границ империи и как внутренняя, то есть подавление смуты, оппозиции, заговоров, преступности. Но ни один нормативный акт не делал попыток дать юридическое токование дефиниции «государственная безопасность». Данная традиция сохранилась и в последующий, советский период. После октябрьской революции более всего обращали внимание именно на государственную безопасность.

Общепризнанным считается факт, что законодательное оформление в июле 1934 года понятия «государственная безопасность» является одним из наиболее ярких признаков огосударствления общества, то есть установления государственного контроля за всеми сферами его жизни: экономической, политической, идеологической (духовной), военной и другими.

Особенно давлеющим был идеологический контроль над общественной жизнью и выполнением советскими гражданами своих обязанностей.

Научное исследование понятия «государственная безопасность» отличалось рядом особенностей:

- приоритетной идеологической направленностью;
- хронологической неравномерностью. Попытки основательного анализа рассматриваемой категории в специальной юридической литературе стали возможны и проявились только в 50-х годах XX века;
- недоступностью для всех желающих заниматься исследованием тематики, связанной с государственной безопасностью.

Государством охраняются права и свободы человека и гражданина, отношения собственности, семья и т.п. Однако данные «ценности» скорее принадлежат объектам национальной, нежели государственной безопасности. Представляется ему спорным и использование термина «конфликт». Конфликт, как правило, означает противоречие во взглядах, разногласие, спор. В процессе повседневной деятельности государства возникает множество конфликтов с иными государствами, политическими структурами, общественными организациями, а также отдельными гражданами. Но далеко не все конфликты подпадают под обеспечение государственной безопасности, а лишь те из них, которые несут в себе реальную угрозу объектам государственной безопасности.

Таким образом, мы можем сделать вывод о том, что понятия «государственная безопасность» и «национальная безопасность» не равны. В то же время государственная безопасность - ключевая составляющая

системы национальной безопасности, которая не может быть приравнена к иным видам национальной безопасности.

## 1.2 Обеспечение государственной безопасности посредством правовой политики

Безопасность как один из фундаментальных устоев общества и государства зиждется на прочных правовых основах: Конституции РФ, федеральных законах, нормативных правовых актах, издаваемых самими органами безопасности. В обеспечении безопасности участвуют в той или иной степени все органы государственной власти: Президент РФ, Федеральное Собрание, Правительство РФ.

В Конституции РФ упоминается такая отрасль (область), сфера управления, как безопасность. В частности, в ч. 5 ст. 13 Конституции говорится о безопасности государства; в ч. 2, 3 ст. 35 -также о безопасности государства; в п. «л» ст. 71 - об отнесении к ведению РФ безопасности; в п. «д» ст. 114 подчеркнуто, что Правительство РФ осуществляет меры по обеспечению государственной безопасности.

Национальные интересы Российской Федерации – совокупность внутренних и внешних потребностей государства в обеспечении защищенности и устойчивого развития личности, общества и государства.

Интересы личности заключаются в реализации конституционных прав и свобод, в обеспечении личной безопасности, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина. Интересы общества заключаются в упрочении демократии, в создании правового, социального государства, в достижении и поддержании общественного согласия, в духовном обновлении России. Интересы государства заключаются в незыблемости конституционного строя, суверенитета и территориальной целостности России, в политической, экономической и социальной стабильности, в безусловном обеспечении

законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

К основным объектам национальной безопасности относятся:

– личность – ее права и свободы;
– общество – его материальные и духовные ценности;
– государство – его конституционный строй, суверенитет и территориальная целостность

Основным субъектом обеспечения безопасности является государство, осуществляющее функции в этой области через органы законодательной, исполнительной и судебной властей. Государство обеспечивает безопасность каждого гражданина на территории РФ. Гражданам Российской Федерации, находящимся за ее пределами, государством гарантируется защита и покровительство.

Информационная безопасность обозначается, в первую очередь, способностью государства создавать полные и защищенные информационные ресурсы для полного функционирования, а также умению сопротивляться информационным угрозам, направленным на технические источники информации. Еще одним немаловажным пунктом является наличие грамотно выработанных навыков безопасного поведения в сети Интернет [12].

Вопросы информационной безопасности имеют в настоящее время первостепенное значение. И это неудивительно, поскольку в современном информационном обществе от уровня информационной безопасности напрямую зависит степень развития общественных отношений и самого социума. Таким образом, все аспекты информационной безопасности сегодня довольно актуальны. К сожалению, большинство исследователей, рассматривавших проблемы, касающиеся информационной безопасности, обычно акцентируют внимание на технической или юридической стороне вопроса, упуская из виду многие психолого-педагогические и личностные моменты. Поэтому представляется необходимым восполнить данный пробел.

В современном обществе сложно представить хоть одну сферу жизни, которая функционирует без информационной структуры. практически всё, что связано с информацией, входит в информационную среду общества и нуждается в обеспечении безопасности, т.е. информационная безопасность представляет собой глобальную проблему. Особое значение информационная безопасность приобретает в сфере воспитания подрастающего поколения, что обусловлено, прежде всего, низким уровнем информационной культуры детей и молодежи. Следует отметить, что информационная культура личности представляет собой довольно сложное понятие, неоднозначное трактуемое в отечественной науке. Чаще всего под информационной культурой понимается такой уровень знаний, умений и навыков человека, который позволяет достаточно эффективно осуществлять взаимодействие с информационной средой.

В настоящее время современное общество называют информационным, а каждое государство развивает информационные технологии и переходит на путь цифровизации экономики. Для России информационная среда и информационная безопасность являются новыми явлениями. Цифровая среда в РФ только развивается и растет темпами выше, чем обычная экономика.

Информационная безопасность является одним из элементов системы национальной безопасности, обеспечение которой является одним из приоритетов государственной политики России. В связи с развитием информационной среды в России актуализировали и проблемы обеспечения информационной безопасности в стране.

В настоящее время существуют проблемы в правовом регулировании процесса обеспечения информационной безопасности, поскольку еще не сформирована база, которая бы являлась основой регулирования данного процесса, как это осуществляется с большинством сфер деятельности в РФ. Информационная безопасность государства включает в себя все уровни реализации (личности, общества, страны). В последние годы все больше людей пользуются Интернетом, совершают покупки в Интернет-магазинах,

обучаются, работают, совершают сделки и занимаются еще десять лет назад непривычными для сети вещами. В настоящее время же информация и информационные ресурсы являются неотъемлемой частью жизни каждого человека. Как у каждого человека, так и, конечно же, у всего государства есть информация, которая требует защиты от стороннего использования. Существует такое понятие как тайна личности, государственная тайна. Такую информацию необходимо защищать, и не позволять все возможные источники угроз, которые могут помешать ее сохранности.

Как часть системы национальной безопасности, информационная безопасность оказывает серьезно воздействие на все сферы деятельности России и защищенности ее интересов в этих сферах [40].

В федеральном законе от 28 декабря 2010 года №390-ФЗ «О безопасности» (далее – Закон о безопасности [34]) не раскрывается легальное определение безопасности. Отметим, что данное положение является серьезным упущением законодателя, т.к. в ранее действовавшем законе РФ от 5 марта 1992 года №2446-1 «О безопасности» это понятие было легализовано. Старый Закон о безопасности под безопасностью понимал состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Данное определение не было удачным, т.к. было достаточно широким. Однако, в ранее действовавшем законодательстве законодателем хотя бы предпринимались попытки легализации понятия «безопасность». По каким соображениям на современном этапе законодатель отказался от этого является непонятным.

Понятие «безопасность» раскрывается в других нормативно-правовых актах. Так, в Соглашении правительств государств-членов Евразийского экономического сообщества о проведении согласованной политики в области технического регулирования, санитарных и фитосанитарных мер от 25 января 2008 года безопасность рассматривается как отсутствие недопустимого риска, связанного с возможностью причинения вреда и (или) нанесения ущерба.

Невозможно не согласиться с точкой зрения Л.К. Терещенко и О.И. Тиунова, которые считают, что основная отличительная черта двух вышеуказанных позиций относительно понятия «безопасности» проявляется в том, что в первом случае законодатель в качестве определяющего элемента указал на субъект защиты, а во втором примере – на объект защиты [58].

Основной признак безопасности как правовой категории – это ее комплексность. Безопасность может применяться в отношении различных сфере жизнедеятельности. Так, выделяются такие виды безопасности как внешняя и внутренняя (национальная) безопасность (данный вид касается направленности угроз), военная безопасность, гуманитарная безопасность, экологическая безопасность и т.п. Информационная безопасность является одной из разновидностей безопасности [19].

Легальное определение «информационная безопасность» было прописано в ранее действовавшей Доктрине информационной безопасности Российской Федерации, утвержденной Президентом РФ 9 сентября 2000 года №Пр-189. Законодатель под информационной безопасностью понимал «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [55].

В научной среде дискуссионным является вопрос определения содержания терминов «информационная безопасность личности». Решение этого вопроса сопутствует обсуждениям более общего и широкого понятия «информационная безопасность», а также его различий от понятия «кибербезопасность». В научной среде также отсутствует единство по поводу объектов и субъектов информационной безопасности [30].

К основным объектам информационной безопасности следует отнести следующие: Во-первых, юридический статус субъектов информационной безопасности. В данный блок входят правомочия субъектов информационной безопасности. Во-вторых, информационные сведения, которые носят особую культурную ценность. В-третьих, информационная инфраструктура. Этот

блок представлен в форме различных библиотек, архивов, музеев и т.п. В-четвертых, информация в виде сообщений. К примеру, распространение различного рода документов [27].

В целом к угрозам России в информационной сфере можно отнести следующее:

- передача секретной информации по телекоммуникационным каналам;
- распространение заведомо ложной информации;
- нарушение охраняемых законом различного вида тайн (к примеру, личной, семейной тайны и т.п.) [7];
- различного рода нарушения при передаче данных;
- хищение важной информации;
- использование незаконных видов защиты информации;
- незаконный доступ к информации ограниченного характера;
- внедрение вредоносного программного обеспечения, которое наносит серьезный вред информационным системам;
- внедрение устройств, которые осуществляют незаконный перехват информации, а также их внедрение в государственные информационные системы;
- нелегальный сбор, а также использование информационных данных.

В целом стоит отметить, что информационная безопасность реализуется при помощи применения как общих, так и специальных принципов. Среди специальных принципов следует особо выделить принципы гласности, сохранения различных видов тайн (имеется ввиду семейная, личная и т.п.), гуманизма и т.п.

С внедрением процессов цифровизации в различные сферы жизни общества, проблема сохранности информации и различных баз данных стоит особенно остро. При этом обеспечение информационной безопасности представляется насущной задачей именно для государства, стремящегося не только защитить права своих граждан в информационном пространстве, но и

сохранить за собой традиционные властные полномочия, не будучи сведенным в своей роли до провайдера услуг.

Иначе говоря, информационная безопасность – это ключевое условие построения модели цифрового государства, при котором последнее сохраняет свой национальный суверенитет в контексте глобализации современного мира.

Правовое обеспечение информационной безопасности представлено органами государственной власти, осуществляющими деятельность в информационной безопасности на правовой основе и саму деятельность по обеспечению защиты информации внутри государства.

Правовое регулирование информационной безопасности в Российской Федерации осуществляется различными нормативно-правовыми актами.

Нормативно-правовая база обеспечения информационной безопасности в России состоит из статей Конституции РФ, которые содержат информацию о правах и свободах граждан, федеральных законов, постановлений Правительства, указов Президента, нормативно-правовых актов субъектов РФ, в которых отражены цель, задачи, принципы, проблемы и направления обеспечения защиты информации в России.

В Конституции Российской Федерации институт цифровизации не закреплен, речь идет только об информации.

Однако общественные отношения развиваются, и в современном мире, где все чаще применяются цифровые алгоритмы, данные технологии стали нуждаться в правовом оформлении [13].

Прежде всего, основные положения и понятия, связанные с внедрением информационно-коммуникационных цифровых технологий, получили свое закрепление в Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации" [43].

Главной причиной формирования информационного общества принято считать развитие информационной и вычислительной техники, т.к появление

информационных технологий значительно снизило стоимость обработки и хранения информации. Создание национальных информационных структур привело к необходимости создания глобальной информационной инфраструктуры. Для решения данной задачи потребовала международного сотрудничества, целью которого стало обеспечение гражданам возможностей для доступа к глобальной информационной структуре. Все это способствовало созданию принципов, которые характеризуют глобальное информационное общество. Во-первых, это обеспечение справедливой конкуренции и поощрение частных инвестиций. Во-вторых, создание таких условий, которые обеспечат равенство возможностей для всех граждан при доступе к информационным услугам. В-третьих, четко отлаженное международное сотрудничество, где особое внимание уделяется развивающимся странам.

В соответствии с Указом Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [41], необходимо развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Указом Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» сформирована национальная программа «Цифровая экономика Российской Федерации» [36]. Указом также закреплена необходимость урегулирования сквозных для различных отраслей законодательства, в том числе для уголовного права, вопросов, связанных с идентификацией субъектов правоотношений в цифровой среде, электронным документооборотом, оборотом данных, в том числе персональных.

В 2019 году Указом Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации", была принята

Национальная стратегия развития искусственного интеллекта на период до 2030 года" [38]. В науке уголовного права разработан ряд определений искусственного интеллекта, а также его свойств [29]. Однако общепринятого понимания искусственного интеллекта в настоящее время еще не разработано.

Интерес вызывает вопрос о мерах, предпринимаемых государством для защиты информационной безопасности.

Так, 15 января 2013 года Президент РФ подписал Указ №31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [39].

Среди задач, стоящих перед государством, по вопросам противодействия киберугрозам стоят:

– поиск «дыр» в сфере информационной безопасности нашей страны; Во-вторых, осуществление координационных связей с другими субъектами информационной сферы по вопросам противодействия киберугрозам современности;

– реализация различных контрольных мероприятий, направленных на обнаружение «дыр» в информационной безопасности нашей страны;

– поиск, а также устранение компьютерных проблем, которые ослабляют информационную безопасность в нашей стране [55].

Важным документом в сфере информационной безопасности выступает указ Президента РФ от 22 мая 2015 года №260 «О некоторых вопросах информационной безопасности Российской Федерации» [37]. В Указе говорится о том, что ФСО России осуществляет мероприятия по преобразованию интернета для органов государственной власти в российскую систему. Это необходимо для защиты каналов связи при помощи использования шифровальных средств.

Информационные технологии оказывают большое влияние на общество и государство. Информационная политика государств направлена

на обеспечение информационной безопасности в стране. Интернет помимо пользы может нанести и вред информационной безопасности.

Обеспечение информационной безопасности осуществляется при помощи реализации различных мер правового, социального, экономического характера.

Таким образом, информационная безопасность является частью системы национальной безопасности и состоит из следующих структурных элементов.

Во-первых, защиты информационных ресурсов государства от несанкционированного доступа. Во-вторых, развитии телекоммуникационных и информационных технологий. В-третьих, соблюдении конституционных свобод и прав граждан в области получения и пользования информацией.

Информационная безопасность обладает специфическим набором идентификационных признаков:

- информационная безопасность проявляется только при одновременном обеспечении заданного уровня безопасности всех прав и интересом, которые реализуемы субъектов рассматриваемых отношений;
- информационная безопасность является таким состоянием, которое характеризует защищенность определенной совокупности прав и интересов данных информационных отношений от воздействия различных видов угроз;
- права и интересы субъектов представляют собой, как правило, развивающуюся систему;
- технологической же основой развития прав и интересов являются процессы информатизации;
- итог обеспечения информационной безопасности – это создание условий, при которых на заданный вектор не оказывают никакого отрицательного влияния как внешние, так и внутренние факторы.

Информационная безопасность - деятельность государства и общества, направленную на защиту определенной совокупности прав и интересов информационных отношений от воздействия различных видов угроз.

Граждане, общественные и иные организации и объединения являются субъектами безопасности, обладают правами и обязанностями по участию в обеспечении безопасности в соответствии с законодательством РФ, законодательством республик в составе Российской Федерации, нормативными актами органов государственной власти и управления краев, областей, автономной области и автономных округов, принятыми в пределах их компетенции в данной сфере. Государство обеспечивает правовую и социальную защиту гражданам, общественным и иным организациям и объединениям, оказывающим содействие в обеспечении безопасности в соответствии с законом.

Угроза безопасности – прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства [56].

Реальная и потенциальная угроза объектам безопасности, исходящая от внутренних и внешних источников опасности, определяет содержание деятельности по обеспечению внутренней и внешней безопасности [54].

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

К числу основных задач в области обеспечения национальной безопасности России относятся:

– своевременное прогнозирование и выявление внешних и внутренних угроз национальной безопасности России;

- реализация оперативных и долгосрочных мер по предупреждению и нейтрализации внутренних и внешних угроз;
- обеспечение суверенитета и территориальной целостности Российской Федерации, безопасности ее пограничного пространства;
- подъем экономики страны, проведение независимого и социально ориентированного экономического курса;
- преодоление научно-технической и технологической зависимости государства от внешних источников;
- обеспечение на территории РФ личной безопасности человека и гражданина, его конституционных прав и свобод;
- подъем и поддержание на достаточно высоком уровне военного потенциала государства;
- укрепление режима нераспространения оружия массового уничтожения и средств его доставки;
- принятие эффективных мер по выявлению, предупреждению и пресечению разведывательной и подрывной деятельности иностранных государств, направленной против Российской Федерации;
- коренное улучшение экологической ситуации в стране.

Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства [57].

Основу системы обеспечения национальной безопасности Российской Федерации составляют силы и средства обеспечения национальной безопасности. Силы обеспечения национальной безопасности – Вооруженные Силы РФ, другие войска, воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или)

правоохранительная служба, а также федеральные органы государственной власти, принимающие участие в обеспечении национальной безопасности государства на основании законодательства РФ. Средства обеспечения национальной безопасности – технологии, а также технические, программные, лингвистические, правовые, организационные средства, включая телекоммуникационные каналы, используемые в системе обеспечения национальной безопасности для сбора, формирования, обработки, передачи или приема информации о состоянии национальной безопасности и мерах по ее укреплению.

В формировании и реализации политики обеспечения национальной безопасности принимает участие ряд федеральных государственных органов. Президент РФ руководит в пределах своих конституционных полномочий органами и силами обеспечения национальной безопасности Российской Федерации; санкционирует действия по обеспечению национальной безопасности; в соответствии с законодательством РФ формирует, реорганизует и упраздняет подчиненные ему органы и силы обеспечения национальной безопасности; выступает с посланиями, обращениями и директивами по проблемам национальной безопасности.

Таким образом, мы можем сделать вывод о том, что государственная и общественная безопасность – ключевые составляющие национальной безопасности. Соответственно, понятийная цепочка «национальная безопасность – государственная безопасность – общественная безопасность» может быть раскрыта, на наш взгляд, следующим образом: безопасность – общее понятие, национальная безопасность – родовое понятие, государственная и общественная – видовое. Как отмечал в своей статье С.В. Хмелевский: «…государственная безопасность выступает средством, а должный уровень общественной безопасности – целью национальной безопасности…».

В целом, мы можем сделать вывод о том, что обеспечение государственной и общественной безопасности – это комплекс мер,

применяемых государством и правоохранительными органами в его лице, который направлен на обеспечение национальной безопасности российского государства. Государственная безопасность является неотделимым звеном в системе национальной безопасности, несмотря на то, что данные понятия не являются тождественными и взаимозаменяемыми. Более того, ни одно из них в условиях современности не может быть полностью приравнено к понятию «национальная безопасность».

# Глава 2 Информационная безопасность как важнейшее направление государственной безопасности

## 2.1 Понятие информационной безопасности, ее правовые основы

В последние годы информационная сфера приобретает все большее значение. Развитие информационных технологий является важной для современной России, т.к. многие преобразования в социально-экономической сфере реализуются через информационное пространство сети Интернет.

Основным нормативным документом, регламентирующим развитие информационных правоотношений в России, выступает Доктрина информационной безопасности Российской Федерации, утвержденная указом Президента Российской Федерации 5 декабря 2016 года [44]

Принятие Доктрины связано с необходимостью поднятия темы важности информационных правоотношений на современном этапе развития российской государственности. М.Ф. Алиева считает, что информационная безопасность выступает в качестве ядра в общей системе безопасности России.

Значение Доктрины 2016 года трудно переоценить. Ее главное значение – это выработка целей информационной защиты. Доктрина выражает позицию законодателей по вопросам обеспечения информационной безопасности не только государства, но и личности и общества в целом.

В Доктрине развитие информационной безопасности выражается в следующем:

– совершенствование не только информационной безопасности, но и информационных технологий;

– внедрение информационной продукции на внутреннем и внешнем рынках;

– обеспечение защиты информационных ресурсов российского государства;

– при использовании информации соблюдение конституционных прав, а также свобод граждан;

– духовное обновление России;

– укрепление потенциала населения России в духовной, нравственной и других сферах;

– эффективная защита населения и государства от киберугроз современности;

– поддержание информационного обеспечения российского государства [59].

В Доктрине информационной безопасности раскрываются следующие информационные угрозы.

Во-первых, наращивание некоторыми западными государствами возможностей для информационного влияния на Россию. Помимо этого, использование информационного потенциала в военной сфере.

Во-вторых, усиление деятельности иностранных организаций, которые осуществляют промышленную и военную разведку на территории Российской Федерации.

Среди внутренних угроз Доктрина выделяет:

Во-первых, слабость российской промышленности, а также экономики;

Во-вторых, низкий уровень информатизации российской власти по сравнению с западными странами;

В-третьих, низкий уровень информатизации во всех сферах жизнедеятельности (в кредитно-финансовой сфере, банковской и др.).

Исследователи считают, что основная угроза виделась в отсутствии общества, воспитанного в духе правового государства.

Само российское общество не готово к преобразованиям. Мы согласны с данной точкой зрения.

На современном этапе развития российского государства в нашей стране отсутствует представления о необходимости обеспечения информационной безопасности. Основной проблемой является отсутствие четкой правовой базы в сфере обеспечения информационной безопасности. Это проявляется в отсутствии четкого механизма ограничения свободы СМИ. Несмотря на то, что свобода слова закреплена на конституционном уровне, до сих пор отсутствуют четкие механизмы реализации данной свободы.

В России активно развивает интернет пространство. Все большую роль приобретают интернет СМИ. Однако, в российском обществе все чаще высказываются негативные отзывы об интернет СМИ, т.к. они нередко манипулируют сознание людей при помощи применения запрещенных журналистских средств (к примеру, «кричащий» заголовок статьи и т.п.). В целом стоит отметить, что сами СМИ стали виновниками своего же поведения. Несмотря на гарантирование свободы СМИ в России данное конституционное положение реализуется не в полном объеме [9].

Отметим, что неприкосновенность частной жизни также реализуется в России с большими проблемами.

Однако, права недостаточно просто провозгласить, и в данном случае на государство возложена обязанность по реализации этих прав. Однако в современной действительности мы можем отметить отсутствие обеспечения государством должным образом прав человека. Зачастую происходят нарушения прав человека, что связано, на наш взгляд, с существующей пробельностью современного законодательства и достаточно ослабленностью гарантий прав граждан. Для большинства населения остаются актуальными вопросы малодоступности высшего образования, медицинского обслуживания, отсутствия жилья и других необходимых благ.

Недостаточность правового регулирования процесса соблюдения прав и свобод человека подрывает доверие граждан к законодательной и исполнительной власти [48].

Доктрина раскрывает и состояние обеспечения информационной безопасности в рамках российской экономики и других отраслях (к примеру, в промышленности, образовании и т.п.).

Мы согласны с позицией Е. Васильева, который указывает на следующий аспект – государство впервые поднимает проблему обеспечения информационной безопасности, а также отсутствия информационных технологий. Законодатель признал их в качестве угрозы национальной безопасности России.

Е.В. Алексеева отмечает, что в Доктрине законодатели достаточно негативно отозвались по поводу научных разработок отечественных ученых в сфере информационной безопасности. Более того, в Доктрине отмечается достаточно малый уровень внедрения российских разработок в сфере обеспечения информационной безопасности [1].

Мы считаем, что российская наука должна больше уделять внимание разработкам в сфере информационной безопасности, т.к. это необходимо для обеспечения национальной безопасности России.

Информационная сфера все чаще применяется в качестве средства борьбы с Россией [61]. Нередко западные спецслужбы прибегают к использованию телекоммуникационных систем для создания негативного информационного фона вокруг России. Западные страны при помощи открытых источников информации фактически распространяют открытую русофобную информацию.

С. Стоякин отмечает, что в России недостаточно финансируется сфере обеспечения информационной безопасности. Более того, на низком уровне находятся разработки в сфере космической разведки, а также в развитии средств радиоэлектронной связи.

По поводу Доктрины 2016 года в научной среде сложились разные точки зрения:

Во-первых, одни авторы считают ее не отвечающей потребностям нового времени;

Во-вторых, другие авторы отмечают ярко выраженный милитаристский характера новой Доктрины.

Несмотря на негативные оценки ученые отметили, что Доктрина 2016 года смогла сосредоточить внимание населения на угрозах в информационной сфере, что является серьезны достижением. В этом проявляется основная положительная сторона Доктрины 2016 года по сравнению с ранее действовавшей Доктриной 2000 года. В Доктрине 2000 года информационная безопасность в основном была направлена на защиту интересов государства, а не личности и общества.

Основная особенность новой Доктрины состоит в том, что она учитывает современные вызовы, стоящие перед нашим государством и обществом (к примеру, террористические угрозы, кибератаки и т.п.). Доктрина имеет большую ориентированность на интересы человека.

Мы считаем, что основным недостатком Доктрины 2016 года выступает чересчур его милитаристский характер. Законодатель в качестве основной угрозы безопасности государства поставили западные страны. С другой стороны, терроризм признан в качестве второсортной угрозы. Мы считаем, что подобная градация является ошибочной. Терроризм несет большую угрозу по сравнению в негативно настроенными против России государствами [14].

С. Стоякин связывает милитаристский характер Доктрины с желанием руководства России отстраниться от других государств. Указание на внешние угрозы необходимо для того, чтобы отвлечь население от внутренних проблем и противоречий. Более того, если слушать российские СМИ, то можно увидеть, что Россия позиционирует себя в качестве единственной страны, которая всецело придерживается в своей деятельности международного права. Мы согласны с позицией автора.

Несмотря на то, что Доктрина была принята в 2016 году, до сих пор нерешенными остаются вопросы обеспечения информационной безопасности в нашей стране. Так, в большинстве своем программное обеспечение на

компьютерах является иностранным, что может создать в дальнейшем угрозу обеспечения национальной безопасности. Более того, разработки российских ученых в информационной сфере является малозначительными. Российские власти не поддерживают отечественные разработки в сфере обеспечения информационной безопасности российского государства. Государство финансирует лишь крупнейшие центры (наиболее известным является Сколково), в которых сконцентрирована лишь небольшая часть разработок в информационной сфере. Несмотря на это отдача от разработок в Сколково является низкой.

К.О. Полыхань отмечает неэффективность российского законодательства в информационной сфере. Более того, автор считает, что российский сегмент информационной безопасности является неэффективным.

Свою позицию автор обосновывает тем, что проблемы в правовом регулировании информационной безопасности являются достаточно серьезными.

Их решение необходимо путем совершенствования законодательства. Более того, по мнению ученого информационная политика российского государства должна быть направлена на расширение прав человека в информационной сфере, а не на ее ограничение как было сделано при помощи принятия пакета нормативных актов, названных в прессе «Законом Яровой» (по имени политика, которая настояла на принятии поправок в законодательство). «Закон Яровой» отдаляет граждан РФ от государства. Граждане страны стали меньше доверять государству [49].

Проблемами России в сфере информационной безопасности являются: ограничения со стороны государственных органов, несовершенство нормативно-правовой базы, зависимость и подчиненность СМИ государственным органам, низкая степень ответственности за предоставление ложной информации, незащищенность личных данных, высокий уровень киберпреступности, недостаточная эффективность

политики в области защиты данных, низкая степень защиты информации, составляющей государственную тайну, утечка квалифицированных кадров, зарубежные технологии по защите информации, недостаточное финансирование информационной безопасности, низкая эффективность борьбы с угрозами информационной безопасности.

Позитивным моментом является то, что посредством доктрины формируется подход и видение исполнительной власти в РФ в отношении существующих проблем, обозначены принципы, которыми руководствуются уполномоченные органы в своей деятельности, однако они также имеют противоречивый характер.

В большинстве случаев правоприменительные органы квалифицируют корыстные посягательства на криптовалюту как хищение, а саму цифровую валюту признают имуществом в уголовно-правовом смысле, хотя она лишена физического признака.

Подобная практика заслуживает поддержки, поскольку отношения, связанные с оборотом криптовалюты, не должны оставаться без уголовно-правовой охраны.

Таким образом, в юриспруденции последних десятилетий появились новые, находящиеся в процессе разработки концепции информационного права и права информационной технологии.

Проведенные исследования позволяют вычленить самостоятельную предметную область – область создания и применения информационных технологий в различных сферах человеческой деятельности.

Для этой области, как и для многих других, характерны не только исключительно положительные элементы, но и негативные проявления, к числу которых относятся правонарушения в информационной сфере. Наиболее общественно опасным являются преступления в сфере компьютерной информации.

Обеспечение информационной безопасности является приоритетным в Российской Федерации. Важным является правовое обеспечение информационной безопасности.

## 2.2 Правовая политика в сфере обеспечения информационной безопасности Российской Федерации

Современная ситуация в Российской Федерации относительно уровня информационной безопасности в стране характеризуется тем, что данный элемент в структуре политики обеспечения национальной безопасности является новым и относительно несформированным. Отсюда наблюдается большое число проблем и угроз, которые требуют комплексного и длительного решения со стороны государственных органов.

В соответствии с Доктриной информационной безопасности, рассмотренной ранее, а также, анализом других нормативно-правовых актов в сфере защиты информации в России, можно отметить следующие основные недостатки в системе информационной безопасности России.

1. Нынешнее состояние большинства основных аспектов уровня развития страны, такие как социально-экономическое положение, политическая структура, внешнеэкономическая деятельность и другие, находятся в противопоставлении желания населения потреблять ту или иную информацию и действующих ограничений со стороны государства, которые дают запрет на использование и распространение тех или иных источников информации и данных, что в большей степени касается информации, приходящей из внешнего окружения России.

2. Следующей проблемой обеспечения информационной безопасности в России является несовершенство нормативно-правовой базы в данной сфере. Данный факт ведет к тому, что в РФ пока еще нет сформированных информационных агентств, источников информации и СМИ общемирового уровня. В некоторых нормативных актах двояко или

искаженно трактуются законы и нормы, которые необходимо соблюдать в сфере защиты информации и ее распространения, однако, нет четкого представления о правах и обязанностях субъектов отношений в области информации, а также, наказании за предоставление ложной информации или меры не являются достаточно жесткими для регулирования подобных случаев. Данные аспекты подтверждают то, что в России в сфере защиты и использования информации нет взаимосвязи между государством, обществом, СМИ и другими структурами.

3. Следующей актуальной проблемой является участие государственных органов в формировании общественного мнения на то или иное событие. Во многих государствах СМИ являются независимыми структурами и в праве самостоятельно преподносить информацию в том виде, в котором они считают возможным и правильным. В России же есть практика того, что большинство СМИ имеют ограничения на публикации со стороны федеральных, региональных и местных органов власти. Данный аспект говорит об искажении информации в интересах власти и нарушении прав граждан [62].

4. Помимо искажения информации в СМИ, существует еще и проблема в выражении людьми своего мнения и преподнесении той или иной информации для общественного пользования. Здесь стоит отметить, что тенденции современного цифрового общества позволяют каждому человеку посредством социальных сетей высказывать свое мнение, которое потом увидит определенное количество человек. Если один из людей публикует новости о каких-то значимых событиях, например, числе погибших в каком-либо происшествии или решении по судебному делу, то он/она должны нести ответственность за свои слова. В большинстве случаев ложная информация наказывается незначительно. Что ведет к потере информацией своих признаков, ведь такая информация не подтверждена фактами и не является достоверной.

5. Следующим проблемным аспектом является незащищенность личной информации каждого гражданина РФ. В законодательстве РФ, в том числе в Конституции, прописаны права и обязанности человека, которые также подразумевают такие аспекты, как семейная тайна, неприкосновенность личной жизни, тайна переписки и другие аспекты, которые в полной мере не соблюдаются, поскольку не имеют должного правового, организационного и технического регулирования.

6. Проблемой, вытекающей из предыдущей, является незащищенность правоохранительными органами, а иногда и использование для собственных нужд, личной информации и персональных данных граждан РФ. Нет должного уровня защиты данных. В РФ один из самых высоких показателей в мире по уровню киберпреступности [63]. Кроме того, для раскрытия преступлений или вычисления тех или иных фактов о человеке, нередко прибегают к взлому аккаунтов социальных сетей и несанкционированному проникновению в частную жизнь человека с превышением предоставленных полномочий.

7. Существует проблема в сфере государственного управления информационным пространством РФ. Кроме того, проявляются негативные аспекты в вовлечении России в глобальное информационное пространство и мировую цифровую экономику. По причинам отставания российских технологий и уровня развития информационного пространства наблюдаются искажения в предоставлении международной информации и эффективность работы СМИ, информационных агентств и других субъектов данной сферы на территории России.

8. Следующая проблема связана с незначительностью помощи со стороны государственных органов в развитии данной сферы в России и устранении угроз информационной безопасности. Здесь подразумевается и неэффективность контроля со стороны федеральных органов власти за региональными в данной сфере и в целом слабой осведомленностью государственных органов, как в регионе, так и в масштабах всей страны об

уровне информационной безопасности, в том числе и хозяйствующих субъектов, являющихся стратегически важными.

9. Низкая эффективность деятельности правоохранительных и других государственных органов по сохранности и целостности данных, составляющих государственную тайну. В последние годы особо обострились проблемы с ложной информацией от государственных деятелей, чиновников и представителей СМИ о тех или иных вопросах, которые вовсе не должны быть представлены на общее обозрение или в данном виде нарушают права на защиту информации и ее неразглашение.

10. Как и во многих других сферах деятельности, исходя из низкого в сравнении с зарубежными странами уровня оплаты труда, существует проблема утечки высококвалифицированных кадров в сфере информационной безопасности. Данный факт приводит к снижению потенциала и эффективности деятельности коллективов по организации защиты информации, ее использованию и предоставлению.

11. В связи с последними событиями в экономико-политической обстановке в России, проблемы которые еще больше обострились с введенными санкциями, низкой эффективностью импортозамещения, кризисом, падением курса рубля и другими, ведут к тому, что отставание технологий и сферы информационной безопасности России, требует от государственных органов привлечение зарубежных фирм для применения методов защиты информации на территории РФ. Зарубежные партнеры тем самым имеют доступ к информации российских компаний, государственных организаций и политическим решениям, и при необходимости могут использовать полученные данные против России. То есть данный факт ведет не только к снижению информационной безопасности, но и к снижению уровня национальной безопасности в целом.

12. Информационные технологии и цифровая экономика являются трендами современного общества, однако, в России не уделяется должного внимания именно защите информации. Уделяется большое внимание

развитию цифровой экономики, совершенствованию методов работы оборудования, применению новых технологий, информатизации всех слоев населения, развитию бизнеса в Интернете и другим аспектам.

Но нет должного нормативно-правового обеспечения регулирования информационной безопасности, не выделяется достаточного финансирования на нивелирование угроз в данной сфере, что ведет к ухудшению уровня защиты информации и применению информационного оружия против политических и экономических интересов России.

Помимо проблем в области защиты информации, существует ряд угроз, которые негативно сказываются на информационной безопасности России:

- связанные с нарушением прав и свобод граждан в области получения, предоставления, защиты информации в соответствии с Конституцией Российской Федерации, Федеральными законами, постановлениями правительства, президента РФ, нормативно-правовыми актами субъектов РФ, органов местного самоуправления и других.

Данные нарушения могут проявляться в осуществлении монопольного права на предоставление информации, отсутствии возможности получения информации у людей с ограниченными возможностями и других важных для граждан аспектов информационной сферы;

- связанные с отсутствием альтернативного источника информации для обеспечения государственной политики РФ в области защиты информации, что ведет к блокированию деятельности отдельных средств СМИ, монополизации информационного рынка РФ, недоверию со стороны граждан к предоставленной информации;

- связанные с развитием информационных технологий и средств предоставления информации на территории РФ, в том числе инструментов и методов в области информатизации общества, телекоммуникационных технологий, средств связи, совершенствования предоставления данных зарубежным партнерам России и компания на внутреннем рынке для эффективного взаимодействия участников внешнеэкономической

деятельности, блокированием доступа российского бизнеса и государственных структур к информационным потокам, а также технологиям получения, накопления и защиты информации на внешних рынках;

- связанные с обновлением и работоспособностью средств по обеспечению информационной безопасности, создаваемых как на территории России, так и за рубежом. Что касается импортных технологий информационных систем, то в России наблюдаются угрозы во многих сферах с предоставлением доступа на реализацию некачественных товаров и услуг, что относится и к сфере информационных технологий и защиты информации.

- связанные с утечкой, хищением, искажением, уничтожением, повреждением, неправильной обработкой, несанкционированным проникновением и другими процессами нарушающими целостность, достоверность, конфиденциальность информации и систем ее защиты.

Нарастающий процесс цифровизации, в недрах которого скрываются представляющие определенную опасность вызовы, предопределяет потребность правового ответа, сопряженного с модификацией уголовно-правового механизма воздействия. В этом механизме свою нишу занимают преступления, совершаемые с использованием цифровых технологий, адаптация которых к современным реалиям становится объективно необходимой. Расширение цифрового пространства вне правового поля увеличивает риски, порождает новые реальные угрозы различным благам и общественным отношениям, нуждающимся в уголовно-правовой защите [16].

Существенным фактором, затрудняющим определение системы преступлений, совершаемых с использованием цифровых технологий, является отсутствие единого термина, объединяющего данные преступления. Понятие «цифровая преступность» в настоящее время на законодательном уровне отсутствует [64]. По сути, м должны говорить о преступлениях, которые совершаются в сфере цифровых технологий или с их использованием.

Рассмотрим типологизацию данных преступлений – обозначим их виды и признаки. Саму типологию приведем в зависимости от расположения объекта посягательства в УК РФ.

К первой подгруппе преступлений, совершаемых с использованием цифровых технологий, следует отнести некоторые преступления против жизни и здоровья. Цифровая трансформация уголовно-правовой охраны личности в Российской Федерации осуществляется в рамках современной государственной политики по созданию необходимых условий для развития цифровой экономики Российской Федерации. Действительно, выполнение вышеуказанной задачи носит масштабный и долговременный характер, ее решение требует значительной государственной поддержки.

В Конституции Российской Федерации институт цифровизации не закреплен, речь идет только об информации. Однако общественные отношения развиваются, и в современном мире, где все чаще применяются цифровые алгоритмы, данные технологии стали нуждаться в правовом оформлении. Прежде всего, основные положения и понятия, связанные с внедрением информационно-коммуникационных цифровых технологий, получили свое закрепление в Федеральном законе от 27.07.2006 № 149-ФЗ (ред. от 02.07.2021) "Об информации, информационных технологиях и о защите информации" [43].

В соответствии с Указом Президента РФ от 09.05.2017 № 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [41], необходимо развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

Указом Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» сформирована национальная программа «Цифровая экономика Российской Федерации» [36]. Указом также

закреплена необходимость урегулирования сквозных для различных отраслей законодательства, в том числе для уголовного права, вопросов, связанных с идентификацией субъектов правоотношений в цифровой среде, электронным документооборотом, оборотом данных, в том числе персональных.

В 2019 году Указом Президента РФ от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации", была принята Национальная стратегия развития искусственного интеллекта на период до 2030 года" [38]. В науке уголовного права разработан ряд определений искусственного интеллекта, а также его свойств [29]. Однако общепринятого понимания искусственного интеллекта в настоящее время еще не разработано.

Б.Т. Разгильдиев приводит следующее определение искусственного интеллекта - это создаваемый (созданный) человеком на основе цифровизации физический продукт, обладающий ограниченной самостоятельностью во времени, пространстве, по характеру и видам системной деятельности, осуществляемой на нравственной основе в целях социального удовлетворения (полезности) для личности, общества, государственной власти, мира и безопасности человечества [53].

А.Г. Блинов справедливо указывает на два момента, которые хотелось бы привести [10]:

– формированию и развитию собственно искусственного интеллекта предшествует и способствует широкая цифровизация общественных отношений. Примерами служат расширение возможностей распознавания преступников по радужной оболочке глаза, внедрение электронного правосудия, аудио-протоколирования заседаний, ВКС-связи, и другие направления все более широкого применения инновационных технологий на службе процессуальной правоохранительной деятельности;

– следует помнить о необходимости защиты ученых, реализующих современные технологии, идущие на определенный риск для достижения общественно полезной цели.

Действительно вопрос о том, кто будет нести ответственность за вред, причиненный при использовании искусственного интеллекта, является важным (это будет изобретатель, инженер-программист, производитель, сама система искусственного интеллекта)? В этом аспекте мы согласны в тем, что крайне осторожно нужно сформировать правовые нормы, позволяющие ученым идти на общественно полезный риск при разработке программ, условий реализации искусственного интеллекта [18].

Следующую подгруппу преступлений, совершаемых с использованием цифровых технологий, составляют преступления против свободы, чести и достоинства личности.

Безграничные возможности в доставке информации и распространении информации, анонимность и широкая аудитория сделало Интернет по сути универсальным средством массовой информации [17]. Очень часто тем или иным способом появляется информация, в социальных сетях, форумах, блогах, потенциально опасная, содержащая оскорбительные и клеветнические сведения.

Преступления против конституционных прав и свобод человека и гражданина также могут быть оценены как преступления, совершаемые с использованием цифровых технологий [22].

Данные хранящиеся на компьютерах, переписка по электронной почте также становится предметом преступного посягательства. Преступления, предусмотренные ст. 137 и 138 УК РФ, получили новый, более быстрый и выгодный, способ совершения.

Совершаться с использованием цифровых технологий могут преступления против семьи и несовершеннолетних.

Дети наравне со взрослыми имеют доступ к Интернету, при помощи которого ребенок или подросток может быть вовлечен в совершение

преступных деяний. Ответственность за вовлечение несовершеннолетних в совершение преступления предусматривается ст. 150 УК РФ. Действия, составляющие диспозицию данной нормы, могут осуществляться преступником не только при непосредственном, но и при удаленном контакте. Действуя через Интернет, преступник сохраняет свою анонимность, снижает риск раскрытия своей личности, а также значительно облегчает себе задачу, прежде всего в поиске несовершеннолетнего.

Наиболее распространенным преступлением во всемирной сети несомненно является интернет-мошенничество.

Применительно к данным составам, важно рассматривать их в аспекте виктимизации жертв таких хищений посредством обмана или злоупотребления доверием, которое совершается с использованием информационных цифровых технологий [23].

Преступления против общественной безопасности. В настоящее время сформирована одна из наиболее опасных разновидностей киберпреступности - кибертерроризм.

В Интернете терроризм развивается стремительно, поскольку сеть - это идеальная среда для его развития и распространения. Отсутствие цензуры приводит к распространению информации, изображений, угроз или сообщений независимо от их законности или потенциального воздействия на человеческое сознание. Данные преступные деяния предусмотрены ст. 205, 205.1, 205.2 УК.

Преступления против здоровья населения и общественной нравственности.

Преступность, связанная с незаконным оборотом наркотических и психотропных веществ посредством сети Интернет – это относительно новое явление, появившееся в конце прошлого века с развитием как технологий, так и самой сети Интернет [33]. Общественная опасность наркопреступности в сети Интернет выражается в первую очередь в том, что в нынешнее время компьютеризация набирает всё большие и большие обороты, компьютерная

техника стала предметом необходимости в работе и быту, и сеть Интернет стала общедоступной для каждого. Всемирная сеть Интернет ориентирована на распространение информации о способах изготовления наркотических средств, о возможных путях их приобретения. Данная сеть, в которую включено неопределенное количество лиц, направлена на создание потребительской аудитории. Особенно следует оберегать от информации такого рода несовершеннолетних детей.

При анализе общественной опасности преступлений рассматриваемой категории, при совершении их с использованием сети Интернет, важно учесть то обстоятельство, что ресурсы, задействованные в данной сфере правоотношений, становятся почти неизмеримыми [24]. Необходимо вести речь о неопределенном круге задействованных в информационном воздействии лиц. Под угрозой оказываются общественные отношения, связанные с поддержанием правопорядка в обществе. Негативным фактором становится воздействие на неокрепшую психику детей, которые достаточно свободно находят информацию в сети Интернет, а фильтров современные технологии пока не разработали. Расширяется аудитория тех лиц, которые могут быть вовлечены в отношения по сбыту и приобретению, а также употреблению наркотических средств и их аналогов. Формируется уже устойчивая криминальная субкультура. Данные социально-негативные явления, связанные с преступностью по незаконному обороту наркотических средств, с использованием информационно-коммуникационных сетей, в том числе сети Интернет, нуждаются в специальных исследованиях, носящих междисциплинарный характер. Требуются познания не только основ уголовной ответственности, но и смежных с уголовным правом отраслей знаний – необходим комплекс знаний юридической психологии, криминологии, судебной медицины, а также наук, связанных с работой информационно-коммуникационных сетей [20].

Однако стоит отметить, что наркопреступность имеет высокую латентность, так как установить конкретное лицо-организатора практически

не предоставляется возможным. А так называемые «закладчики» не знают кто ими руководит, так как выполняют лишь указания, данные им по этим самым мессенджерам без личного контакта с человеком.

Следует также учитывать, что использованием информационно-коммуникационных сетей, в том числе сети Интернет, не ограничивается способ преступлений, связанных с незаконным оборотом наркотических средств и их аналогов. При этом, преступниками применяются еще доступные для криминальной деятельности по сбыту наркотиков мессенджеры и приложения (среди наиболее распространенных – QIWI, ICQ, WhatsApp, Skype, Telegram). Среди наиболее распространенных преступлений, которые совершаются посредством использования Интернет-ресурсов, а именно, ст. 228 и 228.1 УК РФ, наиболее широко в незаконном обороте участвуют каннабиноиды, героин и амфетамины. Применительно к установлению фильтров в информационном потоке сети Интернет, следует признать, что в настоящее время проблема прикладного решения еще не получила. Применение цензуры в потоке информации во всемирной паутине практически невозможно. Доступным языком написана информация о способах и методах приготовления того или иного вида наркотика в домашних условиях, также предлагаются к покупке предметы наркотического обихода (бонги, медвахи), помимо вышесказанного на тематических форумах проводятся опросы пользователей и сборы их подписей в поддержку легализации «лёгких» наркотиков (марихуаны в частности) в России.

Между тем, свободный доступ к мировой паутине в настоящее время возможен дома, в школах, других учебных заведениях, библиотеках, ресторанах и кафе. Отсюда можно сделать вывод, что Интернет стал привычной частью быта большинства современной молодёжи [45]. При этом, многочисленные экспертные сообщения, по сути - пропаганда наркотических средств в сети Интернет, многочисленные комментарии пользователей в глобальной сети о том, что единоразовое употребление никак не скажется на

жизни, что в этой жизни необходимо испробовать всё и т.д. только увеличивают спрос на запрещенные наркотические средства. Доскональные описания методов приготовления, использования, покупки наркотиков вкупе с анонимностью и общедоступностью информации лишь увеличивают количество наркопотребителей, что, соответственно, в свою очередь представляет опасность для здоровья как отдельно взятого лица, так и в целого населения России.

С внедрением возможностей сети Интернет в повседневную жизнь, а в частности социальных сетей, тематических форумов, мессенджеров, пользователи стали объединяться в группы, в которых ведут дискуссии на интересующие темы и обмениваются различной информацией, табуированной в обществе, что разрешает им создавать мнение о наркотиках как о легкодоступных средствах в рамках виртуального пространства Интернета, ежедневно увеличивать число наркопотребителей, и вместе совершать преступную деятельность в сфере незаконного оборота наркотиков. Уровень негативного воздействия разграничивается разновидностью таких преступных групп, в первую очередь это зависит от степени их устойчивости.

Особо опасными являются организованные формы незаконного оборота, в том числе сбыта, наркотических веществ и их аналогов, посредством сети Интернет. Приведем пример. Так, согласно приговора Новомосковского городского суда от 25 сентября 2019 г. по делу № 1-268/2019, осужденный Н. в скрытой сети Интернет, доступной при использовании специального программного обеспечения, создало интернет – магазин, присвоило себе никнейм. Данное лицо, под выбранным никнеймом, желая избежать разоблачения со стороны правоохранительных органов, особое внимание уделил мерам конспирации, заключавшимся в следующем: в использовании при подготовке и совершении наркопреступлений, средств мобильной связи, зарегистрированных на посторонних лиц, не осведомленных о преступных намерениях; в использовании

коммуникационного программного обеспечения, позволяющего осуществлять получение и обмен информацией, посредством информационно-телекоммуникационной сети Интернет, на условиях анонимности, не сообщая о себе подлинных анкетных и установочных данных в мессенджерах, в использовании легального платежного интернет - сервиса, позволяющего осуществлять перечисление и получение денежных средств на условиях анонимности через «КИВИ-кошельки» - условные счета, оформленные на подставных лиц, которые использовались при осуществлении денежных взаиморасчетов в процессе незаконного оборота наркотических средств на созданном интернет-магазине. Н., действующим под никнеймом при создании указанного интернет-магазина была определена следующая структура: лицо, осуществлявшее руководство и координацию деятельности интернет -магазина; вербовку и подбор участников ОПС; загрузку на сайт автоматических продаж интернет -магазина фотографий с местами расположения «тайников-закладок» с наркотиками и их географическими координатами; организацию выплат вознаграждения участникам преступного сообщества за осуществление преступной деятельности; установление мест сбыта наркотических средств; второе лицо, в обязанности которого входило получение крупных оптовых партий наркотических средств и психотропных веществ, их хранение, фасовка и передача по указанию руководителя ОПС и интернет-магазина мелкооптовым сбытчикам («курьерам-закладчикам»); лицо, в обязанности которого входила фасовка на мелкие дозы наркотических средств для сбыта «курьерами-закладчиками» бесконтактным способом, то есть через «тайники-закладки»; лицо, в обязанности которого входило получение через «тайники-закладки», то есть бесконтактным способом, по указанию руководителя ОПС наркотических средств для сбыта приобретателям (потребителям); передача, посредством сети Интернет, фотографий с местонахождением сделанных ими «тайников-закладок» с наркотиками с инструкциями и географическими координатами по их обнаружению

(редактирование), для их дальнейшей загрузки на сайт автоматических продаж интернет-магазина.

8. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации (по ст. 272 УК РФ). Преступления в сфере компьютерной информации - преступления так или иначе связанные с незаконным получением, распространением и собиранием конфиденциальной информации, это преступления 28 главы Уголовного кодекса («Преступления в сфере компьютерной информации») [21].

Преступления, связанные с неправомерным оборотом компьютерной информации, получают все большее распространение в мире, и наша страна не является здесь исключением. Полагаем, что достаточно большое число таких деяний обусловлено развитием научно-технического прогресса, внедрения компьютерных технологий во все сферы жизнедеятельности, все большее число лиц использует электронные средства платежа, имеет к ним доступ с помощью различных приложений, работающих от сети Интернет. При этом, компьютерные технологии используются и на планшетах, смартфонах, множествах различных устройств, в классическом понимании к компьютерной технике не относящихся.

Следует с сожалением констатировать, что компьютерные технологии не только позволяют облегчить жизнь граждан, оптимизировать различные виды деятельности, но и активно используются преступниками в криминальных целях [46].

Преступления в сфере компьютерной информации объединены законодателем в главу 28 УК РФ. Большинство исследователей, рассматривая само появление этих норм как безусловно положительный факт, тем не менее отмечают, что научных наработок в этой сфере ранее практически не было [25], как не было и правовой традиции регламентации подобных общественных отношений в отечественном уголовном праве по объективным причинам: из-за отсутствия самого предмета преступления, появившегося только вследствие вступления нашей страны, наряду с

другими государствами, в информационную эпоху, для которой характерно использование компьютерных технологий во всех сферах жизнедеятельности. Это, по мнению С.Д. Бражника, пагубно сказалось на качестве норм данной главы, которые отличаются "неточностью, неконкретностью, неясностью, несовершенством, неопределенностью" [11]. Криминализация незаконных действий в сфере использования компьютерной техники в целом, а также создания, распространения вредного программного и технического обеспечения в частности, есть, в первую очередь, отображением определенного уровня общественной опасности данных посягательств.

Анализируя общую характеристику этих преступлений можно сделать вывод о необходимости внесения дополнений и изменений в действующее законодательство РФ в этой области. Например, расширить понятийную базу в сфере компьютерной преступности, что позволит правильно и более точно квалифицировать такие деяния.

Нельзя не обратить внимания на то, что устойчивая тенденция возрастания общественной опасности компьютерных преступлений обусловлена стремительным расширением сфер использования информационных технологий и, в частности компьютерной техники экономической, политической, военной областях и др. Соответственно, российской уголовное законодательство в данной сфере не в полной мере отвечает потребностям практики и требует дальнейшего совершенствования составов компьютерных преступлений [47].

9. Виды преступлений, совершение которых возможно с применением информационных технологий, которые требуют конструирования их диспозиции, обозначения конструктивных или квалифицирующих признаков, в которых указан данный способ совершения посягательства.

Предмет преступлений, совершаемых с использованием цифровых технологий, обладает спецификой.

Отметим, что дефиниция компьютерной информации впервые закреплена в федеральном законодательстве [35]. Как объект уголовно-правовой охраны компьютерная информация отвечает трем свойствам: конфиденциальность, целостность и доступность. Современным уголовным законодательством Российской Федерации были восприняты вышеназванные свойства информации. Основная отличительная особенность целостности, конфиденциальности и доступности информации от других ее свойств, состоит преимущественно в том, что они не принадлежат информации как таковой, а появляются в результате применения мер организационного характера.

Информация, обладающая свойствами целостности, конфиденциальности, доступности представляется более значимой по сравнению с иной информацией с точки зрения уголовного законодательства, поскольку общественно-опасные деяния, посягающие на три этих свойства, причиняют значительный ущерб владельцу такой информации. В связи с этим, можно сделать вывод о том, что позиция отечественного законодателя относительно обеспечения защиты информации является целесообразной и логичной.

Федеральным законом от 07.12.2011 № 420-ФЗ составы преступлений, предусмотренные главой 28 УК РФ, были изложены в новой редакции. В отличие от редакции ст. 272 УК РФ от 1996 года, новая формулировка данного термина поставила базовым критерием отнесения информации к компьютерной не средство ее хранения (машинный носитель) или обработки (ЭВМ), а более универсальный – форму ее представления – в виде электрических сигналов без привязки к какому-либо типу средств хранения, обработки и передачи этих сигналов. Такой взгляд на компьютерную информацию сформировался в силу произошедших существенных изменений в сфере информационных технологий.

Активное их внедрение во все сферы деятельности привело к появлению в массовом употреблении наряду с электронными вычислительными машинами иных цифровых электронных устройств,

например, таких как смартфоны, идентификационные карты с микроконтроллером (чипом).

Кроме того, в последние годы широкое распространение получает «умная» бытовая техника и связанный с ней «интернет вещей». Таким образом, персональный компьютер стал рассматриваться лишь одним из многих инструментов обработки цифровой информации, а существовавшее с 1996 года определение технически устаревшим, сужающим рамки применения нормы уголовного закона.

Определение формы информации «в виде электрического сигнала» связано с тем, что на современном этапе развития технологий в сфере передачи и обработки информации самыми массовыми в практическом применении являются именно цифровые технологии (информация представлена в виде дискретного цифрового сигнала), основанные на использовании различных устройств, исполненных на электронных компонентах, работа которых непосредственно связана с электрическими сигналами. К таким устройствам относятся ЭВМ, машинные носители и иные средства вычислительной техники, которые в свою очередь могут быть объединены в системы ЭВМ или включены в информационно-телекоммуникационные сети. Таким образом, в техническом аспекте компьютерная информация представляет собой информацию, представленную в форме, пригодной для циркуляции в указанной среде [60].

Обращаясь к законодательству зарубежных стран, можно отметить, что в зарубежных странах вместо термина «компьютерная информация» чаще используется термин «данные». В чем же заключается принципиальное различие в данных терминах с правовой точки зрения? Канадский ученый Д.К. Пирагофф в своем докладе отмечает, что под информацией следует понимать не вещь, а процесс, происходящий между человеческим сознанием и неким стимулом, а представление этой информации и есть данные, то есть информация является интерпретацией данных [15]. Следовательно, из одних и тех же данных может быть получена различная информация.

Изучая зарубежное законодательство в сфере компьютерных преступлений, можно прийти к выводу о недостаточности понятийного аппарата в российском уголовном законе. В УК РФ дается лишь одно определение, в то время как зарубежные кодексы полноценно раскрывают многочисленные понятия, связанные с компьютерными преступлениями. Например, в уголовном кодексе штата Техас дается определение многих понятий, связанных с компьютерными преступлениями, а именно: «Данные», «Компьютерная программа», «Иметь доступ», «Компьютер», «Вред», «Компьютерная сеть», «Компьютерные услуги», «Компьютерная система», «Компьютерное программное обеспечение», «Компьютерный вирус» [8]. В модельном Уголовном кодексе Союза Независимых Государств даются определения ряда понятий, которых нет в УК РФ, например, компьютерный саботаж, модификация компьютерной информации, неправомерное завладение компьютерной информацией. Законодательно закрепленные определения понятий имеют важное значение для квалификации преступлений, поэтому необходимо расширить понятийный аппарат в законодательстве РФ о компьютерных преступлениях.

Следует обратить внимание на то, что в настоящее время информации технологии активно развиваются, в силу чего, постоянно появляются новые способы обращения с компьютерной информацией, которые не входят в состав ст. 272 УК РФ. Так, к примеру, в настоящее время ей не охватываются такие действия как уничтожение или искажение компьютерной информации путем оказания внешнего воздействия на ее носители, например, магнитными волнами, механическими ударами, иными методами, когда фактически доступ к информации не осуществляется. Однако, в таких ситуациях общественная опасность деяний ничуть не меньше, чем общественная опасность неправомерного доступа к компьютерной информации [31]. Так, к примеру, для собственника информации не будет иметь значения, каким образом она уничтожена – путем форматирования электронного носителя информации или путем, например, его утопления или

сожжения, поскольку последствия для него одинаковы – информация утрачивается [28].

В качестве предмета преступлений, совершаемых с использованием цифровых технологий, вступает криптовалюта. Прежде всего, это предмет корыстных посягательств. Понятие цифровой валюты закреплено в федеральном законодательстве [42]. Вопрос о правовой природе цифровой валюты (криптовалюты) не получил однозначного решения. Одни расценивают криптовалюту как «иное имущество», другие относят ее к категории вещей или так называемых «бестелесных вещей» [32].

Случаи противоправного завладения криптовалютой получили широкое распространение, однако единообразная правоприменительная практика квалификации подобных посягательств пока не сложилась.

Известны случаи, когда суды отказывались признавать криптовалюту предметом преступлений против собственности, ссылаясь на то, что таковая не признается объектом гражданских прав, в результате чего общественно опасные посягательства на криптовалюту оставались без надлежащего уголовно-правового реагирования. Так, Петроградский районный суд г. Санкт-Петербурга исключил из приговора по делу о вымогательстве вмененный предварительным следствием факт вымогательства у потерпевшего криптовалюты. Как было установлено предварительным расследованием, потерпевший перечислил имевшуюся у него криптовалюту на криптокошельки вымогателей под воздействием угроз, сопряженных с требованием о переводе данного платежного средства. Суд, исключая криптовалюту из общего объема требуемого под угрозой имущества [52]. Оценивая это судебное решение, нельзя не отметить, что заложенная в нем правовая позиция, во-первых, полностью выводит имущественные отношения, связанные с оборотом цифровой валюты, из сферы уголовно-правовой охраны, а во-вторых, порождает безнаказанность лиц, незаконно получающих экономическую выгоду за счет умышленного причинения

прямого имущественного ущерба обладателю криптовалюты. Очевидно, что ни то, ни другое не согласуется с назначением уголовного права [26].

Впрочем, такие решения имеют единичный характер. В большинстве случаев суды решают вопрос о возможности признания криптовалюты предметом хищения положительно [5]. Причем обвинительные приговоры по делам о хищении криптовалюты выносились даже до внесения изменений в ст. 128 ГК РФ и принятия федерального закона от 31 июля 2020 г. № 259-ФЗ, определившего статус цифровой валюты. Несмотря на то, что в тот момент отсутствовало необходимое законодательное регулирование отношений, связанных с оборотом криптовалюты, органы предварительного следствия и суды, как правило, не оставляли корыстные посягательства на криптовалюту без уголовно-правовой оценки [4].

В практике оборота криптоактивов встречаются схемы мошеннического хищения цифровой валюты, в частности:

– путем создания интернет-сайтов или мобильных программ для осуществления операций по обмену криптовалюты (криптообменники), торговле цифровой валютой (криптобиржи). Потерпевший, не понимая, что использует созданный мошенниками сайт (программу), например, «клон» существующего криптообменника или легальной криптобиржи, совершает транзакцию по переводу криптовалюты на криптокошелек злоумышленников;

– посредством создания «финансовой пирамиды», в рамках которой обманутые граждане инвестируют криптовалюту в финансовый проект с доходностью в десятки процентов в месяц, некоторое время получают определенную прибыль за счет новых «инвесторов», а затем привлеченная под видом инвестиций криптовалюта похищается мошенниками;

– организации мошеннического ICO (Initial coin offering), т.е. первичного предложения (эмиссии) «монет» (новой криптовалюты или токенов). Мошенники запускают ICO, чтобы продать инвесторам выпущенную ими новую цифровую валюту, инвестиционные токены,

принимая в качестве оплаты безналичные денежные средства или криптовалюту. По этой схеме организаторы мошеннического ICO проекта Razormind похитили около $10 млн в BTC2. Более сложную схему реализовали мошенники при хищении криптовалюты у инвесторов блокчейн проекта Enigma. Они взяли под контроль домен сайта проекта Enigma, учетную запись одного из администраторов на Slack-канале компании и списки рассылок, после чего от имени администрации проекта Enigma разослали предложения об ICO и установили ложную ссылку на веб-сайт Enigma, указав там реквизиты криптокошелька, подконтрольного мошенникам. Прежде чем команда блокчейн проекта Enigma смогла восстановить контроль над доменом, на этот криптокошелек инвесторами была депонирована криптовалюта стоимостью около $5000003.

Цифровая валюта может быть похищена тайно, т.е. в форме кражи. Для кражи криптовалюты используются конфиденциальные учетные данные, предоставляющие доступ к криптокошельку обладателя цифровой валюты, которые получены в результате «взлома» криптобиржи, компьютерных устройств пользователей или посредством «фишинга» (ложные запросы данных от службы безопасности соответствующей криптоплатформы, «фишинговые» сайты, на которых пользователям предлагается ввести учетные данные криптокошелька и т.п.).

Получив эти данные, преступники осуществляют транзакции по переводу криптовалюты, совершая ее тайное хищение. Например, Г., введя в заблуждение потерпевшего З. под предлогом оказания консультации о порядке пользования «P2P» площадкой для осуществления сделки по продаже криптовалюты «Yusra», получил от З. видеозапись, в которой были зафиксированы обозначения логина и пароля от личного кабинета интернет приложения «Yusra Global» З.

Затем Г. совершил неправомерный доступ в личный кабинет интернет приложения «Yusra Global» З. и совершил транзакцию по переводу 700 монет криптовалюты «Yusra» стоимостью 140000 руб. [50].

Более того, известны случаи насильственного хищения криптовалюты. Подобный пример демонстрирует уголовное дело, рассмотренное Кировским районным судом г. Казани.

Участники преступной группы, имея умысел на хищение, договорились с потерпевшим о приобретении у него криптовалюты. Когда потерпевший прибыл на встречу с одним из соучастников, к нему подошли М. и П., которые с целью реализации преступного умысла представились сотрудниками полиции, предъявили поддельные служебные удостоверения, сообщили ложные сведения о том, что потерпевший подозревается в совершении преступления и попросили его пройти с ними в автомашину. Затем соучастники пристегнули потерпевшего за руку к заднему салонному поручню автомашины, применив тем самым в отношении него насилие, не опасное для жизни и здоровья.

В пути следования автомашины М. открыто выхватил из рук потерпевшего мобильный телефон с установленной в нем программой, предназначенной для совершения транзакций с криптовалютой, после чего потерпевшего привезли в безлюдное место.

Далее М. потребовал от потерпевшего при помощи принадлежащего последнему мобильного телефона осуществить перевод криптовалюты с используемого потерпевшим криптокошелька на подконтрольных соучастников криптокошелек, при этом высказал угрозу применения насилия, не опасного для жизни и здоровья, в случае отказа от выполнения его требований. Потерпевший после высказанных в отношении него угроз и примененного в отношении него насилия разблокировал мобильный телефон и осуществил вход в личный кабинет в системе.

После этого М. передал телефон потерпевшего С.М.АА., который, имея доступ к криптокошельку, используемому потерпевшим, осуществил перевод криптовалюты на заранее созданный соучастниками криптокошелек. Указанные действия соучастников квалифицированы судом по п. «б» ч. 3 ст. 161 УК РФ [51].

В другом случае насильственное хищение криптовалюты квалифицировано как разбойное нападение. В результате разбойного нападения группы лиц потерпевший под угрозой применения насилия, опасного для жизни и здоровья, перевел имеющуюся у него криптовалюту на не принадлежащие ему счета, указанные нападавшими. Кроме того, нападавшими было похищено и другое имущество, принадлежащее потерпевшему.

Суд первой инстанции квалифицировал эти действия по п. «б» ч. 4 ст. 162 УК РФ, включив криптовалюту в объем похищенного имущества. Суд апелляционной инстанции согласился с этой квалификацией [3]. Случаи присвоения и растраты криптовалюты в ходе анализа судебной практики не выявлены. Однако исключать возможность хищения цифровой валюты лицом, которому вверено управление ею, конечно, нельзя.

Таким образом, обеспечение информационной безопасности является приоритетным в Российской Федерации. Важным является правовое обеспечение информационной безопасности.

По своей правовой природе, Доктрина информационной безопасности является совокупностью абстрактных и не осуществимых определений и констатации фактов с государственной интеграцией в защиту отдельных явлений и устранения проблем.

В целом, правонарушения в сфере компьютерной информации и вопросы противодействия им являются тем срезом, внимательное изучение которого позволяет заинтересованному глазу увидеть проблему правонарушений в информационной сфере в целом.

## Заключение

В обеспечении информационной безопасности важнейшую роль играет право в качестве средства социального регулирования, поддержанного государственным принуждением. В этой области государство выступает в качестве активного субъекта формирования права правоприменительной деятельности.

В связи с изложенным на современном этапе становления государства интенсивно развивается правовое регулирование отношений в области противодействия угрозам, осознаются и закрепляются приоритетные интересы в информационной сфере.

Активизируется правоприменительная практика в области борьбы с противоправными деяниями против свободы, чести и достоинства личности, конституционных прав и свобод человека и гражданина, реализуемых в информационной сфере, общественной нравственности, законных интересов личности, общества и государства в сфере компьютерной информации.

Все это создает предпосылки для формирования важнейших доктринальных идей правового обеспечения информационной безопасности как важного средства защиты интересов страны в информационной сфере от угроз. Накопленный опыт формирования системы обеспечения информационной безопасности Российской Федерации обнаруживает значительное количество пробелов и противоречий в нормативном регулировании отношений, возникающих в информационной сфере в целом. Именно этим обусловлено определение в Доктрине информационной безопасности Российской Федерации.

Обобщение практики создания системы правового регулирования информационной безопасности и научно-практическое исследование проблем, возникающих в данной области, показало многочисленные недостатки, связанные с отсутствием достаточных теоретических основ правового обеспечения информационной безопасности России.

К преступлениям, совершаемых с использованием цифровых технологий, следует относить преступления, совершаемые в сфере цифровых технологий или с их использованием, в том числе включая незаконное завладение и предложение или распространение информации в информационно-телекоммуникационных сетях и в виртуальной среде, дополняющей реальность. Следует обратить внимание на то, что подобный подход позволяет рассмотреть более широкий круг составов противоправных деяний, совершаемых в рассматриваемой области, чем только киберпреступления (преступления в сфере компьютерной информации).

С определенной долей условности, можно определить следующие типовые варианты применения технологий искусственного интеллекта, при которых необходима продуманная аргументированная уголовно-правовая оценка:

– при создании технологий искусственного интеллекта может быть допущена ошибка, приведшая к совершению преступления;
– в систему искусственного интеллекта был осуществлен неправомерный доступ, повлекший повреждение или модификацию его функций, вследствие чего было совершено преступление;
– искусственный интеллект, обладающий способностью к самообучению, принял решение о совершении действий/бездействия, квалифицируемых как преступление;
– искусственный интеллект был создан самими преступниками для совершения преступлений. Применительно к каждому варианту необходима своя уголовно-правовая оценка.

Выделим основные элементы информационной компетентности, позволяющие обеспечивать достаточную степень информационной безопасности. Во-первых, это знание информационно-коммуникационных технологий и умение работать с ними. Во-вторых, это комплекс знаний, умений и навыков, касающийся функционирования необходимого программного обеспечения. В-третьих, это целевые установки и ценностные

ориентации при работе с информацией, которые должны соответствовать не только нормам законодательства, но и правилам поведения, принятых в конкретном обществе, и мировоззренческим установкам личности.

Отметим, что последний элемент информационной компетентности довольно часто упускается исследователями из виду, а внимание акцентируется на первых двух, хотя именно последняя из указанных составляющих представляется наиболее важной, поскольку именно она является системообразующим фактором, способствующим формированию такого интегративного качества личности, как информационная компетентность.

В свою очередь информационная культура, базирующаяся на информационной компетентности, выступает в качестве такого личностного качества, которое позволяет существенно повышать уровень информационной безопасности. Это особенно важно в школьном возрасте, когда личность наиболее сензитивна к внешнему информационному воздействию, которое в силу несформированности системы ценностных ориентаций и мировоззрения личности подрастающего человека может нанести его психоэмоциональной сфере весьма существенный вред. В этом отношении можно выделить несколько наиболее важных направлений формирования информационной культуры, наиболее важных для обеспечения информационной безопасности детей и молодежи:

- формирование понимания информационной среды не как дикого пространства, живущего по законам джунглей, а как логично организованной структуры;
- формирование критического отношения к информации, поступающей из различных источников, развитие способности оценивать степень её достоверности и качества;
- формирование исследовательского подхода как при работе с информацией, так и в отношении средств информационно-коммуникационных технологий и программного обеспечения.

Осуществленная разработка теоретических и методологических основ правового обеспечения информационной безопасности создает определенный задел для формирования теории и методологии правового обеспечения национальной безопасности, а также вносит определенный вклад в развитие концепции информационного права.

Кроме того, проведенное исследование позволяет:

- обосновать приоритетные направления законотворческой и правоприменительной деятельности государства в области информационной безопасности России;
- эффективно выявлять наиболее острые проблемы недостаточности правового регулирования отношений в области проявления угроз безопасности национальных интересов в информационной сфере и качественно осуществлять подготовку предложений по совершенствованию нормативной базы этого регулирования;
- целенаправленно совершенствовать механизмы правового противодействия угрозам безопасности основных объектов национальных интересов в информационной сфере;
- корректно провести систематизацию законодательства в области обеспечения информационной безопасности Российской Федерации.

Таким образом, информационная безопасность непосредственно определятся уровнем сформированности информационной культуры личности, благодаря которой человек получает возможность ориентироваться в информационных потоках, получать, перерабатывать, создавать и распространять информацию, осуществлять на достаточно высоком качественном уровне любую деятельность в информационной среде.

## Список используемой литературы и используемых источников


1. Алексеева Е. В. Доктрина информационной безопасности Российской Федерации как ключевой аспект правового обеспечения национальной безопасности в информационной сфере / Е. В. Алексеева // Ленинградский юридический журнал. 2016. №4. С. 97-103.
2. Андронникова О. О. Модели девиктимизации человека с ролевой позицией жертвы в социокультурном пространстве // Современные проблемы науки и образования. 2015. № 1. С. 216.
3. Апелляционное определение Ленинградского областного суда от 04 марта 2020 г. по делу № 22-106/2020 [Электронный ресурс] URL: http://sudact.ru/ (дата обращения: 20.03.2022)
4. Апелляционное определение Ленинградского областного суда от 04 марта 2020 г. по делу № 22-106/2020 [Электронный ресурс] URL: http://sudact.ru/ (дата обращения: 20.03.2022)
5. Апелляционное определение Пятого апелляционного суда от 12 марта 2021 г. по делу № 55-15/2021 [Электронный ресурс] URL: http://sudact.ru/ (дата обращения: 20.03.2022)
6. Ахмедшин Р. Л. Юридическая психология: курс лекций Томск: Эль Контент, 2021. 229 с.
7. Бабаш А. В. Информационная безопасность. Лабораторный практикум: Учебное пособие. М. : КноРус, 2016. 188 с.
8. Батчаева З. Х. Информация как предмет преступления в сфере компьютерной безопасности // Актуальные проблемы правоприменения и управления на современном этапе развития общества. Ставрополь, 2021. С. 93-94.
9. Белозеров О. И., Сальникова Е. Ю. Оценка эффективности реализации положений доктрины информационной безопасности Российской Федерации / О.И. Белозеров, Е.Ю. Сальникова // Вестник Хабаровского государственного университета экономики и права. 2019. №2. С. 87-91.

10. Блинов А. Г. Уголовно-правовая охрана личности в эпоху цифровизации и искусственного интеллекта // Уголовный закон в эпоху искусственного интеллекта и цифровизации. Саратов: Изд-во Сарат. гос. юрид. акад., 2021. С. 42-51.

11. Бражник С. Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: автореф. … дисс. на соиск. учен. степ. к.ю.н. Специальность 12.00.08. Ижевск, 2002. С. 12.

12. Вепрев С. Б., Нестерович С. А. О некоторых криминальных направлениях в использовании искусственного интеллекта // Вестник науки. 2019. № 6 (15). С. 377-385.

13. Гомиев Р. Как преступники могут использовать искусственный интеллект? // Hi-News.ru. 07.08.2020. URL: https://hi-news.ru/ (дата обращения: 20.03.2022)

14. Григорьев О. В. К вопросу о реализации административной ответственности за правонарушения в информационной сфере / О. В. Григорьев // Символ науки: международный научный журнал. 2022. № 1-1. С. 38-41.

15. Гурьева Е. Е. Законодательство о компьютерных преступлениях в России и зарубежных странах: сравнительно-правовой анализ // Трансформация права в информационном обществе. Екатеринбург, 2020. С. 355.

16. Джафарова Н. Т. Административно-правовое регулирование отношений, складывающихся в интернет-пространстве / Н. Т. Джаварова // Юридическая наука и правоохранительная практика. 2020. № 4. С. 74-81.

17. Дорогова А. Ваш доктор не будет человеком. Как искусственный интеллект меняет медицину // URL: https://futurist.ru/articles/1452-vash-doktor- (дата обращения: 20.03.2022)

18. Иващенко М. А. Искусственный интеллект в уголовном законодательстве России // Академическая мысль. 2020. № 4 (13). С. 62-65.

19. Информационная безопасность: практикум / С. В. Озёрский, И. В. Попов, М. Е. Рычаго, Н. И. Улендеева. Самара: Самарский юридический институт ФСИН России, 2019. 84с.

20. Информационное право: учебник / под ре. Н.Н. Ковалевой. – Москва: Издательство Юрайт, 2020. С. 73.

21. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 06.03.2022) // Собрание законодательства РФ/ 2002. № 1 (ч. 1). Ст. 1.

22. Конституция Российской Федерации. Принята всенародным голосованием 12.12.1993 г. (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 04.07.2020

23. Корабельников С. М. Преступления в сфере информационной безопасности: учебное пособие / С. М. Корабельников. – Москва: Юрайт, 2020. С. 37.

24. Кто отвечает если беспилотный автомобиль попадет в аварию. URL: https://bespilot.com/chastye-voprosy/kto-otvechaet-esli-ba-popadet-v-avariyu (дата обращения: 20.03.2022)

25. Лавицкая М. И., Крапчатова И. Н. Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации // Российский следователь. 2021. № 6. С. 35 - 41.

26. Малина М. А. Цифровизация российского уголовного процесса: искусственный интеллект для следователя или вместо следователя // Российский следователь. 2021. № 2. С. 29-32.

27. Малюк А. А. Введение в информационную безопасность: Учебное пособие для вузов / А. А. Малюк, В. И. Королев, В. М. Фомичев; Под ред. В. С. Горбатов. Москва: Гор. линия-Телеком, 2017. 288 с.

28. Миронов А. О. Административная ответственность за правонарушения в информационной сфере / А. О. Миронов // EurasiaScience. Москва: Актуальность.РФ, 2021. С. 121-125.

29. Мархат П. М. Искусственный интеллект: правовой взгляд. М. : Буки Веди, 2017. 257 с.

30. Мухаммадиев Ж. У. Информационная безопасность и ее обеспечение: законодательный, административный, процедурный и программно-технический уровни / Ж. У. Мухаммадиев // Юридический факт. 2018. №23. С. 74-78.

31. Найденко С. А. Проблемы уголовно-правовой регламентации преступлений, посягающих на компьютерную информацию // Социально-экономическое развитие России: проблемы, тенденции, перспективы. 2020. С. 80-85.

32. Немова М. И. Криптовалюта как предмет имущественных преступлений // Закон. 2020. № 8. С. 145-154.

33. Никитина Л. С. Влияние цифровизации на способы совершения преступлений в сфере незаконного оборота наркотических средств и психотропных веществ, и их аналогов // Юристъ-Правоведъ. 2021. № 3 (98). С. 198-205.

34. О безопасности : Федеральный закон от 28.12.2010 N 390-ФЗ (ред. от 09.11.2020) // Собрание законодательства РФ. 2011. N 1. Ст. 2.

35. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации : Федеральный закон от 07.12.2011 № 420-ФЗ (ред. от 03.07.2016) // Собрание законодательства РФ. 2011. № 50. Ст. 7362.

36. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года [Электронный ресурс] : Указ Президента РФ от 07.05.2018 № 204 (ред. от 21.07.2020) // Собрание законодательства РФ. 2018. № 20. Ст. 2817.

37. О некоторых вопросах информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ от 22.05.2015 N 260. URL: http://pravo.gov.ru (дата обращения: 20.03.2022).

38. О развитии искусственного интеллекта в Российской Федерации : Указ Президента РФ от 10.10.2019 № 490 (вместе с "Национальной стратегией развития искусственного интеллекта на период до 2030 года") // Собрание законодательства РФ. 2019. № 41. Ст. 5700.

39. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [Электронный ресурс] : Указ Президента РФ от 15.01.2013 N 31с (ред. от 22.12.2017). URL: http://www.pravo.gov.ru (дата обращения: 20.03.2022).

40. О Стратегии национальной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ от 02.07.2021 N 400. URL: http://pravo.gov.ru (дата обращения: 20.03.2022).

41. О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы : Указ Президента РФ от 09.05.2017 № 203 // Собрание законодательства РФ. 2017. № 20. Ст. 2901.

42. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации [Электронный ресурс] : Федеральный закон от 31.07.2020 № 259-ФЗ). URL: http://www.pravo.gov.ru (дата обращения: 20.03.2022).

43. Об информации, информационных технологиях и о защите информации : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 30.12.2021) // Собрание законодательства РФ. 2006. № 31 (1 ч.). Ст. 3448.

44. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс] : Указ Президента РФ от 05.12.2016 N 646. URL: http://www.pravo.gov.ru (дата обращения: 20.03.2022).

45. Об утверждении Концепции развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года

[электронный ресурс] : Распоряжение Правительства РФ от 19.08.2020 N 2129-р. URL: http://www.pravo.gov.ru (дата обращения 20.03.2022).

46. Организационное и правовое обеспечение информационной безопасности: учебник / под ред. Т. А. Поляковой, А. А. Стрельцова. Москва: Юрайт, 2018. С. 125.

47. Осенькина К. В. К вопросу о привлечении к административной ответственности за правонарушения в информационной сфере / К. В. Осенькина // Актуальные проблемы уголовного права и процесса, уголовно-исполнительного права и криминалистики. 2019. С. 161-167.

48. Плешаков В. А. «Форс-мажорная киберпедагогика», или Чрезвычайные условия образования эпохи COVID-19 // Homo Cyberus - электронный научно-публицистический журнал. 2020. № 1 (8). URL: http://journal.hom cyberus.ru/Pleshakov (дата обращения: 20.03.2022).

49. Полыхань К. О. Проблемы и особенности состояния информационной безопасности в соответствии с доктриной информационной безопасности Российской Федерации / К. О. Полыхань // Устойчивое развитие науки и образования. 2019. №5. С. 154-160.

50. Постановление Советского районного суда г. Махачкалы от 09 марта 2021 г. по делу № 1-499/2021 [Электронный ресурс] URL: http://sudact.ru/ (дата обращения: 20.03.2022) Процай А.С. Искусственный интеллект в уголовном праве РФ // Вопросы российской юстиции. 2020. № 10. С. 412-417.

51. Приговор Кировского районного суда г. Казани от 25 апреля 2019 г. № 1-37/2019 [Электронный ресурс] URL: http://sudact.ru/ (дата обращения: 20.03.2022)

52. Приговор Петроградского районного суда г. Санкт-Петербурга по делу № 1-95/2020 [Электронный ресурс] URL: http://sudact.ru/ (дата обращения: 20.03.2022)

53. Разгильдиев Б. Т. Искусственный интеллект и его возможные общественно опасные угрозы // Уголовный закон в эпоху искусственного

интеллекта и цифровизации. Саратов: Изд-во Сарат. гос. юрид. акад., 2021. С. 6-15. 252 с.

54. Рассолов И. М. Информационное право: учебник / И. М. Рассолов. – 5-е изд., перераб. и доп. Москва: Издательство Юрайт, 2020. С. 96.

55. Романова Д. С. Роль информационных технологий в обеспечении национальной безопасности / Д. С. Романова // Научные горизонты. 2020. № 1 (29). С. 182-188.

56. Степенко В. Е. Административная ответственность за правонарушения в информационной сфере / В. Е. Степенко // Юридический мир. 2020. № 8. С. 49-55.

57. Суханов А. Г. Положения по совершенствованию административной ответственности за правонарушения в информационной сфере / А. Г. Суханов // Национальная безопасность России: актуальные аспекты. 2019. С. 65-68.

58. Терещенко Л. К., Тиунов О. И. Информационная безопасность органов исполнительной власти на современном этапе / Л. К. Терещенко, О. И. Тиунов // Журнал российского права. 2015. № 8. С. 100-109.

59. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 09.03.2022) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

60. Фатьянов А. А. О дефиниции «компьютерная информация» в российском уголовном законодательстве // Информационное право. 2017. № 3. С. 11.

61. Федорович В. Ю., Химичева О. В., Андреев А. В. Внедрение технологий информатизации и искусственного интеллекта как перспективные направления развития современного уголовного судопроизводства // Вестник Московского университета МВД России. 2021. № 2. С. 205-210.

62. Хлопов О. А. Проблемы кибербезопасности и защиты критической инфраструктуры // The Scientific Heritage. 2020. № 45-5 (45). С. 64-69.

63. Чемоданова Ю. В. Современные угрозы информационной безопасности РФ // Сибирский экономический журнал. 2019. № 3 (11). С. 4-10.

64. Яковлева Ю. В. Взаимосвязь информационной безопасности и информационной культуры / Ю. В. Яковлева // Вестник науки. 2022. Т. 1. № 1(46). С. 77-81.