Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет»
(национальный исследовательский университет)
институт «Юридический» Кафедра
«Правоохранительная деятельность и
национальная безопасность»

ДОПУСТИТЬ К ЗАЩИТЕ
заведующий кафедрой доцент,
д.ю.н.

_____ Зуев СВ.

«___»_____2019 г.

Информационная безопасность в обеспечении национальной безопасности в Российской Федерации

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА ФГАОУ ВО «ЮУрГУ» (НИУ) .- 40.05.02.2019.604 ВКР

Руководитель работы к.ю.н.,
доцент кафедры
«__ »_____ 2019 г.

Автор работы
Студент группы № Ю-604
_____ Шамин А.С.
« __» _____ 2019 г.

Нормоконтролер к.ю.н., доцент
кафедры
_____ Овчинникова О.В.
« »_____ 2019 г.

Челябинск 2019

АННОТАЦИЯ

Шамин А.С. Выпускная квалификационная работа «Информационная безопасность в обеспечении национальной безопасности в Российской Федерации» ФГАОУ ВО «ЮУрГУ» (НИУ), Ю-604, 82 с., библиогр. список – 62 наим.

Объект исследования – общественные отношения в сфере правового регулирования информационной безопасности РФ.

Предмет исследования – соответствующие статьи нормативных правовых источников, соответствующие разделы и лавы специализированной литературы, материалы правоприменительной практики и периодической печати, раскрывающие вопросы информационной безопасности РФ.

В настоящее время вопрос информационной безопасности остро стоит на уровне как государства, различных организаций, так и отдельных граждан. Важно обеспечить их конституционные права на получение достоверной информации, на ее использование в интересах осуществления законной деятельности учреждений, а также на защиту государственной, коммерческой, семейной, личной и других видов тайн.

Результаты исследования имеют практическую значимость, содержат аргументированные выводы автора, рекомендации автора по совершенствованию норм уголовного права.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 4

1 ПОНЯТИЕ И СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ МЕСТО В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ 5

1.1 Информационная безопасность: понятие, признаки, цели, задачи 5

1.2 Информационная безопасность как составная часть национальной безопасности Российской Федерации 15

1.3 Роль и значение информационной безопасности в жизни современного общества 24

1.4 Становление и развитие института защиты государственной тайны в России 37

2 ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ 44

2.1 Правоохранительные органы как субъекты обеспечения информационной безопасности 44

2.2 Основные направления деятельности правоохранительных органов по обеспечению информационной безопасности 51

2.3 Взаимодействие правоохранительных органов в процессе обеспечения информационной безопасности 59

ЗАКЛЮЧЕНИЕ 71

БИБЛИОГРАФИЧЕСКИЙ СПИСОК 76

ВВЕДЕНИЕ

Актуальность выбранной темы заключается в том, что начало XXI века ознаменовано бурным развитием информационных технологий во всех сферах государственной деятельности и общественной жизни. Информация все в большей мере становится стратегическим ресурсом любого государства, производительной силой и дорогим товаром. Это не может не вызывать стремления государств, организаций и отдельных граждан получить преимущества за счет завладения информацией, нанесения ущерба информационным ресурсам конкурента, а также защиты своих информационных ресурсов. В настоящее время вопрос информационной безопасности остро стоит на уровне как государства, различных организаций, так и отдельных граждан. Важно обеспечить их конституционные права на получение достоверной информации, на ее использование в интересах осуществления законной деятельности учреждений, а также на защиту государственной, коммерческой, семейной, личной и других видов тайн.

Проблемам, связанным с вопросами правового регулирования информационной безопасности РФ, уделяли внимание следующие ученые: В.Я. Богачев, Н.И. Гайдарева, Е.И. Жук, Т.В. Закупень, С.А. Зырянова, Д.В. Иванов, Ю.А. Каптюг, С.А. Клейменов, В.П. Мельников, С.Е. Метелеев, Е.А. Проценко, В.В. Редин, А.А. Соловьев, В.И. Ярочкин и др.

Объект исследования – общественные отношения в сфере правового регулирования информационной безопасности РФ.

Предмет исследования – соответствующие статьи нормативных правовых источников, соответствующие разделы и лавы специализированной литературы, материалы правоприменительной практики и периодической печати, раскрывающие вопросы информационной безопасности РФ.

Цель исследования – комплексно и детально проанализировать правовые основы информационной безопасности РФ, выявить актуальные проблемы в данной сфере, сформулировать рекомендации по их разрешению.

Задачи исследования:

— рассмотреть понятие, признаки, цели и задачи информационной безопасности;

— проанализировать информационную безопасность как составную часть национальной безопасности РФ;

— раскрыть роль и значение информационной безопасности в жизни современного общества;

— изучить международное и российское законодательство в области информационной безопасности;

— рассмотреть Доктрину информационной безопасности РФ;

— выявить актуальные проблемы правового обеспечения информационной безопасности в современной России и определить пути их решения.

Методологическая база исследования представлена следующими методами: методы анализа и синтеза, сравнительно-правовой, обобщения, системный, логический и диалектический методы научного познания.

Нормативно-правовую базу исследования составили законодательные и иные нормативные правовые акты Российской Федерации, регулирующие вопросы информационной безопасности РФ.

Эмпирическая основа настоящего исследования представлена материалами правоприменительной практики.

Практическое значение исследования состоит в том, что сформулированные в нем выводы и предложения могут быть использованы в ходе дальнейшего развития и совершенствования российского законодательства в сфере информационной безопасности РФ.

Структура выпускной квалификационной работы обусловлена целью и задачами настоящего исследования и состоит из введения, основной части (двух глав), заключения и библиографического списка.

1 ПОНЯТИЕ И СУЩНОСТЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЕЕ МЕСТО В СИСТЕМЕ ОБЕСПЕЧЕНИЯ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

1.1 Информационная безопасность: понятие, признаки, цели, задачи

Во всех элементах национальной безопасности – экономической, политической, военной, экологической, правоохранительной и др. – вес информационных факторов постоянно повышается.

Качество информации, ее полнота, своевременность, достоверность определяют не только добротность решений, принимаемых государственными органами и местными органами власти. Информационно-психологические воздействия, реализуемые через СМИ, в обществе могут формировать атмосферу политической нестабильности и напряженности, спровоцировать массовые беспорядки и религиозные, национальные, социальные конфликты, привести к разрушительным последствиям для демократического развития государства.

Незаконное использование, искажение или хищение деловой (статистической, банковской, коммерческой) информации неизбежно влечет возникновение экономических потерь. Уровень развития информационных технологий, на которых базируются современные системы радиоэлектронной борьбы, разведки, управления высокоточным оружием и войсками, значительно предопределяет исход вооруженных конфликтов[1].

Целенаправленные информационные воздействия могут формировать труднопреодолимые препятствия на пути равноправного сотрудничества нашей страны с дружественными странами и развитыми государствами, подорвать авторитет государства на международной арене. Следует также отметить, что информационные воздействия оказывают существенное

[1] Зейналова И.Д., Османов М.Х. Правовое обеспечение информационной безопасности в российском информационном праве // Законность. – 2016. – № 10. – С. 43.

воздействие на процессы формирования, становления личности, ее духовного мира и могут вызвать неадекватное социальное поведение групп людей и определенных лиц, нанести материальный, физический и моральный ущерб людям. Именно в связи с этим национальная безопасность РФ значительным образом зависит от обеспечения информационной безопасности, при этом, в процессе технического прогресса данная зависимость будет только повышаться.

До последнего времени категории «безопасность», методологическим проблемам безопасности как отдельного социального явления уделялось мало внимания, что было обусловлено закрытостью темы безопасности как монопольной сферы политического руководства государства, анализирующего данный термин, большей частью, применительно к военным проблемам государства. В общих энциклопедических изданиях, включая «Новый иллюстрированный энциклопедический словарь» (1999 год), это рассматриваемая категория не предусмотрена. В Большой советской энциклопедии представлен только термин «международная безопасность», который раскрывается как состояние политических, экономических и иных отношений между странами, утверждающее национальную независимость, мирное сосуществование стран на принципах равноправия, самостоятельность народов, а также их свободное становление на демократической основе. Указанным определением «безопасность» сводилось исключительно к противодействию внешним угрозам и опасностям, утверждая, таким образом, официальную позицию того времени об отсутствии внутренних угроз для государственной безопасности[1].

В ст. 3 ФЗ «О безопасности» от 28 декабря 2010 г. № 390-ФЗ содержание деятельности по обеспечению безопасности раскрывается через совокупность следующих элементов:

— прогнозирование, обнаружение, оценка, анализ угроз безопасности;

[1] Гайдарева И.Н. Информационная составляющая национальной безопасности // Общество и право. – 2011. – № 2. – С. 32.

— установление ключевых направлений политики государства и стратегическое планирование в сфере обеспечения безопасности;

— законодательное регламентирование в вышеуказанной сфере;

— использование специальных экономических мер в достижении обеспечения безопасности;

— разработка использование совокупности долговременных и оперативных мер по предупреждению, обнаружению и ликвидации угроз безопасности, локализации и нейтрализации последствий их проявления;

— организация научной деятельности в анализируемой сфере;

— разработка, производство и внедрение современных видов специальной и военной техники, вооружения, а также техники гражданского и двойного назначения в достижении обеспечения безопасности;

— финансирование расходов на обеспечение безопасности, контроль за целевым расходованием выделенных средств;

— координация работы государственных органов федерального уровня, субъектов РФ, местных органов власти в сфере обеспечения безопасности;

— международное сотрудничество в рассматриваемой области;

— реализация иных мероприятий в сфере обеспечения безопасности на основании действующих законодательных норм[1].

Информационная безопасность – сложное многоуровневое, системное явление, на состояние и перспективы становления которого оказывают прямое влияние внутренние и внешние факторы. Наиболее значимыми из них выступают: существование потенциальных внутренних и внешних угроз; мировая политическая обстановка; внутриполитическая обстановка в стране; уровень и состояние информационно-коммуникационного развития государства. Рассматривая вышеуказанную категорию, отдельные авторы нередко раскрывают данное понятие в узком понимании, как совокупность

[1] Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ // Собрание законодательства РФ. – 2010. – № 42. – Ст. 5633.

программных и аппаратных средств для обеспечения сохранности, конфиденциальности и доступности данных в компьютерных сетях. На их взгляд, то, что в 1970-е г.г. именовалось компьютерной безопасностью, а в 1980-е – безопасностью данных, в настоящее время называется информационной безопасностью.

Вышеуказанную категорию они раскрывают как «меры по защите информации от неавторизованного доступа, модификации, разрушения, раскрытия и задержек в доступе», при этом, применяют понятие «критические данные», под которым подразумевают данные, которые требуют защиты по причине вероятности риска (нанесения) ущерба и его размера в том случае, если произойдет умышленное или случайное раскрытие, разрушение или изменение данных[1].

На основании представленной логики цель рассматриваемого явления – обезопасить ценности системы, гарантировать и защитить целостность, точность информации и минимизировать разрушения, которые могут быть, если будет разрушена или модифицирована информация. Информационная безопасность предоставляет гарантию того, что достигаются определенные цели: конфиденциальность критической информации, целостность информации и связанных с ней процессов (создания, обработки, ввода и вывода), доступность информации, когда она необходима, учет всех процессов, с ней связанных. Иные авторы под анализируемой категорией подразумевают «защищенность информации и поддерживающей инфраструктуры от преднамеренных или случайных воздействий искусственного или естественного характера, опасных нанесением ущерба пользователям информации, владельцам и поддерживающей инфраструктуры»[2], обозначая, таким образом, уже два объекта защиты – информационную инфраструктуру и информацию. В Доктрине

[1] Закупень Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности Российской Федерации // Наука. Общество. Право. – 2015. – № 2. – С. 123.
[2] Копылов В.А. Информационное право: учебник. – М.: Норма, 2013. – С. 189.

информационной безопасности РФ данное понятие рассматривается состояние защищенности личности, государства, общества от внешних и внутренних информационных угроз, при котором обеспечиваются осуществление прав и свобод личности, гарантированные Конституцией РФ, достойные уровень и качество жизни населения, устойчивое социально-экономическое развитие РФ, территориальная целостность, суверенитет, безопасность и оборона страны[1].

Информационная безопасность выступает элементом национальной безопасности наряду с государственной, экономической, экологической, общественной, энергетической, транспортной, безопасностью личности (п. 6 Указа Президента РФ от 31 декабря 2015 г. № 683 «О Стратегии национальной безопасности Российской Федерации»).

В соответствии с п. 34 Доктрины информационной безопасности РФ деятельность органов государственной власти по обеспечению информационной безопасности базируется на следующих началах:

— законность общественных отношений в информационной сфере и правовое равенство всех субъектов данных отношений, базирующиеся на конституционном праве граждан свободно искать, передавать, получать, распространять, производить информацию любым законным способом;

— соблюдение баланса между потребностью лиц в свободном обмене информацией и ограничениями, связанными с потребностью обеспечения национальной безопасности, включая, безопасность в рассматриваемой сфере;

— конструктивное взаимодействие органов государственной власти, юридических и физических лиц при выполнении задач по обеспечению анализируемой безопасности;

[1] Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05 декабря 2016 г. № 646 // Российская газета. – 2016. – 16 декабря.

— соблюдение общепризнанных начал и международно-правовых норм, международных договоров РФ, а также российских законодательных норм;

— достаточность сил и средств обеспечения информационной безопасности, устанавливаемая в том числе, с помощью постоянной реализации мониторинга информационных угроз.

Стратегической целью обеспечения анализируемой безопасности в сфере обороны государства выступает охрана жизненно значимых интересов личности, государства и общества от внешних и внутренних угроз, связанных с использованием информационных технологий в военно-политических целях, противоречащих международному праву, в том числе, в достижении реализации враждебных действий и актов агрессии, направленных на нарушение территориальной целостности стран, подрыв суверенитета, и представляющих угрозу стратегической стабильности, безопасности, международному миру (п. 20 Доктрины информационной безопасности РФ).

Стратегическими целями обеспечения исследуемой безопасности в сфере безопасности государства и общества выступает охрана суверенитета, поддержание территориальной целостности РФ, социальной и политической стабильности, обеспечение основных прав и свобод личности, а также защита критической информационной инфраструктуры (п. 22 Доктрины информационной безопасности РФ).

Вышеуказанными целями обеспечения информационной безопасности в экономической сфере выступают сведение к минимально возможному уровню воздействия отрицательных факторов, определенных недостаточным уровнем развития отечественной сферы электронной промышленности и информационных технологий, разработка и выпуск конкурентоспособных средств обеспечения информационной безопасности, а также рост качества и объемов предоставления услуг в рассматриваемой сфере (п. 24 Доктрины информационной безопасности РФ).

Соответствующей целью обеспечения информационной безопасности в сфере технологий, науки и образования выступает поддержка ускоренного и инновационного развития системы обеспечения информационной безопасности, сферы электронной промышленности и информационных технологий (п. 26 Доктрины информационной безопасности РФ).

Применительно к сфере стратегической стабильности и равноправного стратегического партнерства вышеуказанной целью выступает создание устойчивой системы межгосударственных неконфликтных отношений в информационном пространстве (п. 28 Доктрины информационной безопасности РФ).

Задачами органов государственной власти в границах деятельности по обеспечению информационной безопасности признаются:

— обеспечение защиты прав и законных интересов физических и юридических лиц в сфере информации;

— планирование, реализация и оценка результативности совокупности мер по обеспечению информационной безопасности;

— организация деятельности и координация взаимодействия сил обеспечения вышеуказанной безопасности, развитие их организационного, правового, разведывательного, контрразведывательного, оперативно-разыскного, информационно-аналитического, научно-технического, экономического и кадрового обеспечения[1];

— разработка и выполнение мер государственной поддержки юридических лиц, реализующих деятельность по подготовке, выпуску и эксплуатации средств обеспечения информационной безопасности, по предоставлению услуг в анализируемой сфере, а также юридических лиц, реализующих образовательную деятельность в указанной сфере;

— оценка состояния информационной безопасности, прогнозирование и выявление угроз в информационной сфере, установление

[1] Голубчиков С.В., Новиков В.К., Баранова А.В. Уровни и правовая модель информационной безопасности (защиты информации) // Программные продукты и системы. – 2017. – № 2(30). – С. 320.

основополагающих направлений их предотвращения и устранения последствий их проявления.

С.В. Голубчиков, В.К. Новиков и А.В. Баранова отмечают, что ключевыми задачами в анализируемой сфере выступают: осуществление конституционных прав и свобод личности в области информации; интеграция нашей страны в мировое информационное пространство; защита и совершенствование российской информационной инфраструктуры, противодействие угрозе развязывания противоборства в сфере информации[1].

Анализ действующих законодательных норм РФ позволяет сформулировать заключение о том, что они на сегодняшний день включает положения, регламентирующие большое число (несколько десятков) видов тайн. Российские законодательные нормы, регламентирующие правовые отношения, возникающие относительно разных видов тайны, образуют особенный конфиденциальный правовой режим информации ограниченного доступа, характерными признаками которого признаются: неизвестность информации для других лиц; отсутствие свободного доступа к информации на законном основании; существование законных интересов участников в защите указанной информации в присущем ей режиме. Конфиденциальный правовой режим подразделяется на виды в зависимости от разновидностей тайны: режим государственной тайны, режим профессиональной тайны, режим коммерческой тайны, режим личной и семейной тайны, режим персональных данных.

В соответствии с правовым подходом Конституционного Суда РФ, ограничение доступа к информации предусматривается федеральными законами в целях защиты основ конституционного строя, здоровья, нравственности, прав и законных интересов иных лиц, обеспечения обороны

[1] Голубчиков С.В., Новиков В.К., Баранова А.В. Уровни и правовая модель информационной безопасности (защиты информации) // Программные продукты и системы. – 2017. – № 2(30). – С. 321.

государства и безопасности страны; обязательным выступает соблюдение конфиденциальности данной информации[1].

За нарушение конфиденциального правового режима виновные лица привлекаются к юридической ответственности. В качестве примера можно привести материал конкретного гражданского дела, которое находилось в производстве Магнитогорского городского суда Челябинской области, по смыслу которого А.В. Петрова обратилась в суд с иском к центральной районной больнице о взыскании денежной компенсации морального вреда, причиненного в результате разглашения врачебной тайны. В суде установлено, что главным врачом центральной районной больницы в адрес руководителя социальной защиты населения и в адрес Комиссии по делам несовершеннолетних и защите их прав было направлено сообщение, в котором сообщались сведения о факте обращения, постановке на учет и диагнозе А.В. Петровой. Опираясь на предоставленные доказательства и нормы российского законодательства, суд посчитал доказанным факт разглашения ответчиком врачебной тайны, а именно диагноза истицы третьим лицам без ее согласия. Суд решил взыскать в пользу А.В. Петровой с центральной районной больницы денежную компенсацию морального вреда, денежную компенсацию судебных расходов[2].

Проблемой современного законодательства выступает то, что на сегодняшний день не детализированы определения категорий семейной и личной тайны, на которые ссылаются многие законодательные источники (Конституция РФ, ГК РФ, УК РФ, ряд федеральных законов).

На основании п. 31 Указа Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» для защиты данных в РФ следует обеспечить баланс между

[1] Определение Конституционного Суда Российской Федерации от 07 февраля 2013 г. № 134-О // Вестник Конституционного Суда РФ. – 2013. – № 4.
[2] Решение Орджоникидзевского районного суда г. Магнитогорска Челябинской области от 23 марта 2017 г. по делу № 11-24/2017. – Режим доступа: http://sudact.ru/

своевременным внедрением современных технологий обработки данных и защитой прав лиц, включая право на семейную и личную тайну.

Следует отметить, что ни в Стратегии развития информационного общества в РФ, ни в Доктрине информационной безопасности РФ не раскрываются вопросы обеспечения информационной безопасности иностранных лиц и лиц без гражданства, которые находятся на российской территории.

На доктринальном уровне обращается внимание на то, что вопросы обеспечения информационной безопасности как страны в целом, так и граждан являются одними из ключевых. По причине изложенного, целесообразно:

— сделать более конкретным определение информационной безопасности физических лиц (граждан), а также определение семейной и личной тайны физических лиц (граждан) и предусмотреть их в самостоятельном правовом источнике;

— ввести (усилить) ответственность должностных лиц за обеспечение информационной безопасности в отношении подчиненных им сотрудников (работников);

— подготовить комплексную совокупность организационных мер, направленных на обеспечение информационной безопасности физических лиц (граждан) в организациях (учреждениях, предприятиях), где они работают (подготовить типовые политики, процедуры и правила обеспечения информационной безопасности и др.). Предусмотреть в указанной системе орган государственной власти, на который будут возложены вспомогательные полномочия по подготовке определенных мероприятий и контролю за их выполнением, а также координации работы иных государственных органов в данном направлении[1].

[1] Соловьева Е.С. Информационная безопасность в современном обществе // Наука. Практика. Право. – 2015. – № 5. – С. 12.

Даже частичное осуществление указанных мероприятий позволит добиться реального обеспечения безопасности граждан в информационной сфере, а вместе с этим, и информационной безопасности всего российского государства и общества.

Подводя итог, отметим, что под информационной безопасностью подразумевают состояние защищенности личности, государства и общества от внешних и внутренних информационных угроз, при котором обеспечиваются осуществление конституционных прав и свобод личности, достойные уровень и качество жизни людей, устойчивое социально-экономическое развитие РФ, территориальная целостность, суверенитет, безопасность и оборона государства. Информационная безопасность признается элементом национальной безопасности наряду с государственной, экологической, общественной, транспортной, экономической, энергетической, безопасностью личности. Ключевыми задачами обеспечения информационной безопасности выступают: осуществление конституционных прав и свобод личности в информационной сфере; интеграция нашей страны в мировое информационное пространство; защита и совершенствование российской информационной инфраструктуры; противодействие угрозе развязывания противоборства в сфере информации.

1.2 Информационная безопасность как составная часть национальной безопасности Российской Федерации

Национальная безопасность является многоплановым явлением. Ее следует рассматривать, исходя из масштабов обеспечения, как разновидность международной безопасности. Национальная безопасность органически связана с региональной и международной (глобальной) безопасностью[1].

[1] Гайдарева И.Н. Информационная составляющая национальной безопасности // Общество и право. – 2011. – № 2. – С. 32.

Национальная безопасность – состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие РФ, оборону и безопасность государства.

Национальная безопасность характеризует положение страны, при котором ей не угрожает опасность войны либо других посягательств на суверенное развитие. Национальная безопасность – это состояние государства, при котором сохраняется его целостность и возможность быть самостоятельным субъектом системы международных отношений.

Сама по себе национальная безопасность представляет геополитический аспект безопасности вообще, охватывающий весь комплекс вопросов физического выживания государства, защиты и сохранения его суверенитета и территориальной целостности. В той мере, в какой задачи обеспечения национальной безопасности являются производными от национальных интересов, концепции национальной безопасности также связаны с теоретическим обобщением данных интересов[1].

В рамках национальной безопасности национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Угрозами национальной безопасности России в информационной сфере, представляющими серьезную опасность, являются: стремление ряда стран к доминированию в мировом информационном пространстве; вытеснение России с внешнего и внутреннего информационных рынков; разработка рядом государств концепций информационных войн; возможность нарушения нормального функционирования информационных

[1] Закупень Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности Российской Федерации // Наука. Общество. Право. – 2015. – № 2. – С. 124.

и телекоммуникационных систем, получения несанкционированного доступа к ним.

Основными задачами по обеспечению национальной безопасности РФ применительно к теме информационной безопасности являются:

— своевременное выявление и нейтрализация внешних и внутренних угроз национальной безопасности РФ;

— преодоление научно-технической и технологической зависимости РФ от внешних источников;

— обеспечение личной безопасности граждан РФ, их конституционных прав и свобод;

— обеспечение полноты и совершенствование законодательства РФ при обеспечении приоритета федерального законодательства;

— принятие эффективных мер по пресечению разведывательной и подрывной деятельности иностранных государств против РФ;

— разработка организационных и правовых механизмов защиты государственной целостности, единства правового пространства и национальных интересов России;

— выработка и реализация региональной политики, обеспечивающей оптимальный баланс федеральных и региональных интересов;

— совершенствование механизма предупреждения возникновения политических партий и общественных объединений, преследующих сепаратистские и антиконституционные цели, и пресечения их деятельности[1].

Представляется, что решение вышеназванных задач обеспечения национальной безопасности страны возможно лишь при создании целостной системы, включающей совокупность законодательных актов и созданных на их основе структур и механизмов взаимодействия по защите интересов субъектов правоотношений. Устойчивость системы должна основываться на общенациональном согласии.

[1] Зейналова И.Д., Османов М.Х. Правовое обеспечение информационной безопасности в российском информационном праве // Законность. – 2016. – № 10. – С. 43.

Одной из основных составляющих системы обеспечения национальной безопасности является информационная безопасность, выступающая важным связующим звеном всех основных компонентов государственной политики в единое целое. При этом, совершенно очевидно, что роль информационной безопасности и ее место в системе национальной безопасности страны становится все значительней. Это происходит в силу следующих причин:

— национальные интересы, угрозы им и обеспечение защиты от этих угроз во всех областях национальной безопасности выражаются, реализуются и осуществляются через информацию и информационную сферу;

— человек и его права, информация и информационные системы и права на них – это основные объекты не только информационной безопасности, но и основные элементы всех объектов безопасности во всех ее областях;

— решение задач национальной безопасности связано с использованием информационного подхода как основного научно-практического метода;

— проблема национальной безопасности имеет ярко выраженный информационный характер[1].

Вышеназванные обстоятельства, наряду с задачами построения гражданского общества в РФ как общества информационного, возрастанием роли информации, информационных ресурсов и технологий в развитии гражданского общества и государства в XX1 веке выводят вопросы информационной безопасности на первый план в системе обеспечения национальной безопасности.

Роль информационной безопасности и ее место в системе национальной безопасности страны определяется также тем, что государственная информационная политика тесно взаимодействует с

[1] Кучерявый М.М. Анализ концептуальных основ политики национальной безопасности // Среднерусский вестник общественных наук. – 2014. – № 1. – С. 81.

государственной политикой обеспечения национальной безопасности страны через систему информационной безопасности, где последняя выступает важным связующим звеном всех основных компонентов государственной политики в единое целое.

Национальная безопасность неразрывно связана с деятельностью государства. Только оно может, опираясь на свой аппарат, властные органы, деятельность которых поставлена в жесткие рамки и подкрепляется соответствующими правовыми актами, обеспечить покой граждан, создать благоприятные условия для их жизни и деятельности. Никакие другие социальные силы не смогут выполнить этой задачи. Обеспечение собственной безопасности, а также безопасности своих граждан является одной из основных задач, но не функций любого государства[1].

Успешное развитие и само существование России как суверенного государства невозможно без обеспечения ее национальной безопасности. Право не может и не должно оставаться в стороне от решения проблем безопасности государства. Более того, в этом ему должна принадлежать ведущая роль.

В 2014 г. была принята Концепция Евразийской безопасности, в соответствии с которой основными угрозами информационной безопасности являются:

— стремление ряда стран к доминированию в мировом информационном пространстве, разработка рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним;

[1] Шамсуев М.Х. Теоретические аспекты изучения информационной безопасности // Инновационная наука. – 2016. – № 1. – С. 46.

— использование информационных технологий в целях манипуляции общественным мнением;

— использование информационных технологий в целях дезинформации мирового сообщества, информационного обеспечения санкций экономического, политического и военного характера вплоть до военной агрессии;

— использование информационных технологий в качестве инструмента культурного разложения, пропаганды асоциального образа жизни, отрицания норм морали и общекультурных ценностей;

— внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;

— разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

— уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи[1];

— компрометацию ключей и средств криптографической информации;

— утечку информации по техническим каналам;

— внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

— уничтожение, повреждение, разрушение или хищение машин и других носителей информации;

— перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

[1] Зейналова И.Д., Османов М.Х. Правовое обеспечение информационной безопасности в российском информационном праве // Законность. – 2016. – № 10. – С. 43.

— несанкционированный доступ к информации, находящейся в базах данных.

В качестве основных направлений создания системы коллективной информационной безопасности, в соответствии с концепцией Евразийской национальной безопасности определены:

— реализация конституционных прав и свобод граждан в сфере информационной безопасности;

— совершенствование и защита информационной инфраструктуры, интеграция государств (Белоруссии, России, Казахстана, Кыргызстана, Узбекистана) в мировое информационное пространство;

— противодействие угрозе развязывания противоборства в информационной сфере;

— ограничение доступа к информации, содержащей пропаганду террористической, экстремистской и преступной деятельности, травмирующей личность информации, особенно в отношении несовершеннолетних;

— создание системы противодействия монополизации отечественными и зарубежными структурами составляющих информационной инфраструктуры, включая рынок информационных услуг и СМИ;

— разработку, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения[1].

Исходя из того, что информационная безопасность в XXI веке выходит на первое место в системе национальной безопасности, формирование и проведение единой государственной политики в этой сфере должно приобретать приоритетное значение. Однако, как показывает действительность, одним из наиболее существенных факторов, оказывающих

[1] Зейналова И.Д., Османов М.Х. Правовое обеспечение информационной безопасности в российском информационном праве // Законность. – 2016. – № 10. – С. 44.

детерминирующее воздействие на состояние информационной безопасности, являются устойчивые негативные тенденции в развитии информационного пространства в современной России, где среди основных причин выделяются: отсутствие понятной национально-государственной идеологии развития; неопределенность внешнеполитических приоритетов безопасности; недостаток выделяемых финансово-экономических ресурсов для обеспечения информационной безопасности; отсутствие персональной государственной ответственности за данное направление и отсутствие достойного кадрового потенциала; низкая эффективность и ограниченные возможности промышленного комплекса информационных технологий и др.

К тому же, по мнению целого ряда специалистов, развитие информационной организации России является второстепенным направлением деятельности политического руководства. В то же время, в документах нормативного характера и выступлениях первых лиц делается акцент на возросшем значении и увеличении спектра угроз информационной безопасности государства, особенно в связи с усилением активности международного терроризма, высокой вероятностью продолжения внутриполитических конфликтов, влиянием геополитических факторов, а также негативными факторами процессов глобализации[1].

Однако, при этом, политическое руководство не предпринимает радикальных шагов по защите информационного пространства России как одной из составляющих национальной безопасности государства. Об этом свидетельствуют: не всегда успешное и эффективное использование российской дипломатии в целях создания новых межгосударственных структур безопасности и иных механизмов урегулирования конфликтов в ходе переговорных процессов; ускоренное развитие процессов внедрения информационных технологий во все сферы деятельности за рубежом в условиях отсутствия видимых позитивных результатов преобразований в

[1] Иванов Д.В. Правовые проблемы определения объектов информационной безопасности Российской Федерации // Пробелы в российском законодательстве. – 2015. – № 8. – С. 34.

России; активизация распространения продукции информационных технологий зарубежными государствами и насаждение своих стандартов России; недостаточное государственное финансирование программ, обеспечиваюших развитие науки и промышленности в области современных информационных технологий[1].

По нашему мнению, причина кроется в отсутствии государственной политики (идеологии), отражающей потребности строительства сильного независимого государства. Такая идеология должна быть основана на приоритетах человеческих ценностей, социальной справедливости, уважения к духовным и историческим традициям народов, населяющих суверенную территорию, а также на идеях самосохранения и самосовершенствования.

В контексте рассматриваемой проблемы следует особо отметить, что защита информационного пространства (информационная безопасность) органами государственной власти и управления реализуется в отрыве от результатов исследований отечественной науки, то есть научный потенциал страны был и остается практически невостребованным. Это свидетельствует об игнорировании научных основ решения важнейших задач в области защиты информационного пространства и обеспечения информационной безопасности государства, как гуманитарной, так и технической ее составляющей. Между тем, опора на научные исследования в оптимизации государственного управления является важнейшим принципом, используемым в наиболее динамично развивающихся государствах мира. Так, в США неписаной нормой является назначение на должности советников президента по национальной безопасности ученых мировой величины. В свое время эти должности занимали Г. Моргентау, Г. Киссинджер, З. Бжезинский, К. Райс. К тому же в США ни одно из решений политического характера не принимается без предварительной научной экспертизы и рекомендаций научного сообщества. Вполне очевидно, что

[1] Закупень Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности Российской Федерации // Наука. Общество. Право. – 2015. – № 2. – С. 125.

аналогичная потребность использования научного потенциала должна существовать и в России. Разработка же научной методологии деятельности органов государственной власти должна осуществляться в интересах обеспечения эффективности информационной безопасности страны и ее информационных ресурсов. При этом, рациональная стратегия обеспечения информационной безопасности должна основываться на долгосрочных планах, учитывающих характер внешних и внутренних информационных угроз, приоритетах по обеспечению информационной безопасности государства и реальных экономических возможностях. От того, как будут решаться эти вопросы, зависит – в каком обществе мы будем жить[1].

Подводя итог, отметим, что информационная безопасность является составной частью общей и национальной безопасности и охватывает все сферы деятельности государства, гражданина, а также различных организаций и бизнеса.

1.3 Роль и значение информационной безопасности в жизни современного общества

Современная правовая и информационная политика РФ направлена, прежде всего, на построение российского государства в соответствии со ст. 1 Конституции РФ как правового демократического, в котором соблюдается приоритет прав и свобод человека и гражданина, их защита и охрана.

Правовая, информационная системы общества, включающие в себя как субъекты права и информационного поля, так и формы их правового, технического, информационного взаимодействия, активно развивается в сторону информатизации, что необходимо в целях оптимизации юридического документооборота. Однако сегодня, как относительно новая и

[1] Михнев И.П., Михнева С.В., Сальникова Н.А. Информационная безопасность в Российской Федерации: современность и перспективы развития // Общество и право. – 2017. – № 3. – С. 56.

потому еще только развивающаяся сфера современной государственно-правовой действительности информационное пространство не достаточно полно и оптимально урегулировано правовыми нормами.

Нужды и вызовы современной жизни выдвигают ряд требований к законодателю, направленных на повышение эффективности и устранению юридических неточностей, упущений, коллизий и пробелов в сфере защиты информации. И, как следствие, незаконное и (или) случайное распространение информации, носящей строго конфиденциальный характер, вызванное неправомерными действиями сотрудников государственных и муниципальных организаций, учреждений и предприятий проводит к неточному исполнению или к неисполнению должностных профессиональных обязанностей и полномочий, подрывает авторитет государственной власти и муниципальных сообществ[1].

Современная геополитическая ситуация в мире, обусловленная борьбой с террористическими угрозами, нарушающими безопасность людей и, в целом, государств, противоречащими правам человека, диктует принятие своевременных мер, в том числе, по защите информационных ресурсов, систем и обеспечению информационной безопасности. В то же время, обострение конфликтов и столкновение экономических, политических и территориальных интересов различных государств не способствует эффективному взаимному межгосударственному сотрудничеству в разных областях и направлениях, успешному обмену информационными данными, показателями и достижениями.

В связи с чем, все чаще сегодня приходит слышать понятие – информационная война, которое прочно входит в международный оборот, диктуя свои правила игры и условия развития межгосударственных отношений, и целенаправленно разрушает давно уже принятие и

[1] Соловьева Е.С. Информационная безопасность в современном обществе // Наука. Практика. Право. – 2015. – № 5. – С. 12.

узаконенные, ратифицированные всеми государствами принципы и нормы межгосударственных союзов и альянсов.

Современные закономерности и тенденции широкомасштабного ускоряющегося процесса развития и, при этом, совершенствования информационных систем и технологий наглядно демонстрируют возрастание актуальности проблемы поиска высокого уровня технических, юридических, организационных и иных мероприятий обеспечения информационной безопасности в сегодняшних условиях, когда множество внедряющихся компьютерных вирусов и информационные войны угрожают национальной безопасности нашего государства.

В соответствии с законодательством государственное регулирование в сфере применения информационных технологий предусматривает развитие информационных систем различного назначения для обеспечения граждан, организаций, органов государственной власти и местного самоуправления информацией, а также обеспечение взаимодействия таких систем[1].

Актуальность и восстребованность информационных потоков и обеспечение их безопасности позволяет определить с позиции юридической науки в системе права нового структурного элемента – правового обеспечения информационной безопасности, процесс возникновения которого носит объективный характер. Он обусловлен научно-техническим прогрессом, развитием информационных технологий, возрастанием экономической и социальной значимости информации, развитием информационного общества и возникновением угроз интересам его субъектов, необходимостью охраны социально значимых ценностей в информационной сфере и совершенствования законодательства об информационной безопасности.

Информационные потоки охватывают практически все сферы общественной жизнедеятельности, а потому, нуждаются в

[1] Зиновьева Е.С. Развитие информационного общества: проблемы безопасности // Вестник МГИМО Университета. – 2014. – № 4. – С. 36.

скоординированности, внешнем управлении и точном распределении. Прежде всего, управление информационными потоками должно осуществляться на уровне государственной власти. Органы власти и федерального, и регионального уровня осуществляют как общее управление информатизацией общества, так и контроль за этой деятельностью. В связи с чем, важное значение уделяется информационной безопасности в сфере государственного управления, в деятельности органов государственной власти. Не менее важное значение отводится и органам местного самоуправления, которые непосредственно осуществляя муниципальную демократию, работают с местным населением, отвечая за эффективность, доступность и своевременность информационного пространства муниципалитета[1].

Следует отметить, что законодательные основы любого государства в области информационной безопасности являются необходимой мерой, удовлетворяющей первейшую потребность в защите информации при развитии социально-экономических, политических, военных направлений функционирования этого государства. В современных условиях информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности России. Обусловлено это, прежде всего, быстро растущими технологическими возможностями современных информационных систем, которые по своему влиянию на хозяйственно-экономическую жизнь, духовно-идеологическую сферу и умонастроения людей стали в настоящее время решающими.

Информационная безопасность касается, прежде всего, государственных информационных ресурсов, которые несут сведения, представляющие значительную ценность в той или иной степени. Важность их сохранения обусловлена тем, что это информация, которая содержится в государственных информационных системах, а также различного рода

[1] Ахметьянова А.И., Кузнецова А.Р. Проблемы обеспечения информационной безопасности в России и ее регионах // Фундаментальные исследования. – 2016. – № 8. – С. 82.

сведения и документы, имеющиеся в распоряжении государственных органов.

Анализ действующего законодательства, регламентирующего обеспечение информационной безопасности, позволяет выделить элементы правового информационного пространства, то есть элементы, нуждающиеся в информационной безопасности. Прежде всего, важным звеном являются информационные системы. Информационные системы представляют собой разновидность технологических систем, объединяющих в себе и совмещающих технические, программные и другие типы средств, создающих структурно и функционально несколько видов информационных процессов, и при этом, предоставляющих разного рода информационных услуг[1].

В соответствии со ст. 2 ФЗ об информации информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств[2]. Информационные системы включают в себя как государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов федерации, на основании правовых актов государственных органов, так и муниципальные информационные системы, созданные на основании решения органа местного самоуправления. Информация, содержащаяся в государственных информационных системах, является официальной.

Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной

[1] Зиновьева Е.С. Развитие информационного общества: проблемы безопасности // Вестник МГИМО Университета. – 2014. – № 4. – С. 36.

[2] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. – 2006. – № 23. – Ст. 2135.

системе, доступ к указанной информации, а также защиту информации от неправомерных действий, в частности, доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных. Как от имени самой РФ, так и ее субъекта и муниципального образования правомочия обладателя информации осуществляются государственными органами и органами местной власти в пределах их определенных полномочий, установленных соответствующими нормативными правовыми актами[1].

Обладатель информации при осуществлении своих прав обязан принимать меры по защите информации. При этом не может быть ограничен доступ к информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств. Исключением являются сведения, составляющие тайну – государственную или служебную. Введен запрет на ограничение доступа к информации и данным, содержащимся в законодательных и иных нормативно-правовых актах, устанавливающих и закрепляющих правовой статус (положение) организаций, предприятий и учреждений, компетенцию государственных федеральных и региональных органов, юридическое положение муниципалитетов и полномочия органов местного самоуправления.

На основании закрепленных норм и положений закона федеральные и региональные государственные органы и органы местного самоуправления, в частности, – глава муниципального образования, местная дума и местная администрация – должны своевременно и качественно исполнять должностные профессиональные обязанности по обеспечению доступа граждан субъекта или муниципалитета к информации о своей деятельности. В процессе обеспечения информирования жителей закон разрешает органам государственной власти и органам местного самоуправления использовать возможности информационно-телекоммуникационных сетей, в том числе,

[1] Грачев С.И., Герасин О.Н., Колобов А.О., Ливерко М.И. Проблемные аспекты в информационной политике и информационной безопасности России // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2014. – № 1(1). – С. 291.

сети «Интернет». Язык информации определяется как русский, так и государственный язык республики в составе РФ. Эта деятельность должна проходить в соответствии с действующим федеральным и региональным законодательством РФ, а также с учетом положений муниципальных правовых актов. Законом не устанавливается к лицам, желающим получить доступ к информации о правовых основах организации и деятельности органов власти, обязанность обоснования и объяснения необходимости получения таких сведений[1].

Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами РФ, регулирующими правоотношения в рассматриваемой сфере деятельности.

Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с законами различные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулирующими правоотношения в установленной сфере деятельности. Одним из факторов, способствующих повышению опасности угроз информационной безопасности, является

[1] Ковалева Н.Н. Информационное право России: учебник. – М.: Проспект, 2014. – С. 194.

дефицит квалифицированных кадров, обусловленный снижением эффективности системы образования и воспитания, в частности, в сфере информационных систем и технологий[1].

Подготовка квалифицированных кадров в области информационной безопасности и информационных технологий осуществляется по двум основным направлениям – технологическому и гуманитарному. Технологическая составляющая информационной безопасности включает в себя проблемы, связанные с развитием индустрии информатизации, обеспечением потребностей внутреннего рынка ее продукцией и выходом этой продукции на мировой рынок, а также с обеспечением безопасности информационных и телекоммуникационных систем. Современные компьютеры, глобальные информационные сети и сетевые технологии сильно изменили нашу жизнь, но вместе с новыми возможностями у нас появились и новые риски. На повестку дня закономерно встают главные вопросы обеспечения безопасности информационных технологий, в частности о том, как использовать такие возможности, нейтрализуя риски или снижая возможный ущерб от их реализации. Для ответа на этот и другие важные вопросы необходимо решить большое количество разнообразных задач: и политических, и экономических, и научных, и технических, технологических. На сегодняшний день развитие экономических, политических, правовых отношений, увеличение информационного потока и способов его обработки и интерпретации, закономерно предполагает рост информационных технологий, массовость вовлечения их в деятельность органов государственной власти и местного самоуправления.

Анализ действующего федерального законодательства, а также практика его применения позволяют утверждать усиление тенденции обеспечения информационной безопасности в органах государственной власти и муниципального управления в современной России. Однако,

[1] Михнев И.П., Михнева С.В., Сальникова Н.А. Информационная безопасность в Российской Федерации: современность и перспективы развития // Общество и право. – 2017. – № 3. – С. 58.

сегодня, подводя первые итоги функционирования в новых правовых, экономических и политических условиях, нельзя однозначно утверждать о стабильности и эффективности в такой сфере как обеспечение информационной безопасности.

Также следует отметить, что становление информационного общества, позволяя пользоваться благами современной цивилизации, порождает одновременно с этим потенциальные опасности использования информационных технологий в антиобщественных целях. Поэтому деятельность в информационной сфере требует принятия действенных мер, обеспечивающих ее надежной безопасностью. Наряду с уже прочно устоявшимися и утвердившимися принципами организации и осуществления органами государственной власти, реалии и требования общественной жизни диктуют своевременные изменения и совершенствования действующего механизма информационной безопасности государства[1].

Сегодня современное демократическое гражданское общество, обстоятельно требуя от государства максимального обеспечения и удовлетворения интересов, нужд и потребностей в информационных ресурсах в процессе предоставления определенных государственных услуг, нуждается в тщательной и гарантированной системе безопасности своих личных сведений и персональных данных.

Несмотря на действующий сегодня федеральный закон, регламентирующий защиту персональных данных, на практике часто оказывается ситуация, свидетельствующая об утечке информации. Приведем подтверждающий пример из судебной практики. В данном примере речь идет о нарушении правил обработки и хранения персональных данных. ООО АНО ДПО «Учебный Центр Газ-Нефрть» было привлечено к административной ответственности по ст. 13.11 КоАП РФ за отсутствие письменного согласия Н.Г. Тряскиной и Ю.С. Зотовой на передачу их персональных данных

[1] Соловьева Е.С. Информационная безопасность в современном обществе // Наука. Практика. Право. – 2015. – № 5. – С. 12.

третьим лицам и их обработку. Таким образом, нарушен порядок сбора персональных данных Н.Г. Тряскиной и Ю.С. Зотовой, которые в обязательном порядке должны быть ознакомлены под роспись с Положением «О разграничении прав доступа к обрабатываемым персональным данным в АНО «Учебный Центр Газ-Нефрть», а также дать свое согласие на обработку персональных данных[1].

Ст. 17 ФЗ «О персональных данных» закреплено право субъекта персональных данных на обжалование действий или бездействия оператора в т.ч. на возмещение убытков и (или) компенсацию морального вреда в судебном порядке. Так, А. обратилась в суд с иском к ООО о взыскании компенсации морального вреда ввиду обработки персональных данных с нарушением требований закона. Судом было установлено, что А. неоднократно получала почтовые отправления от ООО с указанием о том, что выиграла приз, а также получала каталоги товаров, которые реализует ответчик, в поступающей корреспонденции содержались ее персональные данные - фамилия, имя, отчество, место регистрации и проживания, согласия на размещение указанных данных истец не давала. Разрешая заявленные требования, суд указал, что моральный вред истцу подлежит возмещению, поскольку доказательств ознакомления истца с Положением ответчика о порядке обработки персональных данных клиентов ООО, а также о согласии истца на обработку персональных данных ответчиком представлено не было[1].

По другому делу, судом было установлено, что государственное учреждение в нарушение требований ФЗ «О персональных данных» совершило действия, направленные на раскрытие полученных персональных данных истца неопределенному кругу лиц, путем размещения в общественном месте в качестве образца заявления о выдаче дубликата

[1] Апелляционное определение Московского городского суда от 04 марта 2017 г. по делу № 33-7084. – Режим доступа: http://sudact.ru/

[1] Апелляционное определение Московского городского суда от 10 августа 2017 г. по делу № 33-28318/2017. – Режим доступа: http://sudact.ru/

страхового свидетельства, содержащего персональные данные истца в открытом виде, без согласия последнего. Разрешая заявленные требования, суд первой инстанции, руководствуясь ст. 3, 7, 17, 24 ФЗ «О персональных данных», ст. 151, 1101 ГК РФ, установив факт размещения в общедоступном месте в качестве образца персональных данных истца, пришел к обоснованному выводу о частичном удовлетворении исковых требований, взыскав с ответчика компенсацию морального вреда[2].

На современном этапе развития информационного пространства угрозы информационной безопасности вызваны различными субъективными (индивидуальными) и объективными (общегосударственными) факторами.

Прежде всего, к таким факторам следует отнести недостаточность правового регулирования механизма защиты информации; слабую систему защиты информации со стороны негосударственных институтов; высокую коммерческую стоимость информации; недостаточность знаний в сфере информационной безопасности как населения, так и большинства сотрудников органов власти, их должностных лиц. Тем более, что в органах местного самоуправления недостаточная финансово-экономическая база для обеспечения информационной безопасности, профессиональной подготовки или переподготовки кадров в этой области. Зачастую, не хватает средств для приобретения компьютеров, создания информационных сетей. Развитие информационных систем по всему миру идет с ускоряющейся динамикой. Руководители государств объективно и научно подходят к вопросу о создании актуального эффективного механизма защиты информации.

Однако, и сегодня мы наблюдаем ситуацию, когда частные физические лица могут без особых усилий взломать систему охраны банковских организаций или становимся свидетелями «подрывной» деятельности так называемых хакеров в органах государственной власти. В связи с этим, ФСБ выдвинула инициативу, согласно которой компании, владеющие элементами

[2] Определение Ленинского районного суда г. Челябинска от 24 сентября 2017 г. по делу № 11-24/2017. – Режим доступа: http://sudact.ru/

критической инфраструктуры, также будут нести ответственность за ее защиту. Минэкономразвития РФ предложило создать резервную копию российского сегмента Интернета. По мнению должностных лиц Минэкономразвития, операторы связи должны подключиться к точкам обмена трафиком, которые зарегистрированы в государственном реестре. Такая процедура защитит российский участок в случае внезапного отключения от серверов, которые находятся в распоряжении и юрисдикции других стран, и позволит обеспечить передачу трафика внутри страны[1].

Обеспечение информационной безопасности предполагает объединение совместных усилий на всех уровнях власти: федеральном, региональном – органами государственной власти субъектов РФ, а также на муниципальном уровне – органами местного самоуправления. А также на корпоративном (или внутриорганизационном) уровне сами организации, заинтересованные в достаточно эффективной системе информационной безопасности и защите своих информационных интересов, информационных потоков и документальных, фактологических сведений, должны предусмотреть необходимую инфраструктуру, технические и технологические, материально-финансовые, юридические, программные ресурсы, в целом позволяющие наладить механизм защиты информации в целях обеспечения информационной безопасности конкретного предприятия, организации или учреждения.

Поэтому на внутриорганизационном уровне комплекс мер, направленных на защиту располагаемой информации и обеспечение безопасности, определяется значимостью и важностью получаемой, передаваемой, обрабатываемой и хранимой информации. Сегодня интенсивно развивающееся информационное пространство требует от современных предприятий и учреждений принятия технических и организационных мероприятий. В частности, грамотную установку и

[1] Михнев И.П., Михнева С.В., Сальникова Н.А. Информационная безопасность в Российской Федерации: современность и перспективы развития // Общество и право. – 2017. – № 3. – С. 59.

своевременное обновление информационного технического оборудования, антивирусов и специальных информационных дополнительных программ, используя предварительное их тестирование.

Также необходимо регулярно создавать резервные копии информации, закрывать доступ к портам компьютеров, через которые возможны попытки организации хакерских атак, размещать почтовый сервер организации на собственной аппаратной базе. Что касается внутреннего штата сотрудников, то им следует установить запрет на использование различных социальных сетей, мессенджеров и личных почтовых аккаунтов с рабочих терминалов, при одновременном ограничении их доступа к разделам информации в зависимости от должностного положения. При работе с информацией, имеющей особенно большую ценность, необходимо протоколирование всех действий сотрудников, от которых зависит возможность потенциальной угрозы целостности информации и нарушению режима ее конфиденциальности[1].

Итак, процесс информатизации является неотъемлемой частью современного информационного общества. Этот процесс порождает зависимость субъекта от глобального информационного пространства, которое, в свою очередь, связывает мир в единую общую систему. Государства в такой системе являются информационно взаимозависимыми, а сам субъект (общество или человек) ее неотъемлемая часть. Но процесс информатизации имеет и негативные последствия для общества, например, порождает опасности мирового уровня, связанные с обеспечением информационной безопасности (информационное оружие, информационная война и др.). Информационную безопасность в общем виде можно определить как невозможность нанесения вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой. Обеспечение информационной безопасности является

[1] Хомяков О.Г. Информационная безопасность как составляющая прав граждан Российской Федерации // Вестник Удмуртского университета. – 2014. – Вып. 3. – С. 93.

первоочередной задачей для современного общества. Это достаточно сложный и многофункциональный процесс, который зависит как от внешних, так и от внутренних факторов. Это объясняется тем, что на современном этапе развития общества информационные технологии приобретают все большую значимость в жизни не только отдельного человека, но и целого государства.

1.4 Становление и развитие института защиты государственной тайны в России

В механизме властвования государственная тайна считается одним из значительных элементов. Государственно-властные полномочия осуществляются в условиях государственной тайны. Фундаментальной функцией последней признается защита от распространения конкретной информации, государственная тайна имеет политический оттенок.

При этом, необходимо указать, что столь существенную роль в государственном механизме анализируемый вид тайны занимал не всегда.

В эпоху царской власти главенствующим был подход заключающийся в том, что власть царю дарована от Бога. В связи с этим, не было необходимости в отгораживании себя от других лиц государственной тайной. Сам аппарат государства на данном этапе являлся неразвитым[1].

Обратим внимание на то, что информации о том, каким образом обеспечивалась защита секретов государства на ранних этапах в исторических документах недостаточно. По данной причине рассмотрим более детально историю возникновению основного спутника государственной тайны – шифров. Как отмечается на доктринальном уровне к моменту возникновения Посольского приказа, осуществляющего общее

[1] Гатагонова Р.М. Становление и развитие института защиты государственной тайны в России // Бизнес в законе. – 2015. – № 5. – С. 116.

руководство внешней государственной политикой (1549 г.) относится появление в государстве первых специалистов-тайнописчиков.

Если учитывать, что дипломатия всегда тяготеет к приватности, тайнопись применяется для защиты секретной информации, то уже на данном этапе можно говорить о наличии в рассматриваемой сфере государственной деятельности соответствующих секретов, на данном этапе происходило развитие дипломатических шифров.

Если обратиться к историческим документам, то можно выявить, что в сфере государственной службы обеспечивалась защита государственных секретов, а лица, которыми государственные секреты разглашались – наказывались. Об этом сказано в Указе Петра I от 04 апреля 1714 г., в Генеральном регламенте 1720 г. В дальнейшем защита государственных секретов обеспечивалась нормами Указов российского Императора от 13 и от 16 января 1724 г., Приказа Правительствующего Сената от 05 марта 1724 г. В данных исторических документах был закреплен порядок допуска лиц к к секретным документам и обращения с ними. Законодательная база, регламентирующая защиту государственных секретов, на последующем этапе также получила свое развитие. Со стороны государства осуществлялся контроль за неукоснительным и точным соблюдением норм права. В своем Приказе от 30 апреля 1765 г. Правительствующий Сенат предусмотрел обязанность ставить пометку «секретно» на бумагу и конверты по соответствующей категории дел. В свою очередь, в другом Приказе от 07 января 1768 г. Правительствующий Сенат обратил внимание на допущенные некоторыми губерниями нарушения в части соблюдения действующего порядка к допуску к секретным делам и обязал данные губернии выплатить штраф за допущенные нарушения в сумме 10 рублей[1].

В письме П. Столыпина Государю от 02 августа 1906 г. № 991 речь шла о допущенном Российским телеграфным агентством, нарушении, которое

[1] Гильмуллина Д.А. Государственная тайна в правовом государстве // Известия Оренбургского государственного аграрного университета. – 2015. – № 9. – С. 17.

состояло в том, что произошло разглашение секретной информации о доставке на Амур 10 канонерских лодок и принятии мер по недопущению таких случаев, а также результаты проведенного расследования.

Применительно к дореволюционному историческому периоду, отметим, что в Уложении о наказаниях уголовных и исправительных 1845 г. можно встретить первое упоминание об уголовно-правовой защите государственных секретов. Раздел «О преступлениях государственных» был посвящен данным вопросам. В соответствующем разделе раскрывались такие виды государственных преступлений, как сообщение зарубежным властям секретов государства российскими подданными, государственная измена, умышленное во вред государству злоупотребление доверием дипломатическим или иным чиновником и др.

Более подробно и комплексно были раскрыты государственные преступления в главе «О государственной измене» Уголовного уложения 1903 г. В нормах данного документа были предусмотрены также виды наказаний за совершаемые преступления, самостоятельной статьей предусматривалась уголовная ответственность за «шпионаж». При этом, как таковой вышеуказанный термин в нормах Уложения предусмотрен не был, о нем можно говорить по совокупности отличительных признаков данного преступления[1].

05 июля 1912 г. был принят Закон «Об изменении действующих законов о государственной измене путем шпионства в мирное время», данным законом через категорию «шпионаж» было расширено понятие государственной измены, содержание некоторых статей Уголовного уложения данным законом также было изменено.

I мировой войной (1914 г.) были внесены коррективы в вопросы государственной защиты анализируемого вида тайны. В начале войны был принят первый закон, раскрывающий особенности военной цензуры. Три

[1] Гатагонова Р.М. Становление и развитие института защиты государственной тайны в России // Бизнес в законе. – 2015. – № 5. – С. 118.

перечня сведений, образующих военную тайну, были выведены к Закону от 05 июля 1912 г. в качестве приложений.

В принятом 10 июля 1914 г. Указе «Об утверждении Временного положения о военной цензуре» устанавливался просмотр корреспонденции, это было необходимо для обеспечения пресечения разглашения военной тайны, за всей печатной продукцией, которая выходила в военные годы также осуществлялся контроль.

Относительно истории возникновения и развития законодательства в рассматриваемой сфере, некоторыми учеными обозначаются три основных этапа.

1892 – 1912 г.г. – на данном этапе государство осуществляло борьбу со шпионажем. При этом, его опасность признавалось только применительно к военному времени, шпионаж анализировался как способ ведения боевых действий, возможности его реализации в мирное время не уделялось внимание.

Французский уголовный закон и немецкое уголовное уложение явились основой для формирования российского законодательства в анализируемой сфере.

1912 – 1914 г.г. – наиболее благоприятный этап для правоприменительной практики в сфере противодействия шпионажу. На данном этапе был разработан один из самых глубоких и проработанных законов в Европе, посвященный вопросам защиты государственных секретов. Также на данном этапе были сформированы армия, полиция, корпус жандармерии, то есть большой карательный аппарат. Последний осуществлял борьбу, в том числе, с внутренней оппозицией, отличался успехами в контрразведывательных операциях.

1914 – 1917 гг. – отставание от реалий жизни. В Законе от 05 июля 1912 г. необходимо было предусмотреть конкретные виды информации, которые признавались военной тайной.

Таким образом, развитие российского законодательства о защите государственной тайны, большей частью, охватывало военную сферу.

При этом, наличие государственных секретов было характерно и для других сфер, законодательное определение рассматриваемой категории в нормах отечественного права и законодательства не было закреплено.

Понятие «государственная тайна», а также механизм обеспечения ее защиты на государственном уровне не был предусмотрен в законодательных нормах Российской империи.

Административно-правовая система защиты секретов государства начала складываться в стране в советские годы, начиная с 1917 г. На законодательном уровне обеспечивалась защиты партийной и государственной тайны. Большая часть правовых источников государства находилась под грифом «секретно».

В результате формирования презумпции государственной секретности стала возникать следующая ситуация: те, кто хотел рассекретить или обнародовать определенную информацию должен был доказать нецелесообразность ограничений на ее распространение[1].

Вопросы отнесения информации к анализируемому виду тайны подлежали разрешению как на уровне секретных правительственных постановлений, так и на уровне законодательства.

В результате в 30-е г.г. XX века с каждым годом стало засекречиваться все больше информации.

Основными причинами засекречивания информации можно считать разрыв между словом и делом, между лозунгами и реальностью, в существовавшей в стране ситуации в политической и экономической сферах, шпиономания, а также формирование такого механизма государственных органов, в котором одним из основных элементов является секретность.

---

[1] Гурлеев И.В., Курочкин С.А. Организационно-правовые основы защиты государственной тайны в первые годы Советской власти // Власть. – 2014. – № 11. – С. 12.

Отдельно необходимо отметить, что в исторически сложных условиях происходило формирование в советские годы система защиты государственной тайны. Данная система, по сути, возникла во времена обострения классовой борьбы, в годы Великой Отечественной войны и «холодной войны» только укрепилась.

Вопросы государственной тайны были регламентированы на уровне правовых источников подзаконного уровня, это было удобно, так как позволяло производить в необходимую сторону маневры в данных вопросах.

Так, достаточно сжатым можно признать утвержденный Постановлением Совета Министров СССР от 10 июня 1947 г. Перечень сведений, составляющих государственную тайну, разглашение которых законодательно преследуется.

Информация военного характера, в частности, организация, численность, боеспособность войск, в вышеуказанном перечне была первой закреплена. При этом, уровень засекречивания, в частности, информации о численности войск, их дислокации, начинался с отдельного подразделения.

В итоге заскречивание такого большого объема информации повлекло за собой огромные расходы. При этом, открытый характер изложенного выше перечня следует считать основным недостатком Перечня 1947 г., это приводило к тому, что к государственной тайне Советом Министров СССР могла быть отнесена и иная информация.

Продолжительное время объективному критическому анализу и публичному рассмотрению не подлежали вопросы, связанные с системой защиты государственной тайны: принципы формирования и функционирования данной системы, основные цели, формы, пропорции между положительными результатами и расходами на обеспечение сохранности анализируемого вида тайны и др. Это привело к тому, что произошло отчуждение общественных интересов от института секретности.

Итак, со времен Петра I можно вести отчет в истории организации в стране защиты государственной тайны. Современный порядок обращения с

секретными документами является прообразом системы обеспечения государственных секретов в истории страны. При этом, институт защиты государственной тайны и в настоящее время характеризуется наличием отдельных нерешенных проблем, пробелов в правовом регулировании.

2 ПРАВООХРАНИТЕЛЬНЫЕ ОРГАНЫ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

2.1 Правоохранительные органы как субъекты обеспечения информационной безопасности

Государство признается основным субъектом обеспечения безопасности, в данной сфере государство через систему органов трех ветвей власти реализует соответствующие функции. Для обеспечения безопасности на государственном уровне реализуется политика, в системе исполнительных органов власти формируются органы обеспечения безопасности, разрабатываются и принимаются определенные законодательные нормы (нормы права). Государственные органы федерального и регионального уровня, в которых государственная служба должностных лиц, обладающих полномочиями в сфере обеспечения безопасности, являются органами обеспечения информационной безопасности[1].

Как нами ранее отмечалось, конституционно-правовые нормы и нормы ФЗ «О безопасности» составляют нормативно-правовую базу обеспечения безопасности.

В научной среде обращается внимание на то, что закон, закрепляя в качестве субъектов обеспечения государственной безопасности, государственные органы власти, четко не формулирует соотношение категорий «государство», «исполнительные органы власти», «государственные органы обеспечения безопасности», «государственные организации и объединения». Так, в некоторых статьях указывается формирование органов обеспечения безопасности, основные направления деятельности государственных органов в сфере безопасности, механизм контроля за данными направлениями деятельности (ч. 2 ст. 4); в некоторых

[1] Абубекерова Д.А. Система органов обеспечения безопасности в Российской Федерации // Наука. Общество. Государство. – 2016. – № 4(16). – С. 89.

статьях отмечается, что для фактической реализации функций по обеспечению безопасности государства, общества, личности в системе исполнительной власти формируются определенные органы государственной власти; органы государственной власти всех трех ветвей в совокупности образуют систему безопасности; силы и средства обеспечения безопасности, включая «службы» исполнительных органов власти входят в систему безопасности.

Различными являются методы и формы деятельности, а также степень участия, предусмотренных в ФЗ «О безопасности» государственных органов власти, в решении вопросов безопасности РФ.

Специальными полномочиями в рассматриваемой сфере наделены некоторые органы государственной власти (МВД, ФСБ), для выполнения данной задачи вышеуказанным органам разрешено иметь специальные силы и средства (ст. 12).

Правоохранительные органы являются самостоятельным субъектом обеспечения информационной безопасности.

Правоохранительный орган – специально учрежденный государственный орган, целью деятельности которого является создание условий обеспечения законности и правопорядка посредством решения закрепленных за ним задач и выполнения одной или нескольких специфичных функций по охране и защите прав, свобод и законных интересов граждан и организаций[1].

Остановимся более детально на отдельных видах правоохранительных органов, как субъектах обеспечения информационной безопасности.

Обеспечение безопасности реализуется следующими федеральными специальными службами: Федеральная служба безопасности (ФСБ России), Служба внешней разведки (СВР России), Федеральная служба охраны (ФСО России), Государственная фельдъегерская служба (ГФС России).

[1] Зуев В.И. Правоохранительная деятельность как функция правового государства // Инновационная наука. – 2017. – № 5. – С. 112.

ФСБ России является единой централизованной системой органов ФСБ, задача которой состоит в обеспечении безопасности РФ, реализующей свои полномочия в целях решения данной задачи. Об этом сказано в ФЗ от 03 апреля 1995 г. № 40-ФЗ «О Федеральной службе безопасности»[1].

Положение о ФСБ России и структура органов ФСБ предусмотрены на подзаконном уровне, Указом Президента РФ от 11 августа 2003 г. № 960. Во главе данной службы находится, назначаемый и освобождаемый от должности главой государства, директор ФСБ России.

ФСБ России осуществляет ключевые направления деятельности органов ФСБ, в рамках своих полномочий издает нормативные акты, на местах формирует свои территориальные органы, обеспечивает организацию их деятельности.

Борьба с терроризмом, с преступностью, пограничная, разведывательная и контрразведывательная деятельность, обеспечение информационной безопасности: все изложенное выше ст. 8 ФЗ «О Федеральной службе безопасности» признается в качестве основных направлений деятельности органов ФСБ.

Внешняя разведка в соответствии со ст. 1 ФЗ от 10 января 1996 г. № 5-ФЗ «О внешней разведке» представляет собой систему органов внешней разведки РФ, специально формируемых государством органов, признается составной частью сил обеспечения безопасности РФ, обеспечивающая защиту безопасности государства, общества и личности от внешних угроз с применением средств и методов, предусмотренных законом[2].

В качестве основных целей разведывательной деятельности ст. 5 вышеуказанного закона обозначены:

— обеспечение главы государства, высшего законодательного и исполнительного органа власти, необходимой им для принятия решений в

[1] Федеральный закон «О Федеральной службе безопасности» от 03 апреля 1995 г. № 40-ФЗ // Российская газета. – 1995. – 15 апреля.

[2] Федеральный закон «О внешней разведке» от 10 января 1996 г. № 5-ФЗ // Российская газета. – 1996. – 22 января.

различных сферах (экономика, политика, оборона, экология и др.), разведывательной информацией;

— содействие военно-техническому обеспечению безопасности РФ, экономическому развитию, научно-техническому прогрессу государства;

— обеспечение условий, способствующих эффективному осуществлению государственной политики в сфере безопасности.

В рамках реализации своих полномочий разведывательная деятельность реализуется:

— в сфере экономики, политики, экологии, а также научно-технической и военностратегической сферах, в сфере обеспечения безопасности учреждений РФ, находящихся за границами российской территории, и командированных за границы российской территории граждан РФ, у которых ввиду реализуемой деятельности имеется допуск к информации, составляющей государственную тайну, в сфере засекреченной, шифрованной и других видов специальной связи с применением за границами российской территории радиоэлектронных средств и методов – Службой внешней разведки РФ;

— в военной, военно-технической, -политической, -экономической и экологической сферах – органом внешней разведки Министерства обороны РФ.

В свою очередь, исполнительным органом власти федерального уровня в сфере фельдъегерской связи, действующим в интересах всех трех ветвей государственной власти, включая и интересы государства в целом, выступающим составной частью сил и средств обеспечения безопасности РФ, обеспечивается федеральная фельдъегерская связь в РФ. Об этом сказано в ст. 1 ФЗ от 17 декабря 1994 г. № 67-ФЗ «О федеральной фельдъегерской связи»[1].

[1] Федеральный закон «О федеральной фельдъегерской связи» от 17 декабря 1994 г. № 67-ФЗ // Российская газета. – 1994. – 29 декабря.

Государственная фельдъегерская служба России (ГФС) является специальным органом, реализующим вышеуказанные функции, глава государства осуществляет руководство деятельностью данной службы.

Федеральная таможенная служба также является видом правоохранительных органов, обеспечивающих информационную безопасность.

К силам обеспечения национальной безопасности относятся, в том числе, и таможенные органы. По своему административно-правовому статусу данные органы признаются правоохранительными и военизированными структурами.

Участие таможенных органов в обеспечении безопасности повышается с каждым годом, это во многом связано с международными и внутригосударственными экономическими и политическими проблемами, с возникновением новых рисков и угроз для развития государства, общества и личности, а также с формирующейся геополитической ситуацией[1].

Обеспечение защиты конституционного строя РФ, осуществление правосудия по делам о преступлениях, посягающих на информационную безопасность, обеспечение судебной защиты граждан и юридических лиц: все вышеизложенное относится к основным задачам судебных органов, как вида правоохранительных органов.

Органы прокуратуры также занимают важное место в системе органов государственной власти, обеспечивающих безопасность РФ, включая и информационную безопасность. Органы прокуратуры реализуют надзор за исполнением норм действующего законодательства, прав и свобод личности со стороны государственных органов и местных органов власти, кроме того, координируют деятельность правоохранительных структур по борьбе с преступностью. Отметим, что также могут формироваться федеральные комиссии, выступающие координационными органами, для обеспечения

[1] Воронов А.М. Таможенные органы как субъекты обеспечения безопаности государства // Вестник Московского университета МВД России. – 2015. – № 1. – С. 242.

взаимодействия субъектов, реализующих борьбу с наиболее опасными угрозами государственной безопасности.

Органы внутренних дел, как правоохранительные органы, также являются субъектами обеспечения информационной безопасности. ОВД в рамках реализации возложенных на них полномочий, осуществляют предупреждение, расследование и раскрытие преступлений в информационной сфере. Кроме того, отметим, что ОВД в ходе реализации своих полномочий и функций осуществляют обработку информации, составляющей государственную тайну, персональных данных, оперативной и служебной информации. В 2012 г. была разработана Концепция обеспечения информационной безопасности органов внутренних дел РФ до 2020 г., данный документ был подготовлен для формирования единой политики в сфере обеспечения информационной безопасности. Вышеуказанная Концепция имеет стратегическое значение и применительно к анализируемой сфере, признается основным нормативным документом. Цели, задачи, принципы, основные направления обеспечения информационной безопасности ОВД – данные положения закреплены в нормах Концепции. Также на уровне рассматриваемого документа предусмотрена система мер по защите информации, информационных ресурсов и информационных систем ОВД, которые осуществляются организационно-правовыми, инженерно-техническими, научными, ресурсными и кадровыми мероприятиями.

Достижение требуемого уровня защиты от специальных программно-технических воздействий, технических средств разведки, несанкционированного доступа, а также утечки информации по техническим каналам, в соответствии с вышеуказанной Концепцией, признается в качестве основной цели обеспечения информационной безопасности[1].

По причине повсеместного и активного перехода информационных технологий на автоматизированную основу без применения традиционных

[1] Костюченко К.Л. Новые акценты в обеспечении информационной безопасности органов внутренних дел // Вестник Уральского юридического института МВД России. – 2015. – № 4. – С. 30.

бумажных носителей информации во всех областях деятельности ОВД все более сложной и практически значимой становится проблема обеспечения информационной безопасности.

Обеспечение информационной безопасности в ОВД на сегодняшний день признается необходимым направлением деятельности и подразумевает формирование комплексной системы защиты информации, содержащей в себе ряд средств и методов защиты информации (организационные, правовые, криптографические, инженерно-технические и др.) [1].

На наш взгляд, в ОВД необходимо создавать специализированные службы безопасности и защиты информации. Это позволит в целом повысить уровень защиты ОВД, а также существенно уменьшить вероятность появления угроз, которые могут привести к уничтожению, потере, модификации информации.

Совет безопасности относится к государственным органам власти, специально сформированным для обеспечения защиты безопасности государства.

Данный орган рассматривает стратегические проблемы внешней, внутренней и военной политики РФ, координирует деятельность системы обеспечения безопасности РФ по разработке стратегии в области внутренней, внешней и военной политики, информационной безопасности и военно-технического сотрудничества. Также рассматривает вопросы обеспечения безопасности в экономической, общественной, оборонной, пограничной, информационной, экологической и иных сферах, вопросы охраны здоровья населения, прогнозирования и предотвращения межнациональных и социальных конфликтов, чрезвычайных ситуаций и преодоления их последствий, обеспечения общественного согласия, законности и правопорядка. Осуществляет подготовку предложений и рекомендаций по реализации стратегии и текущей политики обеспечения национальной

[1] Козьминых С.И. Моделирование систем и процессов обеспечения информационной безопасности в органах внутренних дел // Вестник Московского университета МВД России. – 2016. – № 2. – С. 161.

безопасности, по разработке Концепции национальной безопасности. Таким образом, Совет безопасности РФ является конституционно учрежденным органом, реализующим подготовку решений главы государства по вопросам реализации единой политики государства в сфере обеспечения безопасности, по вопросам обеспечения защищенности жизненно важных интересов государства, общества, личности от внешних и внутренних угроз[1].

Итак, одним из субъектов обеспечения информационной безопасности являются правоохранительные органы. К правоохранительным органам, осуществляющим обеспечение информационной безопасности, относятся: МВД России, ФСБ России, ФТС России, СВР России, ФСО России, органы прокуратуры, судебные органы и др.

2.2 Основные направления деятельности правоохранительных органов по обеспечению информационной безопасности

В настоящее время достаточно сложным является решение задачи по обеспечению необходимого уровня информационной безопасности. Решение данной задачи происходит одновременно на государственной уровне, внутриорганизационном уровне и уровне отдельных лиц.

Степенью значимости обрабатываемой информации обуславливается вклад различных участников в данный процесс.

Обеспечение абсолютной информационной безопасности не может осуществляться только силами государства. При этом, на государственном уровне реализуется перечень профилактических мероприятий и обеспечивается юридическая поддержка. ФСБ был разработан законопроект, в соответствии с которым организации должны нести ответственность за

[1] Гавриленко А.А. Понятие и система правоохранительных органов // Общество и право. – 2016. – № 7. – С. 94.

защиту критической инфраструктуры, если они владеют элементами данной инфраструктуры.

Минэкономразвития в январе 2017 г. выступило с предложением образовать резервную копию отечественного сегмента Интернета. Как отмечается в министерстве, операторы связи должны подключиться к точкам обмена трафиком, которые зарегистрированы в госреестре. Данная мера защитит отечественный сегмент в случае непредвиденного отключения от серверов, которые находятся в юрисдикции зарубежных государств и позволит обеспечить передачу трафика внутри государства[1].

Правоохранительные органы в рамках обеспечения информационной безопасности реализуют следующие мероприятия:

— профилактика и предупреждение преступлений, посягающих на информационную безопасность;

— расследование и раскрытие преступлений, посягающих на информационную безопасность;

— осуществление правосудия по делам о преступлениях, посягающих на информационную безопасность.

Рассмотрим данные направления деятельности правоохранительных органов более подробно.

Профилактика преступлений, посягающих на информационную безопасность, представляет собой деятельность, направленную на выявление и устранение причин, порождающих анализируемые преступления, и условий, способствующих их совершению.

К основным задачам превенции данного вида преступности относится выработка и реализация комплекса мер, направленных на предотвращение:

— преступных посягательств на основы конституционного строя, общественную безопасность и общественный порядок в РФ;

[1] Сипок Р.П. Система органов государственной власти, обеспечивающих государственную безопасность Российской Федерации // Армия и общество. – 2014. – № 11. – С. 93.

— угроз информационной безопасности личности, общества, государства, то есть обеспечение возможности безопасного создания, хранения, обработки и передачи вышеуказанными субъектами права не запрещенной законом компьютерной информации;

— несанкционированных действий, направленных на уничтожение, блокирование, модификацию, копирование компьютерной информации или нейтрализацию средств защиты компьютерной информации физических и юридических лиц, либо угрозы причинения указанных последствий;

— противоправных действий, направленных на нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям;

— угроз информационной безопасности коммерческих и некоммерческих организаций, государственных (муниципальных) органов власти, предприятий и учреждений, связанных с обеспечением режима тайны конфиденциальной информации (персональных данных и информации частного характера, сведений, представляющих государственную, служебную, профессиональную, коммерческую и иную тайну);

— несанкционированных действий, направленных на нарушение работы средств защиты, хранения, обработки и передачи компьютерной информации на военных, стратегических и социально значимых объектах (транспортных, промышленных, энергетических, научных, здравоохранительных, образовательных и др.);

— нарушения конституционных прав граждан на свободный поиск, получение, передачу, производство и распространение информации любым

законным способом, неприкосновенность частной жизни, личной и семейной тайны, собственности и др.[1]

Преступные группы и сообщества на сегодняшний день применяют в своей деятельности достижения науки в сфере кибернетики, а также современную компьютерную технику и информационные технологии. Развитие последних привело к появлению в РФ компьютерных преступлений – нового вида преступлений, связанных с применением компьютерных и информационных технологий.

Можно выделить две основные группы предупреждения преступлений, посягающих на информационную безопасность:

— организационно-технические содержат в себе предотвращение утраты, хищения, утечки, искажения и подделки информации, сохранение государственной тайны, предотвращение угроз безопасности государству, обществу и личности;

— правовые меры предоставляют юридическое определение ключевых элементов информационной технологии как объектов правовой охраны, предусматривают права и обязанности собственника на данные объекты, закрепляют уголовную ответственность за преступления в информационной сфере.

На сегодняшний день полноценная профилактика преступлений, посягающих на информационную безопасность, не может проводиться в достаточной степени во многом по причине небольшого объема финансирования, выделяемого на борьбу в анализируемым видом преступности.

Кроме того, отметим, что для расследования преступлений в сфере информационной безопасности правоохранительные органы не располагают необходимой программной и информационно-технической базой. При

[1] Решняк М.Г., Павлова Д.А. О некоторых особенностях раскрытия преступлений в сфере высоких информационных технологий // Экономико-юридический журнал. – 2015. – № 5. – С. 123.

выявлении факта совершения анализируемого преступления, все структуры правоохранительных органов действуют по-разному.

Значительная часть преступлений, посягающих на информационную безопасность остается нераскрытой во многом из-за отсутствия строгого алгоритма взаимодействия подразделений полиции и иных органов. Также следует отметить, что для осуществления эффективного предупреждения и расследования преступлений, посягающих на информационную безопасность, кадровый состав прокуратуры, суда, полиции не имеет достаточного уровня подготовки[1].

В нашей стране действует единая система учета совершенных преступлений, при этом, она не отвечает специфике совершения преступлений в сфере информационной безопасности. Кроме того, отметим, что от действий преступных элементов недостаточно защищены технологии и средства информации.

На международном уровне внедрены единые системы безопасности, приняты соответствующие законы, позволяющие специалистам проводить качественную работу по профилактике преступлений, посягающих на информационную безопасность, успешно расследовать преступления данной категории, для защиты государственных и гражданских интересов отслеживать преступные действия. По нашему мнению, современная система профилактики преступлений, посягающих на информационную безопасность, нуждается в совершенствовании. В числе первоочередных мероприятий выделим следующие:

— разработка и практическая реализация проекта, закрепляющего постоянное функционирование и отслеживание потоков компьютерной информации. Посредством определенных алгоритмов данная система могла бы производить обнаружение попыток совершения преступлений, кроме того, за указанная система могла бы за активными элементами, которые

[1] Костюченко К.Л. Новые акценты в обеспечении информационной безопасности органов внутренних дел // Вестник Уральского юридического института МВД России. – 2015. – № 4. – С. 30.

ведут подозрительную деятельность устанавливать слежение. Для профилактики анализируемых преступлений изложенная выше система также была бы эффективной[1];

— по причине того, что преступления, посягающие на информационную безопасность, совершаются, в том числе, и преступными элементами, находящимися в других государствах, существует необходимость в подготовке и внедрении стандартов, регламентирующих и координирующих порядок взаимодействия отечественных правоохранительных структур и органов зарубежных государств;

— по причине того, что не только полиция и иные правоохранительные органы осуществляют обеспечение информационной безопасности, но также и хранители, носители, владельцы информации, следует упорядочить порядок взаимодействия между банками, социальными фондами, владельцами серверов. Координированные действия заинтересованных в обеспечении информационной безопасности структур позволили бы проводить профилактику преступлений, отслеживать действия подозрительных лиц и эффективно взаимодействовать при обнаружении признаков совершения преступления.

Кроме того, требуется наделить полномочиями в сфере обеспечения компьютерной безопасности лиц, прошедших квалифицированную подготовку. В настоящее время этой работой занимается до 70% специалистов, которые слабо разбираются в специфике распространения компьютерной информации. Это недопустимо для эффективной работы специальных подразделений в сфере обеспечения компьютерной безопасности.

Для эффективного расследования таких преступлений необходимо разработать единую тактику и стратегию. К данной работе следует привлекать высококвалифицированных специалистов. При осуществлении

[1] Синьков Д.А. Повышение эффективности расследования преступлений в сфере компьютерной информации // Современные научные исследования и инновации. – 2017. – № 8. – С. 38.

агентурной работы следует пересмотреть качественный состав субъектов, с целью установления конфиденциального и эффективного сотрудничества.

В арсенал оперативной техники следует включить современные технические приборы и устройства (компьютеры и программное обеспечение). Для личного состава правоохранительных структур необходимо предусмотреть разработку и принятие программ подготовки. С целью выполнения долгосрочной стратегии следует предусмотреть возможности для организации переподготовки специалистов в сфере обеспечения информационной безопасности.

Данными программами должна преследоваться не только качественная теоретическая подготовка специалистов, но и практическая работа по освоению современной компьютерной техники и программных средств. Без соблюдения этих требований результаты оперативно-розыскной деятельности по фактам преступлений в сфере информационной безопасности останутся неудовлетворительными[1].

При выявлении, раскрытии и расследовании преступлений в сфере информационной безопасности используется комплекс оперативно-розыскных мероприятий и следственных действий.

Особую сложность представляет процедура обнаружения, фиксации и изъятии компьютерной информации. Потому для обнаружения данных следов на ряду с традиционными оперативно-разыскными мероприятиями используются и специальные по данной категории преступлений, которые «представляют собой совокупность действий по перехвату и исследованию данных трафика, установление логов веб - и мейл-серверов, системных логов, доменов, принадлежности адреса электронной почты, исследование кейлогеров».

Значительное место в деятельности по выявлению, раскрытию и расследованию данной категории преступлений занимает производство

[1] Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – № 10. – С. 16.

судебных экспертиз, в числе основных судебная компьютерно-техническая, где происходит анализ «цифровых следов».

Судебные органы, как субъекты обеспечения информационной безопасности, осуществляют правосудие по рассматриваемой категории уголовных дел, применяют наказание, как меру борьбы с информационной преступностью, которое предусмотрено уголовным законом.

Так, по одному уголовному делу была осуждена бывший главный эксперт межрегиональной инспекции Главной инспекции ЦБ РФ, признанная виновной в незаконном разглашении сведений, составляющих коммерческую и банковскую тайну, которые стали известны ей по работе (ч. 2 ст. 183 УК РФ). Было установлено, что в 2018 г. рабочей группой указанной инспекции, в состав которой входила осуждённая, проводились проверки одного из банков г. Кирова, в ходе которых ей стали известны сведения, относящиеся к коммерческой и банковской тайне данной организации, включая информацию о клиентах, их расчетных счетах и размерах кредитных обязательств, активах и др. После этого она сообщила соответствующие конфиденциальные сведения представителю другого банка[1].

Как следует из другого примера, приговором Гагаринского районного суда г. Москвы от 10 июня 2017 г. по делу № 1-160/2017 Т. был осужден за разглашение сведений, составляющих коммерческую тайну. Т., будучи начальником отдела продаж ЗАО «ФосАгро АГ», более года в нарушение действующих в данной организации «Общих правил использования информационных ресурсов» собирал сведения, относящиеся к коммерческой тайне, без разрешения их владельца – данного акционерного общества, посредством «хищения информации», содержащей коммерческую тайну, с электронной почты начальника его Управления. Он незаконно осуществлял копирование данных сведений и последующую их отправку через корпоративную сеть на свой личный почтовый ящик. В дальнейшем Т.

[1] В Кирове банковский работник признан виновным в разглашении коммерческой и банковской тайны. – Режим доступа: http:// news.kipov.ru/accidents/v_kirove_bankovskiy_ rabotnik_priznan_vinovnym. (дата обращения: 21.03.2019)

разгласил сведения, составляющие коммерческую тайну ПАО «ФосАгро АГ», полученные им незаконным способом, а также сведения, ставшие ему известными в силу выполнения служебных обязанностей, без согласия их владельца. Эти сведения он неоднократно направлял по электронной почте представителю конкурирующей иностранной организации, использовавшей полученную информацию для получения преимуществ в торговой деятельности с указанным ПАО[1].

Итак, в числе основных направлений деятельности, реализуемых правоохранительными органами в рамках обеспечения информационной безопасности, можно выделить следующие: профилактика и предупреждение преступлений, посягающих на информационную безопасность; расследование и раскрытие преступлений, посягающих на информационную безопасность; осуществление правосудия по делам о преступлениях, посягающих на информационную безопасность.

2.3 Взаимодействие правоохранительных органов в процессе обеспечения информационной безопасности

Быстрое и полное установление всех обстоятельств совершенного преступления, привлечение виновных к уголовной ответственности невозможно без слаженной и согласованной работы участников уголовного судопроизводства. Взаимодействиевуголовном судопроизводстве – это часть тактики, уровень связи между следственными и иными действиями и их субъектами.

В широком смысле под таким взаимодействием понимают деловой контакт, совместную работу в борьбе с преступностью, в узком –

[1] Приговор Гагаринского районного суда г. Москвы от 10 июня 2017 г. по делу № 1-160/2017. – Режим доступа: http://sudact.ru/

согласованную, основанную на законе деятельность административно независимых друг от друга органов по конкретному уголовному делу.

Принципами взаимодействия являются: законность, комплексное использование сил и средств, персональная ответственность исполнителей, непрерывность и согласованность[1].

В связи с тем, что информационная сфера имеет глобальный характер, для проведения расследования случаев противоправных действия необходимо тесное сотрудничество всех правоохранительных органов. Всестороннее расследование помогает выяснять обстоятельства преступления и его составляющую, выявить местонахождение преступных лиц, обеспечить полноту и скорость оперативно-следственных мероприятий по розыску и поимки преступников. Выявление и изобличение лиц, причастных к совершению преступлений в информационной сфере, имеет ряд существенных особенностей, знание которых необходимо для сотрудников правоохранительных органов.

Взаимодействие в ходе расследования преступлений с оперативными сотрудниками органов дознания характеризуется принципом непрерывности – от возбуждения уголовного дела до момента его рассмотрения в суде – и заключается в том, что следователь и оперативники при производстве по уголовному делу согласовывают цели, место работы, время, такое взаимодействие является двухсторонним и строится на взаимной основе.

Необходимо отметить, что взаимодействие следователя и оперативных сотрудников органа дознания в ходе расследования преступлений, в частности на первоначальном этапе, может осуществляться в процессуальной форме (рассмотрение сообщений о преступлениях, работа на месте происшествия, выполнение неотложных следственных действий, поручений и др.) и в непроцессуальной (организационной) форме (согласованное планирование, создание следственно-оперативных групп и др.). Учитывая

[1] Введенская О.Ю. Взаимодействие следователя с оперативными сотрудниками органа дознания при расследовании интернет-преступлений // Общество и право. – 2016. – № 1(55). – С. 204.

общность и специфику задач, стоящих перед следователями и оперативными сотрудниками органов дознания при расследовании преступлений, посягающих на информационную безопасность, следует подчеркнуть тесную связь уголовно-процессуальной и оперативно-розыскной деятельности, определяющую необходимость теснейшего взаимодействия[1].

Несмотря на единство целей и целого ряда общих черт, органы предварительного следствия и оперативные подразделения органов дознания имеют существенные различия, которые связаны с тем, что деятельность следователя носит строго процессуальный характер, а оперативные службы уполномочены использовать с целью раскрытия преступлений не только процессуальные, но и оперативно-розыскные меры. Необходимо не только уметь отличать такие меры, но и знать формы и методы их сочетания, поскольку отрыв следственных и оперативных действий друг от друга зачастую является основной причиной некачественного расследования дела.

Наиболее эффективно такое взаимодействие осуществляется в ходе: совместного планирования следственных действий и оперативно-розыскных мероприятий; взаимного обмена полученной информацией; совместного анализа и оценки полученной информации; оперативного сопровождения расследования; совместной работы в составе СОГ; выдвижения и проверки версий; совместной работы на месте происшествия; при производстве следственных действий; проведения тактических операций (комбинаций); реализации материалов дел оперативного учета.

В научной среде условиями эффективности взаимодействия следователя с сотрудниками оперативных подразделений при расследовании преступлений, посягающих на информационную безопасность, признаются следующие: целеустремленность (четкое обозначение цели и неуклонное следование к ней, единство целей); конкретность (доступное и точное изложение поставленной задачи); обязательность (все законные требования

[1] Введенская О.Ю. Взаимодействие следователя с оперативными сотрудниками органа дознания при расследовании интернет-преступлений // Общество и право. – 2016. – № 1(55). – С. 206.

следователя должны выполняться); взаимную ответственность; профессионализм (как следователя, так и сотрудников органов дознания); общие принципы (законность, компетентность, плановость, динамичность и др).

Чем раньше возникнет такое взаимодействие, тем больший успех может быть достигнут, так как следователь лучше, чем оперативник, может определить наличие или отсутствие в оперативных материалах законных поводов и достаточных оснований для возбуждения уголовного дела.

На этапе принятия решения о возбуждении уголовного дела взаимодействие следователя с оперативниками органа дознания происходит в форме передачи и оценки оперативных материалов, совместного составления плана согласованных следственных действий и оперативно-розыскных мероприятий. В таком согласованном плане, скрепленном письменной резолюцией начальника ОВД, последний делегирует подчиненному сотруднику осуществление уголовно-процессуальных и непроцессуальных обязанностей, определяя конкретных субъектов взаимодействия[1].

Отметим, что значительную долю преступлений, посягающих на информационную безопасность, составляют интернет-преступления. Согласованные действия следователя и оперативных сотрудников органа дознания, осуществляемые в рамках взаимодействия по вышеуказанной категории дел, проводимые в условиях неочевидности, включают в себя: установление пути преступника, включающего в себя всех транзитных провайдеров, с присваемыми ими IP-адресами, как путем процессуальных и следственных действий, так и посредством проведения соответствующих оперативно-розыскных мероприятий; взаимный обмен полученной информацией; проведение оперативным работником оперативно-розыскных мероприятий, направленных на обеспечение розыскной деятельности следователя (установление свидетелей, мест для проведения обысков и

[1] Потапов С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации // Социально-экономические явления и процессы. – 2016. – № 10. – С. 16.

выемок и др.); совместную разработку и проведение тактических комбинаций (операций), направленных на фиксацию доказательственной базы и розыск преступника, а при его обнаружении – организацию внезапного задержания[1]. Если установлен подозреваемый, то действия следователя и оперативного работника направлены на установление и процессуальную фиксацию доказательств его вины. Здесь следует отметить совместное внезапное задержание подозреваемого, избрание меры пресечения, поиск путем проведения оперативно-розыскных мероприятий доказательств вины задержанного в совершении преступления и их реализацию путем проведения следственных действий, выполнение поручений следователя, организацию сбора общими усилиями материалов, характеризующих личность подозреваемого, и иные действия согласно ранее разработанному плану.

Несмотря на то, что закон не содержит перечень следственных действий, которые могут быть проведены оперуполномоченными по поручению следователя, необходимо учитывать персональную ответственность следователя за исход процесса расследования, а также необходимость оценки уровня подготовки в данной сфере оперативных сотрудников органа дознания, которым будет поручено их проведение. По общему негласному правилу следователь поручает органу дознания проведение следственных действий, носящих неотложный характер, незамедлительность получения результатов которых имеет влияние на процесс предварительного расследования.

Необходимым условием повышения эффективности борьбы с преступлениями, посягающими на информационную безопасность, должно быть привлечение к расследованию данной категории преступлений специалистов в различных областях знаний.

---

[1] Введенская О.Ю. Взаимодействие следователя с оперативными сотрудниками органа дознания при расследовании интернет-преступлений // Общество и право. – 2016. – № 1(55). – С. 208.

При расследовании преступлений, посягающих на информационную безопасность, у следователя, как правило, возникает необходимость в привлечении к расследованию специалиста.

Применение специальных знаний при расследовании преступлений – одно из важнейших направлений повышения эффективности расследования, так как значительно расширяет содержание доказывания, увеличивая в первую очередь качество, а также количество фактических данных, используемых в доказывании по уголовному делу[1].

Процессуальный статус следователя не лишает его права самостоятельно применять криминалистическую технику при производстве тех или иных следственных действий. Однако, на практике следователи предпочитают обращаться за помощью к специалисту.

В ходе оказания криминалистической помощи осуществляется обнаружение, фиксация и изъятие следов и объектов, несущих на себе криминалистически значимую информацию. Получение данной информации необходимо для ее дальнейшего экспертного исследования, а также выдвижения и проверки версий. Как правило, такая помощь специалиста необходима при проведении следственных осмотров документов и при проведении обыска, выемки.

Нередки случаи, когда в ходе обыска в компьютере у обыскиваемых обнаруживаются базы данных на владельцев кредитных карточек, номера расчетных счетов и сведения о движении денежных средств коммерческих фирм, иные важные для следствия данные, находящиеся в памяти компьютера или на дискетах. Следователь может не знать всех нюансов работы с базами данных. Поэтому рекомендуется в случае обыска в помещениях, где имеются компьютеры, приглашать специалистов-программистов, системщиков. Сведущее лицо сможет проверить

[1] Решняк М.Г., Павлова Д.А. О некоторых особенностях раскрытия преступлений в сфере высоких информационных технологий // Экономико-юридический журнал. – 2015. – № 5. – С. 123.

информацию на винчестере, дискетах, обратить внимание следователя на «запаролированные» файлы[1].

Если в ходе обыска доступ к компьютерной информации затруднен, следователю не стоит пытаться преодолеть на месте установленную программную защиту. Компьютерное оборудование должно быть изъято и направлено на компьютерно-техническую экспертизу. В ходе расследования преступлений, посягающих на информационную безопасность, следователь осуществляет взаимодействие также с экспертами. По делам анализируемой категории наиболее часто назначаются судебные компьютерно-технические экспертизы, которые подразделяются на четыре вида:

— судебная аппаратно-компьютерная экспертиза, заключающаяся в проведении исследования: технических (аппаратных) средств компьютерной системы: персональных компьютеров; периферийных устройств, сетевых аппаратных средств (серверы, рабочие станции, активное оборудование, сетевые кабели и др.); интегрированных систем (органайзеры, пейджеры, мобильные телефоны и др.); встроенных систем (иммобилайзеры, транспондеры, круиз- контроллеры и др.); любых комплектующих всех указанных компонентов (аппаратные блоки, платы расширения, микросхемы и др.).

При этом решаются задачи: классификации и определения свойств аппаратного средства; выяснения фактического и первоначального состояния; диагностики технологии изготовления, причин и условий изменения свойств (эксплуатационных режимов); определения структуры механизма и обстоятельства события за счет использования выявленных аппаратных средств как по отдельности, так и в комплексе в составе компьютерной системы[1].

---

[1] Лозовский Д.Н., Лозовская Н.Н., Ульянова И.Р. К вопросу о первоначальном этапе расследования интернет-преступлений // Гуманитарные, социально-экономические и общественные науки. – 2017. – № 9. – С. 83.

[1] Алабушева Н.П. XXI век – век преступлений в сфере компьютерной информации // Общество и право. – 2018. – № 4. – С. 89.

— судебная программно-компьютерная экспертиза, назначаемая для исследования программного обеспечения. Объекты включают: системное программное обеспечение; прикладное программное обеспечение (текстовые и графические редакторы, системы управления базами данных, электронные таблицы); авторское программное обеспечение потребительского назначения. Задачами этой экспертизы являются: классификация и определение основных характеристик операционной системы, используемых технологий системного программирования; выявление, исследование функциональных свойств и состояния программного обеспечения; исследование алгоритма программного продукта, типов поддерживаемых аппаратных платформ; определение причин, целей и условий изменения свойств и состояния программного обеспечения; индивидуальное отождествление оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы; установление групповой принадлежности программного обеспечения; выявление индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы;

— судебная информационно-компьютерная экспертиза, имеющая цель поиск, обнаружение, анализ и оценку информации, подготовленной пользователем или порожденной программами для организации информационных процессов в компьютерной системе.

Экспертными задачами здесь являются: установление вида, свойств и состояния информации (фактического и первоначального, в том числе до ее удаления и модификации) в компьютерной системе; определение причин и условий изменения свойств исследуемой информации; определение механизма, динамики и обстоятельств события по имеющейся информации на носителе данных или ее копиям; установление участников события, их роли, места, условий, при которых была создана (модифицирована, удалена) информация; установление соответствия либо несоответствия действий

с информацией специальному регламенту (правилам), например, правомерно ли конкретное использование информации, защищенной паролем, и др.[1]

По делам данной категории могут назначаться судебные экспертизы других классов и родов: судебно-трасологические – для анализа следов взлома, следов рук как на внешних, так и на внутренних поверхностях компьютеров и их комплектующих; судебно-экономические, в частности финансово-экономические и бухгалтерские, если преступления совершаются в кредитно-финансовой сфере; судебно-технические экспертизы документов, когда компьютер используется как средство для изготовления поддельных документов, фальшивых денежных билетов; фоноскопические экспертизы – при использовании средств прослушивания переговоров и др.

Отметим, что в ходе расследования преступлений, посягающих на информационную безопасность, правоохранительные органы также осуществляют взаимодействие с другими организациями, в частности, с операторами связи. Обеспечение защиты граждан от преступных посягательств, эффективное раскрытие и расследование совершенных преступлений в современных условиях невозможно без использования информации, циркулирующей в сетях электросвязи, и без привлечения для этого технических ресурсов операторов связи. Однако действия правоохранительных органов по получению такой информации связаны требованием ч. 2 ст. 23 Конституции РФ, установившей, что право граждан на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений может быть ограничено только на основании судебного решения. В связи с этим возникает вопрос о том, вся ли имеющая значение для предупреждения и раскрытия преступлений информация, находящаяся в распоряжении операторов связи, попадает в сферу действия этого конституционного права, либо какую-то ее часть оно не затрагивает. Готового ответа на этот вопрос законодатель не дает, а ученые и

[1] Козьминых С.И. Моделирование систем и процессов обеспечения информационной безопасности в органах внутренних дел // Вестник Московского университета МВД России. – 2016. – № 2. – С. 163.

правоприменители придерживаются различных позиций о необходимости судебного разрешения на получение, например, персональных данных абонентов сетей связи, сведений об IMEI-номерах мобильных телефонов, данных о соединениях между неопределенным кругом абонентов на конкретной территории и некоторых других сведений.

Между тем, персональные данные абонентов сетей электросвязи составляют отдельную группу сведений, носящих конфиденциальный характер, но не относящихся к тайне телефонных переговоров, а их получение от операторов связи для решения задач оперативно-розыскной деятельности и уголовного судопроизводства не требует судебного разрешения. В качестве дополнительного аргумента к нашему выводу можно сослаться на известное среди специалистов Определение Конституционного Суда РФ от 02 октября 2003 г. № 345-О, в котором применительно к предмету запроса заявителя дано конституционно-правовое толкование права на тайну телефонных переговоров. В мотивировочной части этого решения было установлено, что «право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления.

В силу этого, информацией, составляющей охраняемую Конституцией РФ и действующими на территории РФ законами тайну телефонных переговоров, считаются любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи; для доступа к указанным сведениям органам, осуществляющим оперативно-розыскную деятельность, необходимо получение судебного решения»[1].

[1] Определение Конституционного Суда Российской Федерации «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке

Анализ приведенного положения позволяет заключить, что персональные данные абонента в силу своего содержания и механизма появления не могут быть отнесены к сведениям, «передаваемым, сохраняемым и устанавливаемым с помощью телефонной аппаратуры», которые Конституционный Суд РФ отнес к тайне телефонных переговоров.

Вопрос о правовом режиме получения сведений у операторов связи об IMEI-номере мобильного устройства, как заслуживающий отдельного внимания, был затронут в Обзоре судебной практики Верховного Суда России, который пришел к выводу о «необходимости получения судебного решения для определения местоположения телефонного аппарата относительно базовой станции, а также для определения идентификационных абонентских устройств объектов оперативной заинтересованности» (п. 7.3)[2].

Итак, расследование и раскрытие преступлений, посягающих на информационную безопасность, может быть эффективным только при успешном и слаженном взаимодействии правоохранительных органов. В основе взаимодействия правоохранительных органов находятся следующие принципы: законность, комплексное использование сил и средств, персональная ответственность исполнителей, непрерывность и согласованность. Взаимодействие правоохранительных органов в ходе расследования преступлений, посягающих на информационную безопасность, может быть более эффективным, если на федеральном уровне будут разработаны единые регламенты взаимодействия между структурами.

конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи»» от 02 октября 2003 г. № 345-О // Вестник Конституционного Суда РФ. – 2003. – № 23.

[2] Обзор судебной практики по уголовным делам о преступлениях, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих и ядовитых веществ (утв. Президиумом Верховного Суда Российской Федерации 27 июня 2012 г.) // Бюллетень Верховного Суда РФ. – 2012. – № 18.

ЗАКЛЮЧЕНИЕ

По результатам проведенного исследования, подведем обобщающие итоги по теме выпускной квалификационной работы.

История организации защиты государственной тайны в России документально прослеживается со времен Петра I. Исторический опыт обеспечения сохранности государственных секретов в ряде вопросов явился прообразом настоящего порядка, в частности порядка обращения с секретными документами. Однако, до настоящего времени многие вопросы правового регулирования института защиты государственной тайны в России продолжают оставаться нерешенными.

В настоящее время под информационной безопасностью подразумевают состояние защищенности личности, государства и общества от внешних и внутренних информационных угроз, при котором обеспечиваются осуществление конституционных прав и свобод личности, достойные уровень и качество жизни людей, устойчивое социально-экономическое развитие РФ, территориальная целостность, суверенитет, безопасность и оборона государства. Информационная безопасность признается элементом национальной безопасности наряду с государственной, экологической, общественной, транспортной, экономической, энергетической, безопасностью личности. Ключевыми задачами обеспечения информационной безопасности выступают: осуществление конституционных прав и свобод личности в информационной сфере; интеграция нашей страны в мировое информационное пространство; защита и совершенствование российской информационной инфраструктуры; противодействие угрозе развязывания противоборства в сфере информации.

Информационная безопасность является составной частью общей и национальной безопасности и охватывает все сферы деятельности государства, гражданина, а также различных организаций и бизнеса.

Одним из субъектов обеспечения информационной безопасности являются правоохранительные органы. К правоохранительным органам, осуществляющим обеспечение информационной безопасности, относятся: МВД России, ФСБ России, ФТС России, СВР России, ФСО России, органы прокуратуры, судебные органы и др.

В числе основных направлений деятельности, реализуемых правоохранительными органами в рамках обеспечения информационной безопасности, можно выделить следующие: профилактика и предупреждение преступлений, посягающих на информационную безопасность; расследование и раскрытие преступлений, посягающих на информационную безопасность; осуществление правосудия по делам о преступлениях, посягающих на информационную безопасность.

Расследование и раскрытие преступлений, посягающих на информационную безопасность, может быть эффективным только при успешном и слаженном взаимодействии правоохранительных органов. В основе взаимодействия правоохранительных органов находятся следующие принципы: законность, комплексное использование сил и средств, персональная ответственность исполнителей, непрерывность и согласованность. Взаимодействие правоохранительных органов в ходе расследования преступлений, посягающих на информационную безопасность, может быть более эффективным, если на федеральном уровне будут разработаны единые регламенты взаимодействия между структурами.

В рамках настоящего исследования, нами было установлено, что правоохранительные органы не располагают достаточной информационно-технической и программной базой для расследования преступлений в сфере информационной безопасности. Все структуры правоохранительных органов действуют по-разному, при обнаружении факта совершения преступления.

Отсутствие четкого алгоритма взаимодействия подразделений полиции и других структур ведет к тому, что большая часть преступлений остается нераскрытой, оперативники не могут получить достаточно данных для того,

чтобы квалифицировать преступление, опираясь на его признаки. Кроме того, кадровый состав суда, прокуратуры и полиции не имеет достаточного уровня подготовки для профилактики таких преступлений и их эффективного расследования.

В России действует единая система учета совершенных преступлений, однако, она не отвечает специфике совершения преступлений в сфере информационной безопасности.

С целью повышения эффективности профилактики преступлений в сфере информационной безопасности, расследования преступлений и защиты интересов граждан предлагается применить несколько необходимых мер:

— разработать и внедрить проект, который бы предусматривал постоянное функционирование и отслеживание потоков компьютерной информации. Такая система могла бы выявлять при помощи алгоритмов попытки совершения преступлений, а также устанавливать слежение за активными элементами, которые ведут подозрительную деятельность. Эта система могла бы использоваться и для профилактики преступлений;

— в связи с активизацией преступных элементов за рубежом требуется разработать и внедрить стандарты, которые бы стали регулировать порядок взаимодействия российских правоохранительных органов и органов других стран. В связи с тем, что обеспечение информационной безопасности возложено не только на специальные подразделения и полицию, но и на владельцев, носителей и хранителей информации, необходимо наладить взаимодействие между социальными фондами, банками, владельцами серверов и оборудование путем регламентирования норм взаимодействия. Координированные действия заинтересованных в обеспечении информационной безопасности структур позволили бы проводить профилактику преступлений, отслеживать действия подозрительных лиц и эффективно взаимодействовать при обнаружении признаков совершения преступления;

— для эффективного расследования таких преступлений необходимо разработать единую тактику и стратегию. К данной работе следует привлекать высококвалифицированных специалистов. При осуществлении агентурной работы следует пересмотреть качественный состав субъектов, с целью установления конфиденциального и эффективного сотрудничества;

— для личного состава правоохранительных структур необходимо предусмотреть разработку и принятие программ подготовки. С целью выполнения долгосрочной стратегии следует предусмотреть возможности для организации переподготовки специалистов в сфере обеспечения информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Раздел 1 Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации от 12 декабря 1993 г. // Российская газета. – 1993. – 25 декабря.
2. Федеральный закон «О безопасности» от 28 декабря 2010 г. № 390-ФЗ // Собрание законодательства РФ. – 2010. – № 42. – Ст. 5633.
3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ // Собрание законодательства РФ. – 2006. – № 23. – Ст. 2135.
4. Федеральный закон «О внешней разведке» от 10 января 1996 г. № 5-ФЗ // Российская газета. – 1996. – 22 января.
5. Федеральный закон «О Федеральной службе безопасности» от 03 апреля 1995 г. № 40-ФЗ // Российская газета. – 1995. – 15 апреля.
6. Федеральный закон «О федеральной фельдъегерской связи» от 17 декабря 1994 г. № 67-ФЗ // Российская газета. – 1994. – 29 декабря.
7. Федеральный закон от 17 января 1992 г. № 2202-1 «О прокуратуре Российской Федерации» // Российская газета. – 1992. – 30 января.
8. Указ Президента Российской Федерации «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» от 09 мая 2017 г. № 203 // Российская газета. – 2017. – 15 мая.
9. Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05 декабря 2016 г. № 646 // Российская газета. – 2016. – 16 декабря.
10. Указ Президента Российской Федерации «О Стратегии национальной безопасности Российской Федерации» от 31 декабря 2015 г. № 683 // Российская газета. – 2015. – 31 декабря.

Раздел 2 Литература

11. Абубекерова, Д.А. Система органов обеспечения безопасности в Российской Федерации / Д.А. Абубекерова // Наука. Общество. Государство. – 2016. – № 4(16). – С. 89 – 95.
12. Алабушева, Н.П. XXI век – век преступлений в сфере компьютерной информации / Н.П. Алабушева // Общество и право. – 2018. – № 4. – С. 89 – 95.
13. Алямкин, С.Н. Персональные данные как объект правового регулирования: понятие и способы защиты / С.Н. Алямкин // Мир науки и образования. – 2016. – № 4(8). – С. 31 – 38.
14. Антопольский, А.А. Правовые проблемы обеспечения баланса интересов при регулировании отношений по поводу информации конфиденциального характера / А.А. Антопольский // Юридическая наука и правоохранительная практика. – 2016. – № 2. – С. 164 – 167.
15. Ахметьянова, А.И., Кузнецова, А.Р. Проблемы обеспечения информационной безопасности в России и ее регионах / А.И. Ахметьянова, А.Р. Кузнецова // Фундаментальные исследования. – 2016. – № 8. – С. 82 – 86.
16. Введенская, О.Ю. Взаимодействие следователя с оперативными сотрудниками органа дознания при расследовании интернет-преступлений / О.Ю. Введенская // Общество и право. – 2016. – № 1(55). – С. 204 – 208.
17. Воронов, А.М. Таможенные органы как субъекты обеспечения безопасности государства / А.М. Воронов // Вестник Московского университета МВД России. – 2015. – № 1. – С. 242 – 247.
18. Гавриленко, А.А. Понятие и система правоохранительных органов / А.А. Гавриленко // Общество и право. – 2016. – № 7. – С. 94 – 100.

19. Гайдарева, И.Н. Информационная составляющая национальной безопасности / И.Н. Гайдарева // Общество и право. – 2011. – № 2. – С. 32 – 36.
20. Гатагонова, Р.М. Становление и развитие института защиты государственной тайны в России / Р.М. Гатагонова // Бизнес в законе. – 2015. – № 5. – С. 116 – 119.
21. Гильмуллина, Д.А. Государственная тайна в правовом государстве / Д.А. Гильмуллина // Известия Оренбургского государственного аграрного университета. – 2015. – № 9. – С. 17 – 22.
22. Голубчиков, С.В., Новиков, В.К., Баранова, А.В. Уровни и правовая модель информационной безопасности (защиты информации) / С.В. Голубчиков, В.К. Новиков, А.В. Баранова // Программные продукты и системы. – 2017. – № 2(30). – С. 320 – 328.
23. Грачев, С.И., Герасин, О.Н., Колобов, А.О., Ливерко, М.И. Проблемные аспекты в информационной политике и информационной безопасности России / С.И. Грачев, О.Н. Герасин, А.О. Колобов, М.И. Ливерко // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2014. – № 1(1). – С. 290 – 292.
24. Гурлеев, И.В., Курочкин, С.А. Организационно-правовые основы защиты государственной тайны в первые годы Советской власти / И.В. Гурлеев, С.А. Курочкин // Власть. – 2014. – № 11. – С. 12 – 19.
25. Ефремова, Н.А. Уголовно-правовая охрана сведений, составляющих коммерческую, банковскую и налоговую тайны / Н.А. Ефремова // Вестник Пермского университета. – 2015. – Вып. 1(27). – С. 124 – 130.
26. Закупень, Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности Российской Федерации / Т.В. Закупень // Наука. Общество. Право. – 2015. – № 2. – С. 123 – 128.
27. Зейналова, И.Д., Османов, М.Х. Правовое обеспечение информационной безопасности в российском информационном праве /

И.Д. Зейналова, М.Х. Османов // Законность. – 2016. – № 10. – С. 43 – 52.

28. Зиновьева, Е.С. Развитие информационного общества: проблемы безопасности / Е.С. Зиновьева // Вестник МГИМО Университета. – 2014. – № 4. – С. 36 – 44.
29. Зуев, В.И. Правоохранительная деятельность как функция правового государства / В.И. Зуев // Инновационная наука. – 2017. – № 5. – С. 112 – 117.
30. Иванов, Д.В. Правовые проблемы определения объектов информационной безопасности Российской Федерации / Д.В. Иванов // Пробелы в российском законодательстве. – 2015. – № 8. – С. 34 – 40.
31. Иванько, А.Ф., Иванько, М.А., Шанина, А.А. Информационная безопасность вчера и сегодня / А.Ф. Иванько, М.А. Иванько, А.А. Шанина // Молодой ученый. – 2017. – № 51. – С. 25 – 30.
32. Каптюг, Ю.А. Проблема информационной безопасности: дис. ... канд. юрид. наук / Ю.А. Каптюг. – М., 2009. – 213 с.
33. Ковалева, Н.Н. Информационное право России: учебник / Н.Н. Ковалева. – М.: Проспект, 2014. – 436 с.
34. Козьминых, С.И. Моделирование систем и процессов обеспечения информационной безопасности в органах внутренних дел / С.И. Козьминых // Вестник Московского университета МВД России. – 2016. – № 2. – С. 161 – 168.
35. Козьминых, С.И. Моделирование систем и процессов обеспечения информационной безопасности в органах внутренних дел / С.И. Козьминых // Вестник Московского университета МВД России. – 2016. – № 2. – С. 161 – 168.
36. Копылов, В.А. Информационное право: учебник / В.А. Копылов. – М.: Норма, 2013. – 512 с.
37. Костюченко, К.Л. Новые акценты в обеспечении информационной безопасности органов внутренних дел / К.Л. Костюченко // Вестник

Уральского юридического института МВД России. – 2015. – № 4. – С. 30 – 36.

38. Кучерявый, М.М. Анализ концептуальных основ политики национальной безопасности / М.М. Кучерявый // Среднерусский вестник общественных наук. – 2014. – № 1. – С. 81 – 87.
39. Лозовский, Д.Н., Лозовская, Н.Н., Ульянова, И.Р. К вопросу о первоначальном этапе расследования интернет-преступлений / Д.Н. Лозовский, Н.Н. Лозовская, И.Р. Ульянова // Гуманитарные, социально-экономические и общественные науки. – 2017. – № 9. – С. 83 – 90.
40. Михнев, И.П., Михнева, С.В., Сальникова, Н.А. Информационная безопасность в Российской Федерации: современность и перспективы развития / И.П. Михнев, С.В. Михнева, Н.А. Сальникова // Общество и право. – 2017. – № 3. – С. 56 – 65.
41. Пархоменко, С.В. Предупреждение информационной преступности в Российской Федерации: интегративный и комплексный подходы / С.В. Пархоменко // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – № 2. – С. 265 – 276.
42. Попов, А.Б. Предупреждение преступлений в сфере информации / А.Б. Попов // Вестник ТГУ. – 2015. – Вып. 12(56). – С. 330 – 334.
43. Потапов, С.А. Совершенствование расследования и раскрытия преступлений в сфере компьютерной информации / С.А. Потапов // Социально-экономические явления и процессы. – 2016. – № 10. – С. 16 – 24.
44. Решняк, М.Г., Павлова, Д.А. О некоторых особенностях раскрытия преступлений в сфере высоких информационных технологий / М.Г. Решняк, Д.А. Павлова // Экономико-юридический журнал. – 2015. – № 5. – С. 123 – 128.

45. Рыжова, О.А., Паменкова, И.А. Ответственность за разглашение врачебной тайны / О.А. Рыжова, И.А. Паменкова // Наука. Общество. Государство. – 2017. – № 3(19). – С. 78 – 84.
46. Синьков, Д.А. Повышение эффективности расследования преступлений в сфере компьютерной информации / Д.А. Синьков // Современные научные исследования и инновации. – 2017. – № 8. – С. 38 – 44.
47. Сипок, Р.П. Система органов государственной власти, обеспечивающих государственную безопасность Российской Федерации / Р.П. Сипок // Армия и общество. – 2014. – № 11. – С. 93 – 99.
48. Соловьева, Е.С. Информационная безопасность в современном обществе / Е.С. Соловьева // Наука. Практика. Право. – 2015. – № 5. – С. 12 – 19.
49. Трофимова, И.А. Административная ответственность за нарушение правил обработки и хранения персональных данных / И.А. Трофимова // Закон и право. – 2018. – № 7. – С. 160 – 167.
50. Хаханов, В.И., Литвинова, Е.И. Развитие киберпространства и информационная безопасность / В.И. Хаханов, Е.И. Литвинова // Власть. – 2014. – № 12. – С. 82 – 88.
51. Хомяков, О.Г. Информационная безопасность как составляющая прав граждан Российской Федерации / О.Г. Хомяков // Вестник Удмуртского университета. – 2014. – Вып. 3. – С. 93 – 100.
52. Чечетин, А.Е. Правовой режим доступа правоохранительных органов к информации операторов связи / А.Е. Чечетин // Вестник Воронежского института МВД России. – 2014. – № 3. – С. 98 – 105.
53. Шамсуев, М.Х. Теоретические аспекты изучения информационной безопасности / М.Х. Шамсуев // Инновационная наука. – 2016. – № 1. – С. 46 – 52.

Раздел 3 Постановления высших судебных инстанций и материалы судебной практики

54. Определение Конституционного Суда Российской Федерации от 07 февраля 2013 г. № 134-О // Вестник Конституционного Суда РФ. – 2013. – № 4.
55. Определение Конституционного Суда Российской Федерации «Об отказе в принятии к рассмотрению запроса Советского районного суда города Липецка о проверке конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи»» от 02 октября 2003 г. № 345-О // Вестник Конституционного Суда РФ. – 2003. – № 23.
56. Обзор судебной практики по уголовным делам о преступлениях, связанных с незаконным оборотом наркотических средств, психотропных, сильнодействующих и ядовитых веществ (утв. Президиумом Верховного Суда Российской Федерации 27 июня 2012 г.) // Бюллетень Верховного Суда РФ. – 2012. – № 18.
57. Определение Ленинского районного суда г. Челябинска от 24 сентября 2017 г. по делу № 11-24/2017. – Режим доступа: http://sudact.ru/
58. Апелляционное определение Московского городского суда от 10 августа 2017 г. по делу № 33-28318/2017. – Режим доступа: http://sudact.ru/
59. Приговор Гагаринского районного суда г. Москвы от 10 июня 2017 г. по делу № 1-160/2017. – Режим доступа: http://sudact.ru/
60. Решение Орджоникидзевского районного суда г. Магнитогорска Челябинской области от 23 марта 2017 г. по делу № 11-24/2017. – Режим доступа: http://sudact.ru/
61. Апелляционное определение Московского городского суда от 04 марта 2017 г. по делу № 33-7084. – Режим доступа: http://sudact.ru/