Раздел 3. Теория и практика управления

УДК 004.056 DOI 10.37279/2519-4453-2021-1-53-60

ФОРМИРОВАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРАНЫ И ЕЕ РЕГИОНОВ

Бойченко О.В.[1], Иванюта Д.В.[2]

[1]Институт экономики и управления (СП), ФГАОУ ВО КФУ им. В.И. Вернадского, 295015, г. Симферополь, ул. Севастопольская, 21/4, e-mail: bolek61@mail.ru
[2] Институт экономики и управления (СП), ФГАОУ ВО КФУ им. В.И. Вернадского, 295015, г. Симферополь, ул. Севастопольская, 21/4, e-mail: d.iwanyuta2011@yandex.ua

Аннотация. В статье, на основании статистических данных Министерства внутренних дел Российской Федерации за январь - декабрь 2020 года, обоснована необходимость проведения исследований, направленных на разработку новых подходов сфере обеспечения информационной безопасности страны и ее регионов и формирования соответствующей политики информационной безопасности. Проведен анализ основных подходов в сфере современной специфики обеспечения информационной безопасности страны и ее регионов, изучены основные принципы обеспечения информационной безопасности страны в части проведения последующий мероприятий, направленных на оптимизацию направлений региональной политики обеспечения информационной безопасности, а также уточнением и конкретизацией задач федеральной политики в области обеспечения региональной информационной безопасности.

Ключевые слова: информационная безопасность, регион, принципы, информация, угрозы, проблемы, информационные технологии.

ВВЕДЕНИЕ

В современном обществе информационно-коммуникационные технологии (далее ИКТ) являются важным фактором развития социально-экономической сферы и служат фундаментом процесса формирования прогрессивного и глобального информационного общества. Эффективность их использования способствует техническому прогрессу мирового сообщества, отдельных стран и регионов, и в свою очередь служит залогом экономического роста, обеспечивая устойчивость развития.

Однако внедрение новых технологий стало источником появления новых преступлений. К ним отнесем компьютерное мошенничество, которое может стать причиной экономических потерь, подделку информации, повреждение данных или программ, информационный саботаж. Это подтверждают статистические данные состояния преступности, представленные на сайте Министерства внутренних дел Российской Федерации. Так, за 2020 год число преступлений, совершенных с использованием информационно-телекоммуникационных технологий, возросло на 73,4% по сравнению с 2019 годом, в том числе с использованием сети «Интернет» – на 91,3%, при помощи средств мобильной связи – на 88,3% (рис. 1).

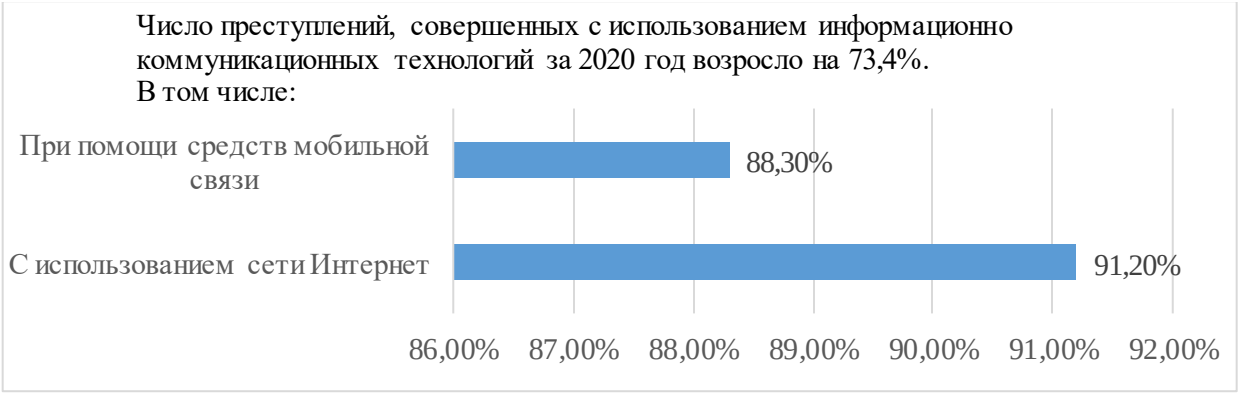

Рис. 1. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года. Составлено авторами по материалам [1]

Преступления в сфере информационных технологий стали причиной негативных социально-экономических последствий. Статистические данные подтверждают, что преступность в информационной сфере неуклонно растет и наносит большой моральный и материальный вред обществу, определяя необходимость совершенствования деятельности по обеспечению информационной безопасности, разработки основных теоретических положений и решения поставленных задач в этом направлении.

В связи с этим требуется учитывать, что в настоящее время ряд важных вопросов обеспечения информационной безопасности Российской Федерации и ее регионов еще недостаточно разработаны и требуют постоянного контроля и исследований.

Также процесс формирования эффективной системы обеспечения информационной безопасности должен способствовать выработке единого подхода к пониманию данных вопросов и рассмотрения их особенностей, задач и принципов. При этом эффективное взаимодействие между органами власти различных уровней, будет благоприятно сказываться на повышении эффективности решения поставленных проблем.

В ходе процесса формирования региональной политики в области информационной безопасности были определены следующие проблемы, требующие первоочередного решения. Приведем результаты проведенного анализа в таблице 1.

Таблица 1.

Проблемы формирования региональной политики в области информационной безопасности *

№ п/п	Проблемы	Описание
1	2	3
1	Выявление субъектами Российской Федерации жизненно важных интересов в информационной сфере в рамках предметов их совместного с Федерацией и исключительного ведения	Из множества важных целей социально-экономического развития региона необходимо выделить цели, успешность достижения которых определяет информационная сфера, при этом их защита является предметом региональной информационной безопасности
2	Обеспечение безопасного развития регионального информационного рынка	Вопрос обеспечения безопасности информационных ресурсов, их развития и использования должен рассматриваться как приоритетный, в деятельности региональных властей. Также важно понимание ценности таких ресурсов для всех субъектов информационного рынка, как отечественных, так и зарубежных
3	Обеспечение безопасности региональной информационной инфраструктуры	Рассмотрение основных угроз в этом направлении требует анализа надежности функционирования региональных информационных и телекоммуникационных систем и системы связи. Решение вопросов обеспечения безопасности информационных и телекоммуникационных систем федерального уровня должны регулироваться федеральным законодательством, что уже в значительной степени разработано. Особое внимание сейчас уделяют вопросам регулирования отношений в области обеспечения безопасности региональной составляющей информационной сферы России. На данный момент вопросы не решены в полном объеме и требуют отражения в договорах, определяющих разграничение полномочий между Российской Федерацией и ее субъектами
4	Развитие региональных информационных и телекоммуникационных систем как сегментов единого информационного пространства России.	Необходимо решать проблемы, связанные с сопряжением федеральной и региональной составляющей этого пространства, с целью содействия эффективности функционирования экономики России, развитию отечественного рынка товаров и услуг. В этой связи необходимо рассматривать не только информационные и системы, но и систему массового информирования граждан

*Источник: составлено авторами

Учитывая важность влияния ИКТ на формирование современного информационного общества, социально-экономическое развитие страны и ее регионов, также необходимо понимать, что информационные технологии уже стали своеобразной основой формирования глобального информационного общества.

В России для исследования и эффективного решения вопроса согласования федеральной и региональной политики по обеспечению информационной безопасности ведется работа по организации процесса рабочего взаимодействия между аппаратом Совета Безопасности Российской Федерации и межведомственными органами, создаваемыми субъектами.

АНАЛИЗ ПУБЛИКАЦИЙ, МАТЕРИАЛОВ И МЕТОДОВ

В статье использованы статистические данные о состоянии преступности в Российской Федерации, опубликованные на сайте Министерства внутренних дел Российской Федерации, за январь - декабрь 2020 года, которые подтверждают тенденцию роста преступлений, совершенных с использованием ИКТ.

Также в последнее время вышло большое количество публикаций, связанных с обеспечением информационной безопасности в социально-экономической сфере региона. В данных работах представлен неоднозначный подход к данному вопросу, а понятие «информационная безопасность» имеет различные толкования. Поэтому в нашей статье основным источником информации мы определили теоретические положения, представленные в Доктрине информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) (далее Доктрина). В данном документе сформулировано развернутое определение информационной безопасности и приведен исчерпывающий перечень принципов, на которых основана деятельность государственных органов по обеспечению информационной безопасности.

Хочется подчеркнуть, что, рассматривая состояние информационной безопасности в области современной науки и технологий в Доктрине, мы сталкиваемся с резкой критикой в адрес научного общества: подчеркивается «недостаточная эффективность научных исследований» в данной сфере, ведется речь о «низком уровне внедрения отечественных разработок» и «недостаточном кадровом обеспечении». В этой связи от современной науки ожидается значительные шаги по развитию технологических инноваций, способствующих укреплению информационной безопасности государства. Также обозначена серьезная проблема - проводимые мероприятия по обеспечению безопасности информационной инфраструктуры зачастую не имеют комплексной основы.

ЦЕЛЬ И ПОСТАНОВКА ЗАДАЧИ ИССЛЕДОВАНИЯ

Целью исследования является изучение принципов обеспечения информационной безопасности страны, формировании на их основе аспектов региональной политики информационной безопасности и постановки соответствующих задач по отношению к регионам.

Задачами исследования являются: изучение нормативно-правовых документов, определяющих основные направления обеспечения информационной безопасности страны, исследовании принципов деятельности государственных органов по обеспечению информационной безопасности, проведению анализа формирования региональной политики и основных задач федеральной политики в области обеспечения информационной безопасности по отношению к регионам.

ОСНОВНОЙ РАЗДЕЛ

Безопасность информационной системы страны предполагает обеспечение ее защиты от случайного или преднамеренного вмешательства в процесс функционирования, предотвращения попыток незаконных хищений, модификаций, разрушений ее компонентов. Для достижения безопасности системы требуется обеспечить конфиденциальность обрабатываемой информации, а также целостность и доступность компонентов и ресурсов системы.

Базовым документом выработки необходимых мер по совершенствованию системы обеспечения информационной безопасности является Доктрина информационной безопасности Российской Федерации. В данном нормативном правовом документе представлен официальный взгляд на решение вопроса обеспечения национальной безопасности страны в информационной сфере.

В Доктрине определено понятие информационной безопасности, под которой понимают «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [2].

Также особое внимание в документе уделено внутренним и внешним информационным угрозам, анализ которых должен быть полноценным с условием выявления источников внешних и внутренних угроз, способных потенциально оказать на систему защиты информации негативное и отрицательное воздействие. В ходе проведения анализа необходимо также учитывать такие виды угроз, как зависимость политической и экономической сферы общественной жизни России от зарубежных информационных структур, а также возможность манипулировать информацией (например, дезинформация, искажение или сокрытие информации).

Учитывая угрозы экономической и информационной безопасности, можно рассмотреть их влияние не только на отдельные компоненты государственной системы, но и регионы, а также крупные хозяйствующие субъекты и территориальные образования.

Например, информационные системы, в которые включены современные телекоммуникации, аналитическая и прогнозируемая информация имеют возможность воздействовать на состояние рынка ценных бумаг, а также состояние финансовой системы страны в целом. Результатом таких действий является колебание курсов национальных валют, изменение цен и снижение конкурентоспособности товаров и услуг. В итоге возникают угрозы экономической безопасности субъектов рынка государства.

Примером негативного характера, подтверждающим необходимость обеспечения информационной безопасности в экономической системе государства, является дефолт 1998 года, который произошел в процессе трансформации российской экономики.

Для достижения успеха в организации информационной безопасности необходимо рассмотреть создание единого механизма, который будет построен на общепризнанных принципах и нормах права.

В Доктрине представлены следующие принципы, на которых основана деятельность государственных органов по обеспечению информационной безопасности:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

Воздействуя на информационную среду становится возможным реализовать угрозы национальной безопасности в различных сферах человеческой деятельности. Это относится к формированию отношений в обществе и его реакции на происходящие процессы. В сфере экономики требуется предупредить рост уязвимости экономических структур от недостоверности, запаздывания и незаконного использования экономической информации.

Рассматривая причины появления внутренних факторов, порождающих опасность в информационной сфере, хочется выделить недостаточную сбалансированность интересов субъектов общественных отношений и необходимость активной деятельности государственных институтов, направленных на повышение уровня информационной безопасности [3].

Также требуется учитывать принципы разделения вопросов, находящихся в ведении Федерации и ее субъектов, порядок организации регулирования соответственных отношений в областях, с учетом определения предметов, отнесенных к совместному ведению, а также

выполнение федерального законодательства в части регулирования обеспечения безопасности России. Эти принципы определены в Конституции Российской Федерации.

Основанием для обеспечения информационной безопасности Российской Федерации служит единство федеральной и региональной политики в области информационной безопасности, которое должно быть реализовано при условии безусловного соблюдения федерального законодательства.

В нашей работе под регионом будем понимать территорию «субъекта Российской Федерации или ассоциаций субъектов Федерации, если эти ассоциации имеют необходимые полномочия по решению задач обеспечения региональной информационной безопасности».

Относительно самостоятельные аспекты региональной политики обеспечения информационной безопасности приведены на рис. 2.

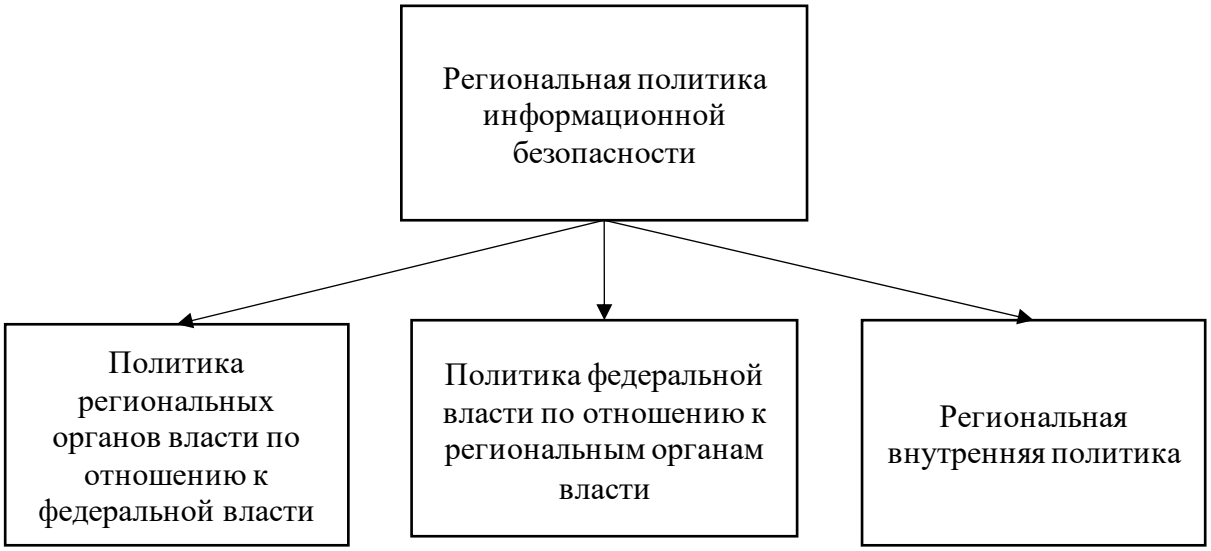

Рис. 2. Аспекты региональной политики обеспечения информационной безопасности
Источник составлен авторами

Региональная политика федеральной власти в области информационной безопасности формируется с учетом необходимости обеспечения защиты жизненно важных интересов Российской Федерации в информационной сфере по предметам совместного ведения Федерации и субъектов Федерации, предоставления необходимой помощи субъектам Федерации в защите их жизненно важных интересов в информационной сфере. К вопросам информационной безопасности в экономической сфере также относятся безопасность информационных систем управления промышленностью, отраслями, предприятиями, банками [4].

Также необходимо понимать, что процесс распространения ИКТ может служить в качестве создания естественного канала для проведения «информационной войны» в проблемных регионах Российской Федерации. Благодаря возможностям сети Интернет можно передавать указания и координировать действия, определяя цели и задачи различным террористическим и экстремистским группировкам, «внесистемной оппозиции» и организованным преступным сообществам.

Следовательно, необходимость участия регионов Российской Федерации в процессе международного информационного обмена требует разработки адекватных мер по обеспечению информационной безопасности с учетом взаимодействия с мировыми электронными коммуникациями [5].

Противодействие угрозам информационной безопасности в регионах Российской Федерации должно иметь высокую степень эффективности. При этом приоритетным объектом защиты во всех субъектах Федерации считают информационные ресурсы. Уделяется особое внимание сохранности информационных систем обеспечения деятельности органов государственной власти. Данное положение дел требует сформулировать комплекс задач, определяющих защиту информации в субъекте Федерации. Таким образом, для достижения надлежащего уровня информационной

безопасности и создания единого механизма первоочередного решения требуется решить следующие задачи (рис. 3).

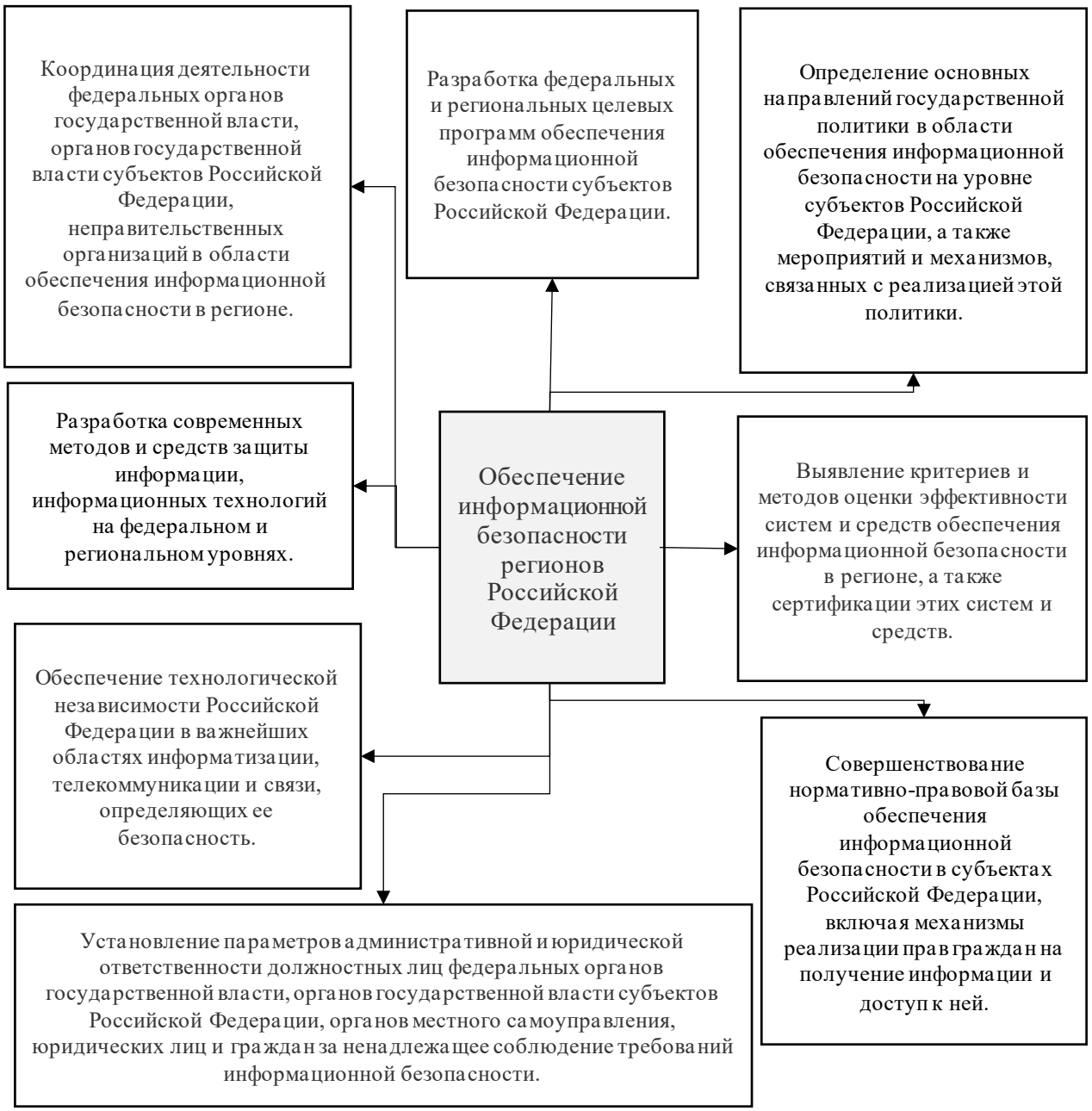

Рис. 3. Обеспечение информационной безопасности регионов Российской Федерации. Составлено авторами по материалам [6, с.64-71]

Считаем, что успех достижения поставленных задач федеральной политики в области обеспечения информационной безопасности по отношению к регионам предполагает проведение необходимого анализа, учета специфики и возможностей конкретного субъекта Российской Федерации.

ВЫВОДЫ

Вопрос обеспечения информационной безопасности социально-экономической сферы региона будет актуальным во все времена, а сейчас особенно, так как в стране и ее регионах полным ходом идет процесс государственного строительства и преодоления последствий мирового экономического кризиса. Успешное решение данного вопроса на государственном уровне зависит от полноты, достоверности информации, регулярности ее поступления не только из мировых и

национальных, но и в значительной степени из региональных источников. На данный момент необходимо рассматривать вышеперечисленные проблемы с учетом дальнейшего эффективного развития системы телекоммуникаций. Также предлагаем обратить особое внимание на недостаточную проработанность вопросов, связанных с отсутствием необходимых знаний и информации на уровне локальных социальных агрегаций, муниципальных институтов и органов государственного управления субъектов Федерации.

Таким образом, для обеспечения должного уровня информационной безопасности региона, требуется проведение глубокого анализа его социально-политических и экономических особенностей, рассмотрев при этом имеющиеся полномочия, ресурсы, и угрозы информационной безопасности.

В результате исследования к наиболее важным проблемам, требующим первоочередного внимания в процессе формирования политики обеспечения информационной безопасности и ее реализации, отнесем координацию цифрового неравенства, обеспечение прозрачности власти, защиту информационных ресурсов, работу по повышению уровня развития регионального законодательства в информационной сфере.

В заключении отметим, что информационная безопасность в современных условиях имеет большое значение и приобретает все большую актуальность. Этот факт требует глубокого теоретического осмысления основных понятий, принципов и задач применительно к обеспечению информационной безопасности в социально- экономической сфере региона.

ПЕРСПЕКТИВЫ ДАЛЬНЕЙШИХ ИССЛЕДОВАНИЙ

Рассматривая перспективы обеспечения информационной безопасности в социально-экономической сфере страны и ее регионов, предлагаем выполнение следующих действий с применением современных и эффективных средств и технологий:

Активизировать регулирование вопросов, направленных на противодействие монополизации, проводить необходимые мероприятия по предупреждению и пресечению недобросовестной конкуренции в информационной сфере, пресекать пропаганду и агитацию по разжиганию социальной розни;

Исследовать проблему осуществления контроля за развитием информационного рынка региона, способствовать решению проблем, касающихся обеспечения безопасности информационных ресурсов регионов, организации профилактики правонарушений в информационной сфере, исключив все возможные преступные посягательства на важную информацию различных группировок и отдельных лиц.

ЛИТЕРАТУРА

1. Официальный сайт Министерства внутренних дел Российской Федерации. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года от 21 января 2021 г. [Электронный ресурс] – Режим доступа: URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/.

2. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] – Режим доступа: URL: https://www.garant.ru/products/ipo/prime/doc/71456224/.

3. Гайсарова А.А. Особенности менеджмента информационной безопасности на современном этапе / А.А. Гайсарова //Экономика строительства и природопользования. – 2017. – № 1(2). – С. 64–70.

4. Емельянов, Г.В. Проблемы обеспечения информационной безопасности субъектов Российской Федерации [Текст] / Г.В. Емельянов, А.А. Стрельцов // Информационное общество. – М, 1998. – №6. – С.38-41.

5. Бойченко, О.В. Защита клиентской базы предприятия при использовании CRM-систем [Текст] / О.В. Бойченко, Е.С. Тупота // Актуальные проблемы и перспективы развития экономики: XIV Междунар. науч.-технич. конф., 12-14 ноября 2015 г.: тезисы докладов. – Симферополь, 2015. – С. 240-241.

6. Кафтанчиков, Д.П. Обеспечение информационной безопасности региона в условиях информатизации российского общества: актуальные проблемы и опыт ЦФО [Текст] / Д.П. Кафтанчиков // Среднерусский вестник общественных наук. – 2008. – № 2 (7). – С.64-71.

FORMATION OF INFORMATION SECURITI POLICY COUNTRIES AND ITS REGIONS

Boychenko O.V. [1], Ivanyuta D.V. [2]

[1] [2]Institute of Economics and Management, V. I. Vernadsky Crimean Federal University, Simferopol, Crimea

Annotation. The article, based on the statistical data of the Ministry of Internal Affairs of the Russian Federation for January - December 2020, substantiates the need for research aimed at developing new approaches to ensuring the information security of the country and its regions and the formation of an appropriate information security policy. The main approaches in the field of modern specifics of ensuring information security of the country and its regions were analyzed, the main principles of ensuring information security of the country were studied in terms of carrying out subsequent events aimed at optimizing the directions of the regional information security policy, as well as clarifying and specifying the objectives of the federal policy in the field of ensuring regional information security.

Key words: information security, region, principles, information, threats, problems, information technologies.